Ez a dokumentum kizárólag tájékoztató jellegű és nem vált ki joghatást. Az EU intézményei semmiféle felelősséget nem vállalnak a tartalmáért. A jogi aktusoknak – ideértve azok bevezető hivatkozásait és preambulumbekezdéseit is – az Európai Unió Hivatalos Lapjában közzétett és az EUR-Lex portálon megtalálható változatai tekintendők hitelesnek. Az említett hivatalos szövegváltozatok közvetlenül elérhetők az ebben a dokumentumban elhelyezett linkeken keresztül

►B

A BIZOTTSÁG (EU) 2016/799 VÉGREHAJTÁSI RENDELETE

(2016. március 18.)

a menetíró készülékek és alkatrészeik kialakítására, tesztelésére, beépítésére, működtetésére és javítására vonatkozó követelményeket meghatározó 165/2014/EU európai parlamenti és tanácsi rendelet végrehajtásáról

(EGT-vonatkozású szöveg)

(HL L 139., 2016.5.26., 1. o.)

Helyesbítette:

►C1 Helyesbítés, HL L 146., 2016.6.3., 31. o. (2016/799)

►C2 Helyesbítés, HL L 27., 2017.2.1., 169. o. (2016/799)

▼B

A BIZOTTSÁG (EU) 2016/799 VÉGREHAJTÁSI RENDELETE

(2016. március 18.)

a menetíró készülékek és alkatrészeik kialakítására, tesztelésére, beépítésére, működtetésére és javítására vonatkozó követelményeket meghatározó 165/2014/EU európai parlamenti és tanácsi rendelet végrehajtásáról

(EGT-vonatkozású szöveg)

1. cikk

Tárgy és hatály

(1) Ez a rendelet meghatározza a menetíró készülékekkel kapcsolatos alábbi szempontok egységes alkalmazásához szükséges rendelkezéseket:

a) a jármű helyzetének rögzítése bizonyos pontokon a járművezető napi munkaideje során;

b) az intelligens menetíró készülékeken végzett esetleges manipulációk és visszaélések korai távészlelése;

c) a menetíró készülékeket és az intelligens közlekedési rendszereket összekapcsoló interfész;

d) a menetíró készülékek típusjóváhagyására vonatkozó közigazgatási és műszaki követelmények, ideértve a biztonsági mechanizmusokat is.

(2) Az intelligens menetíró készülékek és alkatrészeik kialakítását, tesztelését, beépítését, vizsgálatát és javítását az e rendelet 1C. mellékletében meghatározott műszaki követelményeknek megfelelően kell végezni.

(3) A nem az intelligens menetíró készülékék kategóriájába tartozó menetíró készülékeknek kialakításuk, tesztelésük, beépítésük, vizsgálatuk és javításuk tekintetében továbbra is, értelemszerűen vagy a 3821/85/EGK tanácsi rendelet ([1]) I., vagy I. B. mellékletében meghatározott követelményeknek kell megfelelniük.

(4) A 96/53/EK irányelv 10d. cikkének megfelelően a korai távészlelő eszköznek a járművek fedélzetén elhelyezett tömegmérő berendezések segítségével mért adatokat is továbbítania kell az esetleges csalások mihamarabbi felderítése érdekében.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában a 165/2014/EU rendelet 2. cikkében szereplő fogalommeghatározások alkalmazandók.

Ezenkívül az alábbi fogalommeghatározásokat kell alkalmazni:

1. „digitális menetíró készülék” vagy „első generációs menetíró készülék”: olyan digitális menetíró készülék, amely nem tartozik az intelligens menetíró készülékék kategóriájába;

2. „külső GNSS-eszköz”: olyan eszköz, amely magában foglalja a GNSS-vevőt – abban az esetben, amikor a járműegység nem egyetlen egység –, valamint azokat a további alkatrészeket, amelyek a helyzetmeghatározási adatoknak a járműegység többi része felé való kommunikációjának védelmére szolgálnak;

([1]) A Tanács 1985. december 20-i 3821/85/EGK rendelete a közúti közlekedésben használt menetíró készülékekről (HL L 370., 1985.12.31., 8. o.).

▼B

3. „adatközlő mappa”: a teljes – papíralapú vagy elektronikus formátumú – mappa, amely a gyártó vagy meghatalmazottja által a típusjóváhagyó hatósághoz a menetíró készülék vagy valamelyik alkatrészének típusjóváhagyása céljára benyújtott összes információt tartalmazza, köztük a 165/2014/EU rendelet 12. cikkének (3) bekezdésében említett tanúsítványokat, valamint az e rendelet mellékletében meghatározott tesztek elvégzéséről készült jegyzőkönyveket, csakúgy mint rajzokat, fényképeket és egyéb idevágó dokumentumokat;

4. „információs csomag”: a papíralapú vagy elektronikus formátumú adatközlő mappa, minden olyan dokumentummal együtt, amelyet a típusjóváhagyó hatóság feladatköre ellátása során csatolt az adatközlő mappához, ideértve a típus-jóváhagyási folyamat végén a menetíró készüléknek vagy alkatrészének EK-típusbizonyítványát;

5. „az információs csomag tartalomjegyzéke”: az információs csomag számokkal ellátott részeit felsoroló és annak minden lényeges elemét azonosító dokumentum. A dokumentumban az EK-típusjóváhagyási folyamat egymást követő lépéseinek elkülöníthetőnek kell lenniük, és meg kell adni az információs csomag minden egyes felülvizsgálatának és aktualizálásának dátumát is;

6. „korai távészlelő eszköz”: a járműegység azon berendezése, amelyet célzott közúti ellenőrzések végzésére használnak;

7. „intelligens menetíró készülék” vagy „második generációs menetíró készülék”: a 165/2014/EU rendelet 8., 9. és 10. cikkének, valamint e rendelet mellékletének megfelelő digitális menetíró készülék;

8. „menetíró készülék alkatrésze” vagy „alkatrész”: a következő elemek valamelyike: járműegység, mozgásérzékelő, tachográfkártya, adatrögzítő lap, külső GNSS-eszköz és korai távészlelő eszköz;

9. „típusjóváhagyó hatóság”: a menetíró készülék vagy alkatrészei típusjóváhagyásának elvégzéséért, az engedélyezési eljárásért, valamint a típusbizonyítványok kiadásáért, illetve adott esetben visszavonásáért felelős tagállami hatóság, amely más tagállamok típusjóváhagyó hatóságainak viszonylatában kapcsolattartó pontként működik, és gondoskodik arról, hogy a gyártók eleget tegyenek az e rendelet követelményeinek teljesítésére vonatkozó kötelezettségeiknek.

3. cikk

Helyzetalapú szolgáltatások

(1) A gyártók kötelesek gondoskodni arról, hogy az intelligens menetíró készülékek kompatibilisek legyenek a Galileo navigációs rendszer és az európai geostacionárius navigációs lefedési szolgáltatási (EGNOS) rendszer által biztosított helyzetmeghatározási szolgáltatásokkal.

(2) A gyártók dönthetnek úgy is, hogy az (1) bekezdésben említett rendszerek mellett más műholdas navigációs rendszerekkel is biztosítják a kompatibilitást.

▼B

4. cikk

A menetíró készülékek és alkatrészeik típus-jóváhagyási eljárása

(1) A menetíró készülék vagy bármely alkatrészének vagy alkatrészei csoportjának típusjóváhagyására irányuló kérelmet a gyártó vagy meghatalmazottja nyújtja be az egyes tagállamok által kijelölt típusjóváhagyó hatóságokhoz. A kérelem az egyes alkatrészekkel kapcsolatos információkat tartalmazó adatközlő mappából áll, amely magában foglalja adott esetben a menetíró készülék kiegészítéséhez szükséges további alkatrészek típusbizonyítványait, valamint minden egyéb idevágó dokumentumot.

(2) A tagállamok minden olyan menetíró készülékre, azok alkatrészére, illetve alkatrészeik csoportjára megadják a típusjóváhagyást, amely megfelel az 1. cikk (2) vagy értelemszerűen (3) bekezdésében említett közigazgatási és műszaki követelményeknek. Ebben az esetben a típusjóváhagyó hatóság a kérelmezőnek az e rendelet II. mellékletében meghatározott mintának megfelelő típusbizonyítványt állít ki.

(3) A típusjóváhagyó hatóság a gyártót vagy meghatalmazottját további információk benyújtására kérheti.

(4) A gyártó vagy meghatalmazottja annyi menetíró készüléket, illetve annyi alkatrészt bocsát a típusjóváhagyó hatóságok és a 165/2014/EU rendelet 12. cikkének (3) bekezdésében említett tanúsítványok kiállításáért felelős jogi személyek rendelkezésére, amennyi alapján megfelelő módon elvégezhető a típus-jóváhagyási eljárás.

(5) Amennyiben a gyártó vagy meghatalmazottja a menetíró készülék bizonyos alkatrészeire vagy alkatrészcsoportjaira kér típusjóváhagyást, a típusjóváhagyó hatóságok rendelkezésére bocsátja az egyéb, már típusjóváhagyást kapott alkatrészeket, valamint a teljes menetíró készülék kialakításához szükséges egyéb részeket annak érdekében, hogy az említett hatóságok a szükséges teszteket el tudják végezni.

5. cikk

A típusjóváhagyások módosításai

(1) A gyártó vagy meghatalmazottja haladéktalanul tájékoztatja az eredeti típusjóváhagyást megadó típusjóváhagyó hatóságokat a menetíró készülék szoftverének vagy hardverének vagy a készülék legyártásához használt, az adatközlő mappába bejegyzett anyagok jellegének bármilyen módosításáról, és a típusjóváhagyás módosítására irányuló kérelmet nyújt be.

(2) A típusjóváhagyó hatóságok felülvizsgálhatják vagy kiterjeszthetik a meglévő típusjóváhagyást, vagy a módosítások jellegének és jellemzőinek megfelelően új típusjóváhagyást adhatnak ki.

„Felülvizsgálatra” akkor kerül sor, ha a típusjóváhagyó hatóság úgy ítéli meg, hogy a menetíró készülék szoftverének vagy hardverének, illetve a készülék legyártásához használt anyagok jellegének módosítása nem számottevő. Ebben az esetben a típusjóváhagyó hatóság kiadja az információs csomagot alkotó dokumentumok felülvizsgált változatát, amelyekben feltünteti a módosítások jellegét és az idevágó jóváhagyás megadásának időpontját. Az e követelménynek való megfelelés teljesíthető az információs csomag aktualizált, egységes szerkezetbe foglalt és az elvégzett módosítások részletes leírásával kiegészített változatával.

▼B

„Kiterjesztésre” akkor kerül sor, ha a típusjóváhagyó hatóság úgy ítéli meg, hogy a menetíró készülék szoftverének vagy hardverének, illetve a készülék legyártásához használt anyagok jellegének módosítása számottevő mértékű. Ebben az esetben új tesztek elvégzését kérheti, amiről tájékoztatja a gyártót vagy annak meghatalmazottját. Ha e tesztek eredménye megfelelőnek bizonyul, a típusjóváhagyó hatóság felülvizsgált típusbizonyítványt állít ki, amely a megadott kiterjesztés számát is tartalmazza. A típusbizonyítványban meg kell adni a kiterjesztés indokát és a dokumentum kiállításának időpontját.

(3) Az információs csomag tartalomjegyzékében fel kell tüntetni a típusjóváhagyás legutóbbi kiterjesztésének vagy felülvizsgálatának vagy a típusjóváhagyás legutóbbi aktualizálásának és egységes szerkezetbe foglalásának időpontját.

(4) Új típusjóváhagyásra akkor lehet szükség, ha a típusjóváhagyásban részesített menetíró készülék vagy alkatrészeinek kért módosításai új biztonsági vagy interoperabilitási tanúsítvány kiállítását vonnák maguk után.

6. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ezt a rendeletet 2016. március 2-től kell alkalmazni.

Mellékletei azonban csak 2019. március 2-től alkalmazandók, a 16. függelék kivételével, amelyet szintén 2016. március 2-től kell alkalmazni.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

▼B

I. C. MELLÉKLET

Kialakítási, tesztelési, beépítési és vizsgálati követelmények

BEVEZETÉS

1. FOGALOMMEGHATÁROZÁSOK

2. AZ ADATRÖGZÍTŐ KÉSZÜLÉK ÁLTALÁNOS JELLEMZŐI ÉS FUNKCIÓI

2.1. Általános jellemzők

2.2. Funkciók

2.3. Üzemmódok

2.4. Biztonság

3. AZ ADATRÖGZÍTŐ KÉSZÜLÉK KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

3.1. A kártyabehelyezések és -kivételek nyomon követése

3.2. Sebesség-, helyzet- és távolságmérés

3.2.1. A megtett távolság mérése

3.2.2. Sebességmérés

3.2.3. Helyzetmérés

3.3. Időmérés

3.4. A járművezető tevékenységének nyomon követése

3.5. A járművezetési állapot nyomon követése

3.6. Adatbevitel a járművezetők által

3.6.1. Azon helyek bevitele, ahol a munkanapok kezdődnek és/vagy végződnek

3.6.2. A járművezető tevékenységével kapcsolatos adatok és a járművezető ITS-interfésszel kapcsolatos hozzájárulásának kézi bevitele

3.6.3. Különleges körülmények bevitele

3.7. A vállalkozások általi lezárások kezelése

3.8. Az ellenőrzési tevékenység nyomon követése

3.9. Események és/vagy hibák észlelése

3.9.1. „Érvénytelen kártya behelyezése”

3.9.2. „Kártyaütközés”

3.9.3. „Időátfedés”

3.9.4. „Járművezetés megfelelő kártya nélkül”

3.9.5. „Kártya behelyezése járművezetés közben”

3.9.6. „Utolsó kártyakapcsolat nem megfelelő lezárása”

3.9.7. „Gyorshajtás”

3.9.8. „Áramellátás megszakadása”

3.9.9. „Kommunikációs hiba a távoli kommunikációs eszközzel”

3.9.10. „A GNSS-vevőből származó helyzetmeghatározási információk hiánya”

▼B

3.9.11.	„Kommunikációs hiba a külső GNSS-eszközzel”
3.9.12.	A „mozgásadatok hibája”
3.9.13	„A jármű mozgásával kapcsolatos ellentmondás”
3.9.14.	A „biztonsági rendszer megsértésére irányuló kísérlet”
3.9.15.	„Időütközés”
3.9.16.	Kártyahiba
3.9.17.	Az „adatrögzítő készülék” hibája
3.10.	Beépített és önellenőrző tesztek
3.11.	Az adatmemória leolvasása
3.12.	Rögzítés és tárolás az adatmemóriában
3.12.1.	Készülékazonosítási adatok
3.12.1.1.	Járműegység-azonosítási adatok
3.12.1.2.	A mozgásérzékelő azonosítási adatai
3.12.1.3.	A globális navigációs műholdrendszerek azonosítási adatai
3.12.2.	Kulcsok és tanúsítványok
3.12.3.	A járművezetői vagy műhelykártya behelyezési és kivételi adatai
3.12.4.	A járművezető tevékenységére vonatkozó adatok
3.12.5.	Azok a helyek (helységnév és földrajzi hely), ahol a munkanapok kezdődnek, végződnek és/vagy ahol a megszakítás nélküli járművezetési idő eléri a három óra többszörösét
3.12.6.	A kilométer-számláló adatai
3.12.7.	Részletes sebességadatok
3.12.8.	Az eseményekkel kapcsolatos adatok
3.12.9.	A hibákkal kapcsolatos adatok
3.12.10.	Kalibrálási adatok
3.12.11.	Időbeállítási adatok
3.12.12.	Az ellenőrzési tevékenységre vonatkozó adatok
3.12.13.	A vállalkozások általi lezárások adatai
3.12.14.	A letöltési tevékenységre vonatkozó adatok
3.12.15.	A különleges körülményekre vonatkozó adatok
3.12.16.	A tachográfkártya adatai
3.13.	A tachográfkártyák leolvasása
3.14.	Rögzítés és tárolás a tachográfkártyákon
3.14.1.	Rögzítés és tárolás az első generációs tachográfkártyákon
3.14.2.	Rögzítés és tárolás a második generációs tachográfkártyákon
3.15.	Kijelzés
3.15.1.	Az alapértelmezett adatok kijelzése
3.15.2.	Figyelmeztető kijelzés

▼B

3.15.3. A menü elérése

3.15.4. Egyéb kijelzett információk

3.16. Nyomtatás

3.17. Figyelmeztetések

3.18. Adatletöltés külső adathordozókra

3.19. Távoli kommunikáció a célzott közúti ellenőrzések céljára

3.20. Külső kiegészítő eszközök számára kiadott adatok

3.21. Kalibrálás

3.22. Közúti kalibrálási ellenőrzés

3.23. Időbeállítás

3.24. Teljesítményjellemzők

3.25. Anyagok

3.26. Jelölések

4. A TACHOGRÁFKÁRTYÁK KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

4.1. Látható adatok

4.2. Biztonság

4.3. Szabványok

4.4. Környezeti és elektromos előírások

4.5. Adattárolás

4.5.1. Az azonosítást és a kártya kezelését szolgáló elemi fájlok

4.5.2. Az integrált áramkörös kártyák azonosítása

4.5.2.1. Chipazonosítás

4.5.2.2. DIR (csak második generációs tachográfkártyákban van jelen)

4.5.2.3. ATR-információ (korlátozott, csak második generációs tachográfkártyákban van jelen)

4.5.2.4. Kiterjesztett hosszúságú információk (korlátozott, csak második generációs tachográfkártyákban van jelen)

4.5.3. Járművezetői kártya

4.5.3.1. Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.3.1.1. Alkalmazásazonosító

4.5.3.1.2. Kulcsok és tanúsítványok

4.5.3.1.3. A kártya azonosítása

4.5.3.1.4. A kártyatulajdonos azonosítása

4.5.3.1.5. Kártyaletöltés

4.5.3.1.6. Információk a vezetői engedélyről

4.5.3.1.7. Az eseményekkel kapcsolatos adatok

4.5.3.1.8. A hibákkal kapcsolatos adatok

4.5.3.1.9. A járművezető tevékenységére vonatkozó adatok

▼B

4.5.3.1.10. Az üzemeltetett járművek adatai

4.5.3.1.11. A munkanap kezdő és/vagy végső helye

4.5.3.1.12. Kártyakapcsolati adatok

4.5.3.1.13. Az ellenőrzési tevékenységre vonatkozó adatok

4.5.3.1.14. A különleges körülményekre vonatkozó adatok

4.5.3.2. Második generációs tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.3.2.1. Alkalmazásazonosító

4.5.3.2.2. Kulcsok és tanúsítványok

4.5.3.2.3. A kártya azonosítása

4.5.3.2.4. A kártyatulajdonos azonosítása

4.5.3.2.5. Kártyaletöltés

4.5.3.2.6. Információk a vezetői engedélyről

4.5.3.2.7. Az eseményekkel kapcsolatos adatok

4.5.3.2.8. A hibákkal kapcsolatos adatok

4.5.3.2.9. A járművezető tevékenységére vonatkozó adatok

4.5.3.2.10. Az üzemeltetett járművek adatai

4.5.3.2.11. A munkanap kezdő és/vagy végső helye (helységnév és földrajzi hely)

4.5.3.2.12. Kártyakapcsolati adatok

4.5.3.2.13. Az ellenőrzési tevékenységre vonatkozó adatok

4.5.3.2.14. A különleges körülményekre vonatkozó adatok

4.5.3.2.15. Az üzemeltetett járműegységek adatai

4.5.3.2.16. Azon helyek adatai, ahol a megszakítás nélküli járművezetési idő elérte a három órát

4.5.4. Műhelykártya

4.5.4.1. Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.4.1.1. Alkalmazásazonosító

4.5.4.1.2. Kulcsok és tanúsítványok

4.5.4.1.3. A kártya azonosítása

4.5.4.1.4. A kártyatulajdonos azonosítása

4.5.4.1.5. Kártyaletöltés

4.5.4.1.6. Kalibrálási és időbeállítási adatok

4.5.4.1.7. Az eseményekkel és a hibákkal kapcsolatos adatok

4.5.4.1.8. A járművezető tevékenységére vonatkozó adatok

4.5.4.1.9. Az üzemeltetett járművek adatai

4.5.4.1.10. A munkanapok kezdetére és/vagy végére vonatkozó adatok

4.5.4.1.11. Kártyakapcsolati adatok

4.5.4.1.12. Az ellenőrzési tevékenységre vonatkozó adatok

▼B

4.5.4.1.13. A különleges körülményekre vonatkozó adatok

4.5.4.2. Második generációs tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.4.2.1. Alkalmazásazonosító

4.5.4.2.2. Kulcsok és tanúsítványok

4.5.4.2.3. A kártya azonosítása

4.5.4.2.4. A kártyatulajdonos azonosítása

4.5.4.2.5. Kártyaletöltés

4.5.4.2.6. Kalibrálási és időbeállítási adatok

4.5.4.2.7. Az eseményekkel és a hibákkal kapcsolatos adatok

4.5.4.2.8. A járművezető tevékenységére vonatkozó adatok

4.5.4.2.9. Az üzemeltetett járművek adatai

4.5.4.2.10. A munkanapok kezdetére és/vagy végére vonatkozó adatok

4.5.4.2.11. Kártyakapcsolati adatok

4.5.4.2.12. Az ellenőrzési tevékenységre vonatkozó adatok

4.5.4.2.13. Az üzemeltetett járműegységek adatai

4.5.4.2.14. Azon helyek adatai, ahol a megszakítás nélküli járművezetési idő elérte a három órát

4.5.4.2.15. A különleges körülményekre vonatkozó adatok

4.5.5. Ellenőrzőkártya

4.5.5.1. Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.5.1.1. Alkalmazásazonosító

4.5.5.1.2. Kulcsok és tanúsítványok

4.5.5.1.3. A kártya azonosítása

4.5.5.1.4. A kártyatulajdonos azonosítása

4.5.5.1.5. Az ellenőrzési tevékenységre vonatkozó adatok

4.5.5.2. Második generációs (G2) tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.5.2.1. Alkalmazásazonosító

4.5.5.2.2. Kulcsok és tanúsítványok

4.5.5.2.3. A kártya azonosítása

4.5.5.2.4. A kártyatulajdonos azonosítása

4.5.5.2.5. Az ellenőrzési tevékenységre vonatkozó adatok

4.5.6. Vállalkozáskártya

4.5.6.1. Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.6.1.1. Alkalmazásazonosító

4.5.6.1.2. Kulcsok és tanúsítványok

4.5.6.1.3. A kártya azonosítása

▼B

4.5.6.1.4. A kártyatulajdonos azonosítása

4.5.6.1.5. A vállalkozás tevékenységére vonatkozó adatok

4.5.6.2. Második generációs (G2) tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.6.2.1. Alkalmazásazonosító

4.5.6.2.2. Kulcsok és tanúsítványok

4.5.6.2.3. A kártya azonosítása

4.5.6.2.4. A kártyatulajdonos azonosítása

4.5.6.2.5. A vállalkozás tevékenységére vonatkozó adatok

5. AZ ADATRÖGZÍTŐ KÉSZÜLÉK BEÉPÍTÉSE

5.1. Beépítés

5.2. Illesztési címke

5.3. Plombák

6. ELLENŐRZÉSEK, VIZSGÁLATOK ÉS JAVÍTÁSOK

6.1. Szerelők, műhelyek és járműgyártók jóváhagyása

6.2. Új vagy javított készülékek ellenőrzése

6.3. A beépítés vizsgálata

6.4. Időszakos vizsgálatok

6.5. A hibák mérése

6.6. Javítások

7. KÁRTYAKIBOCSÁTÁS

8. AZ ADATRÖGZÍTŐ KÉSZÜLÉKEK ÉS A TACHOGRÁFKÁRTYÁK TÍPUSJÓVÁHAGYÁSA

8.1. Általános szempontok

8.2. Biztonsági tanúsítvány

8.3. Működési tanúsítvány

8.4. Interoperabilitási tanúsítvány

8.5. Típusbizonyítvány

8.6. Különleges eljárás: első interoperabilitási tanúsítványok második generációs adatrögzítő készülékek és tachográfkártyák számára

BEVEZETÉS

Első generációs digitális menetíró rendszereket 2006. május 1. óta alkalmaznak. Ezek a készülékek a belföldi fuvarozásban élettartamuk végéig használhatók. A nemzetközi fuvarozásban ellenben 15 évvel e bizottsági rendelet hatálybalépését követően minden járművet az előírásoknak megfelelő, második generációs intelligens menetíró készülékkel kell felszerelni, mely használatát e rendelet vezeti be.

E melléklet azokat a követelményeket határozza meg, amelyek a második generációs adatrögzítő készülékekre és tachográfkártyákra vonatkoznak. Bevezetésük időpontjától kezdve kötelező lesz második generációs adatrögzítő készülékeket beépíteni az első alkalommal nyilvántartásba vett járművekbe, és második generációs tachográfkártyákat kell kiadni.

A második generációs menetíró rendszerek zökkenőmentes bevezetése érdekében

▼B

— a második generációs tachográfkártyákat úgy kell megtervezni, hogy első generációs járműegységekben is használni lehessen őket,

— bevezetésük időpontjában nem kell az érvényes első generációs tachográfkártyákat lecserélni.

Így a járművezetők mindkét rendszert használhatják majd egyedi járművezetői kártyájukat megtartva.

A második generációs adatrögzítő készülékek kalibrálása azonban csak második generációs műhelykártyákkal lesz lehetséges.

E melléklet az első és a második generációs menetíró rendszerek közötti interoperabilitással kapcsolatos összes követelményt tartalmazza.

A 15. függelék további információkat tartalmaz arra vonatkozóan, hogy a két rendszer egyidejű használata miként valósítható meg.

Függelékek listája

1. függelék: ADATSZÓTÁR

2. függelék: A TACHOGRÁFKÁRTYÁKRA VONATKOZÓ ELŐÍRÁSOK

3. függelék: PIKTOGRAMOK

4. függelék: KINYOMATOK

5. függelék: KIJELZÉS

6. függelék: ELŐLAPI KALIBRÁLÁSI ÉS LETÖLTŐ CSATLAKOZÓ

7. függelék: ADATLETÖLTÉSI PROTOKOLLOK

8. függelék: KALIBRÁLÁSI PROTOKOLL

9. függelék: TÍPUSJÓVÁHAGYÁS ÉS A MINIMÁLISAN ELŐÍRT TESZTEK JEGYZÉKE

10. függelék: BIZTONSÁGI KÖVETELMÉNYEK

11. függelék: KÖZÖS BIZTONSÁGI MECHANIZMUSOK

12. függelék: A GLOBÁLIS NAVIGÁCIÓS MŰHOLDRENDSZEREN (GNSS-RENDSZEREN) ALAPULÓ HELYZETMEGHATÁROZÁS

13. függelék: ITS-INTERFÉSZ

14. függelék: TÁVOLI KOMMUNIKÁCIÓS FUNKCIÓ

15. függelék: MIGRÁLÁS: KÜLÖNFÉLE GENERÁCIÓJÚ KÉSZÜLÉKEK EGYÜTTES MŰKÖDTETÉSE

16. függelék: AZ M1 ÉS N1 KATEGÓRIÁJÚ JÁRMŰVEKBE ÉPÍTENDŐ ADAPTER

1 FOGALOMMEGHATÁROZÁSOK

Ebben a mellékletben:

a) „aktiválás”:

az a szakasz, amelyben a menetíró készülék a műhelykártya használata révén teljes mértékben üzemképessé válik, és valamennyi funkcióját üzembe helyezi, beleértve a biztonsági funkciókat is;

b) „hitelesítés”:

azon funkció, amelynek célja a személyazonosság megállapítása és ellenőrzése;

c) „hitelesség”:

az ellenőrizhető személyazonosságú felektől származó információk tulajdonsága;

d) „beépített teszt (BIT)”:

olyan, kérésre végrehajtott tesztek, amelyeket a kezelő vagy valamely külső berendezés indít el;

▼B

e) „naptári nap”:

00 óra 00 perctől 24 óra 00 percig terjedő nap. Minden naptári nap az egyeztetett világidőhöz (UTC) viszonyítandó;

f) intelligens menetíró készülék „kalibrálása”:

az adatmemóriában tárolandó járműparaméterek frissítése vagy megerősítése. A járműparaméterek magukban foglalják a jármű azonosító adatait (jármű jármű-azonosító száma [VIN], rendszáma [VRN] és a nyilvántartásba vétel szerinti tagállam), valamint a jármű jellemzőit (w, k, l, abroncsméret; a sebességkorlátozó készülék beállítása [adott esetben], az aktuális UTC idő, a kilométer-számláló aktuális értéke); az adatrögzítő készülék kalibrálása során minden, a típusjóváhagyás szempontjából lényeges plomba típusát és azonosítóját el kell menteni az adatmemóriába;

az UTC idő aktualizálását, illetve megerősítését nem kalibrálásnak, hanem időbeállításnak kell tekinteni, amennyiben ez nem mond ellent a 409. követelménynek;

az adatrögzítő készülék kalibrálásához műhelykártya használata szükséges;

g) „kártyaszám”:

azon 16 alfanumerikus karakterből álló szám, amely egyértelműen azonosítja a tachográfkártyát egy tagállamon belül. A kártyaszám magában foglalja a kártya konszekutív indexét (adott esetben), a kártyacsereindexet és a kártya megújítási indexét;

a kártya egyértelmű azonosítása tehát a kiállító tagállam kódjával és a kártyaszámmal lehetséges;

h) „a kártya konszekutív indexe”:

a kártyaszám tizennegyedik alfanumerikus karaktere, amely arra szolgál, hogy a több tachográfkártyát is átvenni jogosult társaságnak, műhelynek vagy ellenőrző hatóságnak kibocsátott különböző kártyákat megkülönböztesse. A társaság, a műhely vagy az ellenőrző hatóság egyértelmű azonosítása a kártyaszám első 13 karakterével lehetséges;

i) „a kártya megújítási indexe”:

a kártyaszám tizenhatodik alfanumerikus karaktere, melyet a tachográfkártya minden egyes megújítása alkalmával eggyel növelnek;

j) „kártyacsereindex”:

a kártyaszám tizenötödik alfanumerikus karaktere, melyet a tachográfkártya minden egyes cseréje alkalmával eggyel növelnek;

k) „a jármű jellemző együtthatója”:

az a jellemző számérték, amely megadja a jármű és az adatrögzítő készülék közötti kapcsolatot biztosító alkatrész (sebességváltó kimenőtengelye vagy a keréktengely) által azon idő alatt kibocsátott kimenő jel értékét, mialatt a jármű a 414. követelményben meghatározott rendes vizsgálati feltételek mellett egy kilométernyi távolságot megtesz. A jellemző együtthatót kilométerenkénti impulzusszámban (w = … imp/km) kell kifejezni;

l) „vállalkozáskártya”:

egy tagállam hatóságai által azon fuvarozási vállalkozások részére kiállított tachográfkártya, amelyek menetíró készülékkel felszerelt járműveket kötelesek üzemeltetni; e kártya azonosítja a fuvarozási vállalkozást, és lehetővé teszi a menetíró készülékben tárolt, az adott fuvarozási vállalkozás által lezárt adatok megjelenítését, letöltését és kinyomtatását;

▼B

m) „az adatrögzítő készülék állandója”:

az egy kilométernyi megtett távolság kijelzéséhez és rögzítéséhez szükséges bemenő jel értékét megadó jellemző számérték; ezen állandót kilométerenkénti impulzusszámban (k = … imp/km) kell kifejezni;

n) a „megszakítás nélküli járművezetési időt” az adatrögzítő készülék számítja ki a következő módon ([1]):

a megszakítás nélküli járművezetési időt egy meghatározott járművezető utolsó KÉSZENLÉTE vagy SZÜNETE/PIHENÉSE vagy legalább 45 perces ISMERETLEN ([2]) időszaka óta eltelt mindenkori halmozott járművezetési idejeként kell kiszámítani (ez az időszak az 561/2006/EK európai parlamenti és tanácsi rendelet ([3]) értelmében több rövidebb időszakból is állhat). A számítások céljára a járművezetői kártyán rögzített korábbi tevékenységeket is szükség szerint figyelembe kell venni. Amennyiben a járművezető nem helyezte be a kártyáját, a számítások azokon az adatokon alapulnak, amelyeket a memória a megfelelő időtartam (amikor nem volt kártya a készülékben) és a megfelelő kártyaolvasó egység vonatkozásában tárol;

o) „ellenőrzőkártya”:

egy tagállam hatóságai által az illetékes nemzeti ellenőrző hatóság részére kiállított tachográfkártya, amely azonosítja az ellenőrző szervet és opcionálisan az ellenőrző tisztviselőt, valamint lehetővé teszi az adatmemóriában vagy a járművezetői kártyán és opcionálisan a műhelykártyán tárolt adatokhoz való hozzáférést leolvasás, nyomtatás és/vagy letöltés céljából.

A kártya egyben lehetővé teszi, hogy a közúti ellenőrzések során kalibrálást végezzenek, és hozzáférést biztosít a korai távészleléssel történő kommunikációhoz használt leolvasó adataihoz.

p) a „halmozott pihenőidőt” az adatrögzítő készülék számítja ki a következő módon ([1]):

a halmozott pihenőidőt egy meghatározott járművezető utolsó KÉSZENLÉTE vagy SZÜNETE/PIHENÉSE vagy legalább 45 perces ISMERETLEN ([2]) időszaka óta eltelt mindenkori halmozott KÉSZENLÉTE vagy SZÜNETE/PIHENÉSE vagy legalább 15 perces ISMERETLEN ([3]) időszakai összegeként kell kiszámítani (ez az időszak az 561/2006/EK rendelet értelmében több rövidebb időszakból is állhat).

A számítások céljára a járművezetői kártyán rögzített korábbi tevékenységeket is szükség szerint figyelembe kell venni. Az ismeretlen, negatív tartamú (az ismeretlen időszak kezdete > az ismeretlen időszak vége), két különböző adatrögzítő készülék közötti időátfedésekből eredő időszakokat nem kell a számításnál figyelembe venni.

([1]) A megszakítás nélküli járművezetési idő és a halmozott pihenőidő számításának e módja arra szolgál, hogy az adatrögzítő készülék kiszámítsa, hogy mikor kell kibocsátani a megszakítás nélküli járművezetési idővel kapcsolatos figyelmeztetést. E számítási mód nem befolyásolja ezen időtartamok jogi értelmezését. A megszakítás nélküli járművezetési idő és a halmozott pihenőidő kiszámítására alternatív módszerek is alkalmazhatók, amennyiben e fogalommeghatározásokat újakkal kell felváltani, mivel azok az egyéb idevágó jogszabályok aktualizálása következtében elavulttá válnak.

([2]) Az ISMERETLEN időszakok azoknak az időszakoknak felelnek meg, amikor nem volt járművezetői kártya az adatrögzítő készülékben, és amikor a járművezetői tevékenységek kézi bevitele sem történt meg.

([3]) Az Európai Parlament és a Tanács 2006. március 15-i 561/2006/EK rendelete a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról, a 3821/85/EGK és a 2135/98/EK tanácsi rendelet módosításáról, valamint a 3820/85/EGK tanácsi rendelet hatályon kívül helyezéséről (HL L 102., 2006.4.11., 1. o.).

▼B

Amennyiben a járművezető nem helyezte be a kártyáját, a számítások azokon az adatokon alapulnak, amelyeket a memória a megfelelő időtartam (amikor nem volt kártya a készülékben) és a megfelelő kártyaolvasó egység vonatkozásában tárol;

q) „adatmemória”:

az adatrögzítő készülékbe épített elektronikus adattároló berendezés;

r) „digitális aláírás”:

egy adatblokkhoz csatolt olyan adat vagy az adatblokk olyan titkosított átalakítása, amelynek révén az adatblokk címzettje meggyőződhet az adatblokk hitelességéről és integritásáról;

s) „letöltés”:

a járműegység adatmemóriájában vagy a tachográfkártya memóriájában tárolt teljes adatkészletnek vagy annak egy részének a digitális aláírással együtt történő lemásolása azzal a feltétellel, hogy a tárolt adatok nem módosulnak és nem vesznek el.

A digitális menetíró készülékekbe szánt járműegységek gyártóinak, valamint az adatfájlok letöltésére tervezett és szánt berendezések gyártóinak minden ésszerű lépést meg kell tenniük annak érdekében, hogy az ilyen adatok letöltése a lehető legkisebb időveszteséget okozza a fuvarozási vállalkozások vagy járművezetők számára.

A részletes sebességadatok letöltése nem feltétlenül szükséges az 561/2006/EK rendeletnek való megfelelés megállapításához, hanem egyéb célokat szolgálhat, például balesetek kivizsgálását;

t) „járművezetői kártya”:

valamely tagállam hatóságai által egy adott járművezető részére kiállított tachográfkártya, amely azonosítja a járművezetőt, és lehetővé teszi a járművezető tevékenységére vonatkozó adatok tárolását;

u) „gumiabroncsok tényleges kerülete”:

azon távolságok átlaga, amelyet a járművet mozgató egyes kerekek (hajtókerekek) egy teljes fordulat során megtesznek. E távolságokat a 414. követelményben meghatározott rendes vizsgálati feltételek mellett kell lemérni, és „l = … mm” formában kell kifejezni. A járműgyártók e távolságmérést elméleti számítással is helyettesíthetik, amelynek során a terheletlen menetkész jármű tömegének tengelyek közötti eloszlásából indulnak ki ([1]). Az ilyen elméleti számításra vonatkozó módszerek csak akkor alkalmazhatók, ha azokat a tagállam illetékes hatósága jóváhagyja, és e számításokat még a menetíró készülék aktiválása előtt el kell végezni.

v) „esemény”:

az intelligens menetíró készülék által észlelt olyan rendellenes művelet, amely feltételezhetően csalási kísérlet eredménye;

w) „külső GNSS-eszköz”:

olyan eszköz, amely magában foglalja a GNSS-vevőt – abban az esetben, amikor a járműegység nem egyetlen egység –, valamint azokat a további alkatrészeket, amelyek a helyzetmeghatározási adatoknak a járműegység többi része felé való kommunikációjának védelmére szolgálnak;

([1]) A Bizottság 2012. december 12-i 1230/2012/EU rendelete a 661/2009/EK európai parlamenti és tanácsi rendeletnek a gépjárművek és azok pótkocsijainak tömegével és méreteivel kapcsolatos típus-jóváhagyási előírások tekintetében történő végrehajtásáról és a 2007/46/EK európai parlamenti és tanácsi irányelv módosításáról (HL L 353., 2012.12.21., 31. o.). a legutóbb módosított formájában.

▼B

x) „hiba”:

az intelligens menetíró készülék által észlelt olyan rendellenes művelet, amely feltételezhetően egy berendezés hibás működésének vagy meghibásodásának eredménye;

y) „GNSS-vevő”:

olyan elektronikus készülék, amely veszi és digitálisan feldolgozza egy vagy több globális navigációs műholdrendszer (angol rövidítéssel GNSS) jeleit a jármű helyzetére, sebességére és az időre vonatkozó információk rendelkezésre bocsátása érdekében;

z) „beépítés”:

a menetíró készülék beszerelése a járműbe;

aa) „interoperabilitás”:

a rendszerek és az alapjukat képező üzleti folyamatok adatcserére és információmegosztásra való képessége;

bb) „interfész”:

rendszerek közötti felület, amely az összekapcsolódást és interakciót lehetővé tévő közegként szolgál;

cc) „helyzet”:

a jármű földrajzi koordinátái egy adott pillanatban;

dd) „mozgásérzékelő”:

a menetíró készülék azon része, amely jelet bocsát ki a jármű sebességének és/vagy megtett távolságának jelzésére;

ee) „nem érvényes kártya”:

olyan kártya, amely hibásnak bizonyul, vagy amelynek a kezdeti hitelesítése nem sikerült, vagy amely nem érte még el érvényességi idejének kezdetét, illetve amelynek már lejárt az érvényességi ideje;

ff) „nyílt szabvány”:

olyan szabvány, amelynek leírása szerepel egy díjmentesen vagy névleges díj ellenében hozzáférhető dokumentumban, amelynek sokszorosítása, terjesztése vagy felhasználása díjmentesen vagy névleges díj ellenében engedélyezett;

gg) „menetíró készülék nem szükséges”:

az az eset, amikor az adatrögzítő készülék használata – az 561/2006/EGK rendelet előírásainak megfelelően – nem szükséges;

hh) „gyorshajtás”:

a jármű engedélyezett sebességének túllépése, amely definíció szerint az a 60 másodpercet meghaladó időszak, amely alatt a jármű mért sebessége meghaladja a 92/6/EGK tanácsi irányelv legutóbb módosított változatában [1] a sebességkorlátozó készülékek beállítására meghatározott legnagyobb értéket;

ii) „időszakos vizsgálat”:

annak ellenőrzésére végzett műveletek sorozata, hogy a menetíró készülék megfelelően működik, beállításai megfelelnek a jármű paramétereinek, és nem csatlakozik hozzá manipulációs eszköz;

[1] A Tanács 1992. február 10-i 92/6/EGK irányelve a Közösségben egyes gépjármű-kategóriákra sebességkorlátozó készülékek felszereléséről és használatáról (HL L 57., 1992.3.2., 27. o.).

▼B

jj) „nyomtató”:

az adatrögzítő készülék azon összetevője, amely biztosítja a tárolt adatok kinyomtatását;

kk) „korai távészleléssel történő kommunikáció”:

a korai távészleléssel történő kommunikációhoz használt eszköz és a korai távészleléssel történő kommunikációhoz használt leolvasó közötti kommunikáció célzott közúti ellenőrzések alatt, amelyeket az adatrögzítő készüléken végzett esetleges manipulációk és visszaélések korai távészlelésének céljára végeznek;

ll) „távoli kommunikációs eszköz”:

a járműegység azon berendezése, amelyet célzott közúti ellenőrzések végzésére használnak;

mm) „a korai távészleléssel történő kommunikációhoz használt leolvasó”:

az ellenőrző tisztviselők által a célzott közúti ellenőrzések során használt rendszer;

nn) „megújítás”:

egy új tachográfkártya kibocsátása abban az esetben, amikor a meglévő kártya érvényességi ideje lejárt, vagy a kártya meghibásodott, és a kibocsátó hatósághoz visszaküldték. Megújításkor mindenképpen meg kell győződni arról, hogy nem létezik-e egy időben két érvényes kártya;

oo) „javítás”:

egy mozgásérzékelő, egy járműegység vagy egy kábel bármely olyan javítása, amelyhez az áramellátás kiiktatása, a menetíró készülék más alkatrészektől történő elválasztása, illetve a mozgásérzékelő vagy a járműegység felnyitása szükséges;

pp) „kártyacsere”:

új kártya kibocsátása egy meglévő tachográfkártya pótlására, amelyről bejelentették, hogy elveszett, ellopták vagy meghibásodott, és nem küldték vissza a kibocsátó hatósághoz. A cserénél mindig felmerül annak kockázata, hogy egy időben két érvényes kártya létezik;

qq) „biztonsági tanúsítás”:

az az eljárás, melynek során egy Common Criteria szerinti tanúsító szerv tanúsítja, hogy a vizsgálandó adatrögzítő készülék (vagy annak valamely alkatrésze), illetve tachográfkártya megfelel az idevágó védelmi profilban meghatározott biztonsági követelményeknek;

rr) „önellenőrzés”:

az adatrögzítő készülék által a hibák észlelése érdekében ciklikusan és automatikusan végrehajtott tesztek;

ss) „időmérés”:

az egyeztetett világidő (UTC) folyamatos, digitális rögzítése;

tt) „időbeállítás”:

az aktuális idő automatikus, rendszeres időközönkénti, legfeljebb egy perccel való kiigazítása, illetve kalibrálás közben végzett beállítás;

uu) „abroncsméret”:

az abroncsok (külső hajtókerekek) méreteinek megjelölése a 92/23/EGK tanácsi irányelv ([1]) legutóbbi módosításának megfelelően;

([1]) A Tanács 1992. március 31-i 92/23/EGK irányelve a gépjárművek és pótkocsijaik gumiabroncsairól és azok felszereléséről (HL L 129., 1992.5.14., 95. o.).

▼B

vv) „jármű azonosítása”:

a jármű azonosítására szolgáló számok: a jármű rendszáma (VRN) a nyilvántartásba vétel szerinti tagállam megjelölésével, valamint a jármű jármű-azonosító száma (VIN) ([1]);

ww) az adatrögzítő készülékben történő számítást szolgáló „hét” szó:

a hétfő 00.00 óra UTC időponttól a vasárnap 24.00 óráig terjedő időszak;

xx) „műhelykártya”:

valamely tagállam által jóváhagyott menetírógyártó, -szerelő, járműgyártó vagy műhely kijelölt személyzete részére az adott tagállam hatóságai által kiadott tachográfkártya, amely azonosítja a kártyatulajdonost és lehetővé teszi a menetíró készülék tesztelését, kalibrálását, aktiválását és/vagy az arról való letöltést;

yy) „adapter”:

a jármű sebességének és/vagy megtett távolságának jelzésére folyamatosan jelet kibocsátó eszköz, amely nem tartozik a független mozgásérzékeléshez használt berendezések kategóriájába, és:

— kizárólag 2006. május 1. után üzembe helyezett (a 2007/46/EK európai parlamenti és tanácsi irányelv ([2]) legutóbb módosított változatának II. mellékletében található meghatározások szerinti) M1 és N1 kategóriájú járművekbe építik be,

— abban az esetben építik be, ha mechanikai okokból más típusú mozgásérzékelő nem építhető be, jóllehet az megfelel az ebben a mellékletben és e melléklet 1–15. függelékében foglalt előírásoknak,

— a járműegység és azon pont közé építik be, ahol az integrált érzékelők vagy alternatív interfészek a sebességre/megtett távolságra vonatkozó impulzusokat generálják,

— a járműegység szempontjából tekintve az adapter viselkedése ugyanolyan, mintha a járműegységre egy, az e mellékletben és e melléklet 1–16. függelékében foglalt előírásoknak megfelelő mozgásérzékelőt csatlakoztatnának.

Az ilyen adapternek a fent leírt járművekbe történő beépítésével lehetővé válik az e mellékletben foglalt valamennyi követelménynek megfelelő járműegység beépítése és megfelelő alkalmazása;

az ilyen járművek esetében az intelligens menetíró készüléknek a szükséges kábelek, az adapter és a járműegység is részét képezik;

([1]) A Tanács 1975. december 18-i 76/114/EGK irányelve a gépjárművek és pótkocsijaik hatóságilag előírt tábláira és feliratraira, valamint elhelyezésükre és rögzítési módjukra vonatkozó tagállami jogszabályok közelítéséről (HL L 24., 1976.1.30., 1. o.).

([2]) Az Európai Parlament és a Tanács 2007. szeptember 5-i 2007/46/EK irányelve a gépjárművek és pótkocsijaik, valamint az ilyen járművek rendszereinek, alkatrészeinek és önálló műszaki egységeinek jóváhagyásáról (keretirányelv) (HL L 263., 2007.10.9., 1. o.).

▼B

zz) „adatok integritása”:

a tárolt adatok pontossága és konzisztenciája, amely abban nyilvánul meg, hogy egy adatrekord két frissítése között nem mutatkozik különbség az adatokban. Az integritás azt jelenti, hogy az adatok az eredeti adatok pontos másolatai, azaz nem sérültek sem a tachográfkártyára vagy egy kijelölt berendezésre való írás és a kártyáról vagy a berendezésről való leolvasás, sem pedig az adatátvitel folyamata során, történjen az bármilyen kommunikációs csatornán;

aaa) „adatvédelem”:

azok az átfogó műszaki intézkedések, amelyeket a 95/46/EK európai parlamenti és tanácsi irányelvben ([1]), valamint a 2002/58/EK európai parlamenti és tanácsi irányelvben ([2]) megállapított elvek megfelelő végrehajtása érdekében alkalmaznak;

bbb) „intelligens menetíró rendszer”:

az adatrögzítő készülék, a tachográfkártyák, valamint e rendszerek kialakítása, beépítése, használata, tesztelése és ellenőrzése során minden közvetlenül vagy közvetve egymásra ható berendezés, mint például kártyák, a távoli kommunikációhoz használt leolvasó és az adatok letöltésére vagy elemzésére, illetve a biztonsági elemek kalibrálására, generálására, kezelésére vagy bevezetésére stb. szolgáló bármilyen egyéb berendezések;

ccc) „a bevezetés időpontja”:

36 hónappal a 165/2014/EU európai parlamenti és tanácsi rendelet ([3]) 11. cikkében említett részletes rendelkezések hatálybalépését követően.

Az a dátum, amelyet követően az első alkalommal nyilvántartásba vett járműveket/járműveknek:

— *fel kell szerelni műholdas navigációs rendszeren alapuló helyzetmeghatározási szolgáltatáshoz csatlakoztatott menetíró készülékkel,*

— *mozgás közben képesnek kell lenniük arra, hogy továbbítsák a célzott közúti ellenőrzésekhez szükséges adatokat az illetékes ellenőrző hatóságoknak,*

— *el lehet látni szabványosított interfészekkel, amelyek lehetővé teszik, hogy egy külső eszköz a menetíró készülékek által rögzített vagy előállított adatokat működési üzemmódban használni tudja;*

ddd) „védelmi profil”:

a Common Criteria szabvány szerinti tanúsítási folyamat során használt dokumentum, amely az információvédelemre vonatkozó biztonsági követelmények leírását tartalmazza, függetlenül a követelmények végrehajtásától;

([1]) Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.)

([2]) Az Európai Parlament és a Tanács 2002. július 12-i 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (HL L 201., 2002.7.31., 37. o.).

([3]) Az Európai Parlament és a Tanács 2014. február 4-i 165/2014/EU rendelete a közúti közlekedésben használt menetíró készülékekről, a közúti közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendelet hatályon kívül helyezéséről és a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról szóló 561/2006/EK európai parlamenti és tanácsi rendelet módosításáról (HL L 60., 2014.2.28., 1. o.).

▼B

eee) „a GNSS pontossága”:

a menetíró készülékek helyzetének globális navigációs műholdrendszerrel való feljegyzésének összefüggésében a vízszintes pontossághígulás (HDOP) értéke, amelyet a rendelkezésre álló GNSS-rendszer által begyűjtött HDOP-értékek minimumaként számítanak ki.

2 AZ ADATRÖGZÍTŐ KÉSZÜLÉK ÁLTALÁNOS JELLEMZŐI ÉS FUNKCIÓI

2.1 **Általános jellemzők**

Az adatrögzítő készülék rendeltetése, hogy rögzítse, tárolja, kijelezze és kinyomtassa a járművezető tevékenységére vonatkozó kimeneti adatokat.

Az e melléklet rendelkezéseinek megfelelő adatrögzítő készülékkel felszerelt minden járművön sebességkijelzőnek és kilométer-számlálónak is kell lennie. Az adatrögzítő készülék maga is tartalmazhatja e funkciókat.

(01) Az adatrögzítő készülék kábelekből, egy mozgásérzékelőből és egy járműegységből áll.

(02) A mozgásérzékelők és a járműegységek közötti interfésznek meg kell felelnie a 11. függelék követelményeinek.

(03) A járműegységnek a 12. függelék előírásai szerint globális navigációs műholdrendszer(ek)hez kell csatlakoznia.

(04) A járműegységnek a 14. függelék előírásai szerint kommunikálnia kell a korai távészleléssel történő kommunikációhoz használt leolvasókkal.

(05) A járműegység magában foglalhat egy, a 13. függelékben meghatározott ITS-interfészt.

Az adatrögzítő készüléket további interfészek és/vagy az opcionális ITS-interfész segítségével egyéb eszközökhöz is csatlakoztatni lehet.

(06) Amennyiben az adatrögzítő készülékbe pótlólagos berendezést vagy funkciót építenek be, illetve ahhoz ilyen berendezést kapcsolnak, ezek – függetlenül attól, hogy jóváhagyottak-e vagy sem – nem kelthetnek zavart az adatrögzítő készülék megfelelő és üzembiztos működésében, és elméletileg sem lehetnek alkalmasak erre, továbbá nem lehetnek ellentétesek e rendelet rendelkezéseivel.

Az adatrögzítő készülék használói tachográfkártyával azonosítják magukat.

(07) Az adatrögzítő készülék szelektív hozzáférési jogokat biztosít az adatokhoz és funkciókhoz a felhasználó típusa és/vagy személyazonossága szerint.

Az adatrögzítő készülék rögzíti, és a memóriájában, a távoli kommunikációt lehetővé tevő eszközön, valamint a tachográfkártyán tárolja az adatokat.

Ez a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK irányelvnek ([1]), az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK irányelvnek ([2]), valamint a 165/2014/EU rendelet 7. cikkének megfelelően történik.

([1]) HL L 281., 1995.11.23., 31. o.
([2]) HL L 201., 2002.7.31., 37. o.

▼B

2.2 **Funkciók**

(08) Az adatrögzítő készülék a következő funkciókat látja el:

— a kártyabehelyezések és -kivételek nyomon követése,

— sebesség-, távolság- és helyzetmérés,

— időmérés,

— a járművezető tevékenységének nyomon követése,

— a járművezetési állapot nyomon követése,

— a járművezetők által végzett kézi adatbevitel:

— azon helyek bevitele, ahol a munkanapok kezdődnek és/vagy végződnek,

— a járművezető tevékenységének kézi bevitele,

— különleges körülmények bevitele,

— vállalkozás általi lezárás kezelése,

— az ellenőrzési tevékenység nyomon követése,

— események és/vagy hibák észlelése,

— beépített és önellenőrző tesztek,

— az adatmemória leolvasása,

— rögzítés és tárolás az adatmemóriában,

— a tachográfkártya leolvasása,

— rögzítés és tárolás a tachográfkártyákon,

— kijelzés,

— nyomtatás,

— figyelmeztetés,

— adatletöltés külső adathordozókra,

— távoli kommunikáció a célzott közúti ellenőrzések céljára,

— kimenő adatok továbbítása kiegészítő készülékekre,

— kalibrálás,

— közúti kalibrálási ellenőrzés,

— időbeállítás.

2.3 **Üzemmódok**

(09) Az adatrögzítő készülék négy üzemmóddal rendelkezik:

— működési üzemmód,

— ellenőrzési üzemmód,

— kalibrálási üzemmód,

— vállalkozási üzemmód.

(10) Az adatrögzítő készüléknek a kártyainterfész-eszközbe behelyezett érvényes tachográfkártyáknak megfelelően az alábbi üzemmódokba kell kapcsolnia. Az üzemmód meghatározása szempontjából a tachográfkártya generációja lényegtelen, az a fontos, hogy a behelyezett kártya érvényes legyen. A második generációs járműegységbe helyezett első generációs műhelykártyát mindig érvénytelennek kell tekinteni.

▼B

Üzemmód		Járművezetői kártyaolvasó egység				
		Nincs kártya	Járművezetői kártya	Ellenőrzőkártya	Műhelykártya	Vállalkozáskártya
Járműkísérői kártyaolvasó egység	Nincs kártya	működési	működési	ellenőrzési	kalibrálási	vállalkozási
	Járművezetői kártya	működési	működési	ellenőrzési	kalibrálási	vállalkozási
	Ellenőrzőkártya	ellenőrzési	ellenőrzési	ellenőrzési (*)	működési	működési
	Műhelykártya	kalibrálási	kalibrálási	működési	kalibrálási (*)	működési
	Vállalkozáskártya	vállalkozási	vállalkozási	működési	működési	vállalkozási (*)

(*) Az ilyen helyzetekben az adatrögzítő készülék csak a járművezetői kártyaolvasó egységbe helyezett tachográfkártyát használhatja.

(11) A készülék a behelyezett nem érvényes kártyákat figyelmen kívül hagyja, azonban az adatok lejárt kártyáról való kijelzésének, kinyomtatásának vagy letöltésének lehetségesnek kell lennie.

(12) A 2.2. pontban felsorolt minden funkciónak minden üzemmódban működnie kell, az alábbi kivételekkel:

— a kalibrálási funkció csak a kalibrálási üzemmódban hozzáférhető,

— a közúti kalibrálási ellenőrzési funkció csak az ellenőrzési üzemmódban hozzáférhető,

— a vállalkozás általi lezárás kezelése funkció csak a vállalkozási üzemmódban hozzáférhető,

— az ellenőrzési tevékenységek nyomon követése funkció csak az ellenőrzési üzemmódban működik,

— a letöltési funkció a működési üzemmódban nem hozzáférhető (a 193. követelmény szerinti esetek kivételével), kivéve a járművezetői kártya adatainak letöltése során, amikor más kártya nincs behelyezve a járműegységbe.

(13) Az adatrögzítő készülék bármely adatot kiadhat kijelzésre, kinyomtatásra vagy külső interfészre a következő kivételekkel:

— a működési üzemmódban minden olyan személyazonosítót (családi név és utónév[nevek]), amely nem felel meg a behelyezett tachográfkártyának, ki kell takarni, és minden olyan kártyaszámot, amely nem felel meg a behelyezett tachográfkártyának, részlegesen ki kell iktatni (minden második karaktert – balról jobbra haladva – ki kell iktatni),

— a vállalkozási üzemmódban a járművezetőre vonatkozó adatok (102., 105. és 108. követelmény) csak olyan időszakokban jelezhetők ki, amikor nincs lezárás, illetve másik vállalkozás (amelyet a vállalkozáskártya számának első 13 karaktere azonosít) sem hajt végre lezárást,

— amennyiben nem helyeztek kártyát az adatrögzítő készülékbe, csak a járművezetővel kapcsolatos adatok jelezhetők ki az adott és az azt megelőző nyolc naptári napra vonatkozóan,

— a járműegységből származó személyes adatokat a járműegység ITS-interfésze csak abban az esetben adhatja ki, ha az a járművezető, akire az adatok vonatkoznak, hozzájárulását adta, és a hozzájárulást ellenőrizték,

▼B

— a járműegységek üzemeltetésének szokásos érvényességi ideje 15 év, mely időszak azon a napon kezdődik, amelyen a járműegység tanúsítványait kiállították, a járműegységeket azonban kizárólag adatletöltés céljára további 3 hónapig használni lehet.

2.4 **Biztonság**

A rendszerbiztonság célja az adatmemória következő módon történő védelme: az adatokhoz való jogosulatlan hozzáférés és az adatok manipulációjának megakadályozása és minden, erre irányuló kísérlet felderítése, a mozgásérzékelő és a járműegység között kicserélt adatok integritásának és hitelességének védelme, az adatrögzítő készülék és a tachográfkártyák között kicserélt adatok integritásának és hitelességének védelme, az adatrögzítő készülék és a külső GNSS-eszköz között kicserélt adatok integritásának és hitelességének védelme, csakúgy mint az ellenőrzés céljára végzett, korai távészleléssel történő kommunikáció során kicserélt adatok titkosságának, integritásának és hitelességének védelme, valamint a letöltött adatok integritásának és hitelességének védelme.

(14) A rendszerbiztonság elérése érdekében a következő alkatrészeknek meg kell felelniük a védelmi profiljukban meghatározott biztonsági követelményeknek, amint azt a 10. függelék előírja:

— járműegység,

— tachográfkártya,

— mozgásérzékelő,

— külső GNSS-eszköz (a védelmi profil csak a külső GNSS-változat esetében szükséges, és csak arra vonatkozik).

3 AZ ADATRÖGZÍTŐ KÉSZÜLÉK KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

3.1 **A kártyabehelyezések és -kivételek nyomon követése**

(15) Az adatrögzítő készülék ellenőrzi a kártyainterfész-eszközt, és felismeri a kártyabehelyezéseket és -kivételeket.

(16) A kártyabehelyezéskor az adatrögzítő készülék érzékeli, hogy a behelyezett kártya érvényes tachográfkártya-e, ha igen, akkor azonosítja a kártya típusát és generációját.

Ha az adatrögzítő készülékbe korábban egy ugyanolyan számú, de nagyobb megújítási indexű kártyát helyeztek, a kártyát érvénytelennek kell nyilvánítani.

Ha az adatrögzítő készülékbe korábban egy ugyanolyan számú és megújítási indexű, de nagyobb csereindexű kártyát helyeztek, a kártyát érvénytelennek kell nyilvánítani.

(17) Az adatrögzítő készüléknek a 15. függeléknek megfelelően (MIG003) az első generációs tachográfkártyákat érvénytelennek kell tekintenie, ha valamely műhely beszüntette az első generációs tachográfkártyák használatának lehetőségét.

(18) A második generációs adatrögzítő készülékbe helyezett első generációs műhelykártyákat érvénytelennek kell tekinteni.

▼B

(19) Az adatrögzítő készüléket úgy kell megtervezni, hogy a tachográfkártyák a kártyainterfész-eszközbe való megfelelő behelyezés esetén abban a helyzetben rögzüljenek.

(20) A tachográfkártya kioldása csak akkor lehetséges, ha a jármű álló helyzetben van, a megfelelő adatok a kártyán tárolásra kerültek, és a felhasználó egy szándékos, erre irányuló műveletet végez.

3.2 **Sebesség-, helyzet- és távolságmérés**

(21) A sebesség- és távolságmérési adatok fő forrása a mozgásérzékelő (az adapter részét is képezheti).

(22) E funkciónak a mozgásérzékelőtől jövő impulzusok alapján folyamatosan mérnie kell és meg kell adnia a jármű által megtett teljes távolságnak megfelelő kilométerszámláló-értéket.

(23) E funkciónak a mozgásérzékelőtől jövő impulzusok alapján folyamatosan mérnie kell és meg kell adnia a jármű sebességét.

(24) A sebességmérő funkció annak megállapítására is szolgál, hogy a jármű mozgásban van-e vagy megállt. A járművet mozgásban lévőnek kell tekinteni, amennyiben a funkció legalább 5 másodpercen keresztül a mozgásérzékelőből több mint 1 imp/sec értéket érzékel; ellenkező esetben a járművet állónak kell tekinteni.

(25) Azoknak a sebességet (kilométeróra) és a teljes megtett utat (kilométer-számláló) kijelző berendezéseknek, amelyeket az e rendelet rendelkezéseinek megfelelő adatrögzítő készülékkel felszerelt járműbe építettek be, meg kell felelniük az e mellékletben (3.2.1. és 3.2.2. pont) a megengedhető tűréshatárokkal kapcsolatban megállapított követelményeknek.

(26) A mozgásadatok manipulálásának kimutatásához a mozgásérzékelőből származó információkat meg kell erősíteni a jármű mozgására vonatkozó, a GNSS-vevőből és lehetőség szerint a mozgásérzékelőtől független egy vagy több további adatforrásból származó információkkal.

(27) E funkció a következő adatok automata rögzítése céljából méri a jármű helyzetét:

— azok a földrajzi helyek, ahol a járművezető és/vagy a járműkísérő megkezdi munkanapját,

— azok a földrajzi helyek, ahol a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét,

— azok a földrajzi helyek, ahol a járművezető és/vagy a járműkísérő befejezi munkanapját.

3.2.1 *A megtett távolság mérése*

(28) A megtett távolság mérése a következő célokat szolgálhatja:

— vagy az előre és a hátrafelé irányuló mozgások összegzése,

— vagy csak az előre irányuló mozgások figyelembevétele.

(29) Az adatrögzítő készüléknek a megtett távolságot 0 és 9 999 999,9 km között kell mérnie.

▼B

(30) A távolságmérésnek az alábbi tűréshatárokon belül kell maradnia (ha a megtett távolság legalább 1 000 m):

— ± 1 % beépítés előtt,

— ± 2 % beépítéskor és az időszakos vizsgálatok során;

— ± 4 % üzemeltetés közben.

(31) A távolságmérés pontosságának legalább 0,1 km-nek kell lennie.

3.2.2 *Sebességmérés*

(32) Az adatrögzítő készülék sebességmérési tartománya 0–220 km/h.

(33) Annak érdekében, hogy a kijelzett sebesség a ± 6 km/h megengedhető tűréshatáron belül maradjon üzemeltetés közben, valamint figyelembe véve a következőket:

— ± 2 km/h tűréshatár a bemeneti eltérésekre való tekintettel (eltérő gumiabroncsok stb.),

— ± 1 km/h tűréshatár a beépítés és az időszakos vizsgálatok során végzett méréseknél,

az adatrögzítő készüléknek 20 és 180 km/h közötti sebességnél és a jármű 4 000 és 25 000 imp/km közötti jellemző együtthatójánál ± 1 km/h tűréshatáron belül kell mérnie a sebességet (állandó sebességen).

Megjegyzés: Az adattárolási pontosság miatt további ±0,5 km/h tűréshatárral kell számolni az adatrögzítő készülék által tárolt sebességadatok tekintetében.

(34) A sebességmérés pontosságának egy adott – legfeljebb 2 m/s^2 ütemű – sebességváltozás végétől számított 2 másodpercen belül a szokásos tűréshatárokon belül kell maradnia.

(35) A sebességmérés pontosságának legalább 1 km/h-nak kell lennie.

3.2.3 *Helyzetmérés*

(36) Az adatrögzítő készüléknek a GNSS-vevő segítségével a jármű abszolút földrajzi helyzetét kell mérnie.

(37) Az abszolút földrajzi helyzetet a földrajzi szélesség és hosszúság koordinátáival kell mérni, fokokban és percekben kifejezve, 1/10 perc pontossággal.

3.3 **Időmérés**

(38) Az időmérő funkciónak folyamatosan mérnie kell és digitálisan meg kell adnia az UTC dátumot és időt.

(39) Az adatrögzítő készülékben a dátum megjelölésekor (adatrögzítések, adatcserék), valamint a 4. függelékben („Kinyomatok”) meghatározott valamennyi kinyomaton az UTC dátumot és időt kell feltüntetni.

(40) A helyi idő megjelenítése érdekében lehetővé kell tenni a kijelzett idő félórás lépésekben való megváltoztatását. A félórák negatív vagy pozitív többszörösén kívül minden egyéb átállítás tilos.

(41) Az időbeli eltérésnek típus-jóváhagyási körülmények között, időbeállítás nélkül a ± 2 másodperc/nap értéken belül kell maradnia.

▼B

(42) Az időmérés pontosságának legalább 1 másodpercnek kell lennie.

(43) Az időmérésre típus-jóváhagyási körülmények között egy 12 hónapnál rövidebb külső áramkimaradás nem lehet hatással.

3.4 **A járművezető tevékenységének nyomon követése**

(44) E funkciónak állandóan és külön-külön nyomon kell követnie egy járművezető és egy járműkísérő tevékenységét.

(45) A járművezető tevékenységei: JÁRMŰVEZETÉS, MUNKA, KÉSZENLÉT vagy SZÜNET/PIHENÉS.

(46) A járművezető és/vagy a járműkísérő számára lehetővé kell tenni, hogy manuálisan válassza ki a MUNKÁT, KÉSZENLÉTET vagy a SZÜNETET/PIHENÉST.

(47) Ha a jármű mozgásban van, a készüléknek a járművezető esetében automatikusan a JÁRMŰVEZETÉST kell kiválasztania, a járműkísérő esetében pedig automatikusan a KÉSZENLÉTET.

(48) Amikor a jármű megáll, a készüléknek automatikusan a MUNKÁT kell kiválasztania a járművezető esetében.

(49) Úgy kell tekintetni, hogy az első, SZÜNETRE/PIHENÉSRE vagy KÉSZENLÉTRE történő tevékenységváltás, amely 120 másodpercen belül azután következett be, hogy a jármű megállása következtében automatikus váltás történt a MUNKÁRA, a jármű leállásakor következett be (és ezért a MUNKÁRA való átváltást adott esetben törölni kell).

(50) E funkciónak egyperces pontossággal kell jeleznie a tevékenységváltozást az adatrögzítő funkciók felé.

(51) Ha egy naptári percet közvetlenül megelőző és a percet közvetlenül követő egy percen belül bármiféle JÁRMŰVEZETÉSI tevékenység feljegyzésre kerül, akkor az egész percet JÁRMŰVEZETÉSNEK kell tekinteni.

(52) Ha egy naptári perc az előbbi 051. követelmény alapján nem tekinthető JÁRMŰVEZETÉSNEK, az egész percet az adott percen belüli leghosszabb folyamatos tevékenységnek megfelelő tevékenységnek kell tekinteni (azonos hosszúságú tevékenységek esetében pedig a későbbi tevékenységnek).

(53) E funkciónak emellett állandóan nyomon kell követnie a járművezető megszakítás nélküli járművezetési idejét és halmozott pihenőidejét.

3.5 **A járművezetési állapot nyomon követése**

(54) E funkciónak állandóan és automatikusan nyomon kell követnie a járművezetési állapotot.

(55) A SZEMÉLYZET járművezetési állapot kerül kiválasztásra, amikor két érvényes járművezetői kártya kerül behelyezésre a berendezésbe, minden egyéb esetben pedig az EGYEDÜLI járművezetési állapot.

3.6 **Adatbevitel a járművezetők által**

3.6.1 *Azon helyek bevitele, ahol a munkanapok kezdődnek és/vagy végződnek*

(56) E funkció azon helyek bevitelére szolgál, ahol a járművezető és/vagy a járműkísérő szerint az adott munkanap elkezdődött és/vagy végződött.

▼B

(57) Hely alatt az országot, és ahol emellett szükséges, a régiót kell érteni, melyeket kézzel visznek be, illetve erősítenek meg a rendszerben.

(58) A járművezetői kártya kivételének időpontjában az adatrögzítő készüléknek emlékeztetnie kell a járművezetőt (vagy a járműkísérőt) arra, hogy rögzítse azt a helyet, ahol a munkanap végződött.

(59) Erre a járművezetőnek, egyelőre ideiglenes adatbevitelként, fel kell jegyeznie a jármű aktuális helyét.

(60) Azon helyek bevitelének, ahol a munkanap kezdődik és/vagy végződik, a menüben szereplő parancsok segítségével lehetségesnek kell lennie. Ha egy naptári percen belül több ilyen bevitelre kerül sor, akkor a munkanap kezdetének és befejezésének csak az ezen időn belül legutoljára bevitt helye kerül rögzítésre.

3.6.2 *A járművezető tevékenységével kapcsolatos adatok és a járművezető ITS-interfésszel kapcsolatos hozzájárulásának kézi bevitele*

(61) A járművezetői (vagy műhely-) kártya behelyezésekor, és csak ezen időpontban, az adatrögzítő készüléknek lehetővé kell tennie a tevékenységekkel kapcsolatos adatok kézi bevitelét. A tevékenységek kézi bevitelét a járműegység esetében aktuálisan meghatározott helyi időt és időzóna-paramétereket (UTC-től való eltérés) megadva kell elvégezni.

A járművezetői (vagy műhely-) kártya behelyezésekor az adatrögzítő készüléknek a következőkre kell emlékeztetnie a kártya tulajdonosát:

— az utolsó kártyakivétel dátuma és időpontja,

— opcionálisan: a járműegység esetében aktuálisan meghatározott helyi idő.

A járműegység számára az adott pillanatban ismeretlen járművezetői kártya vagy műhelykártya első behelyezésekor a készülék arra kéri a kártya tulajdonosát, hogy járuljon hozzá a menetíró készülékkel kapcsolatos személyes adatainak az opcionális ITS-interfészen keresztüli továbbításához.

A járművezető (illetve a műhely) hozzájárulása bármikor aktiválható vagy kikapcsolható a menüben szereplő parancsok segítségével, ha a járművezetői (illetve műhely-) kártya be van helyezve.

A tevékenységek a következő korlátozások mellett vihetők be:

— a tevékenységtípus csak MUNKA, KÉSZENLÉT vagy SZÜNET/PIHENÉS lehet,

— minden egyes tevékenység kezdési és befejezési időpontjának az utolsó kártyakivétel és az aktuális kártyabehelyezés közti időszakba kell esnie,

— a tevékenységek között nem lehet időbeli átfedés.

Szükség esetén lehetővé kell tenni a kézi bevitelt a korábban nem használt járművezetői (vagy műhely-) kártya első behelyezésekor.

▼B

A tevékenységek kézi bevitelének eljárása annyi egymást követő lépést foglal magában, amennyi az egyes tevékenységek típusának, kezdési és befejezési időpontjának meghatározásához szükséges. A kártyatulajdonos az utolsó kártyakivétel és az aktuális kártyabehelyezés közötti időszak bármely részét illetően választhatja azt a lehetőséget, hogy nem jelent be tevékenységet.

A kártyatulajdonos számára lehetőséget kell biztosítani arra, hogy a kártyabehelyezéssel kapcsolatos kézi adatbevitel során – adott esetben – rögzítse a következő adatokat:

— az előző munkanap befejezésének helye, a megfelelő időponthoz kapcsolva (felülírva akár a legutóbbi kártyakivételnél bevitt adatot),

— az aktuális munkanap kezdetének helye, a megfelelő időponthoz kapcsolva.

Ha a kártyatulajdonos nem rögzít semmit a munkanap kezdetének vagy végének helye gyanánt a kártyabehelyezéskor lehetséges kézi adatbevitel során, akkor úgy kell tekinteni, mintha nyilatkozatot tett volna arról, hogy munkanapja nem változott az utolsó kártyakivétel óta. Amikor a következő alkalommal rögzítik a helyet a munkanap végén, az az adatbevitel felülírja a legutóbbi kártyakivétel során ideiglenesen bevitt adatokat.

Helyre vonatkozó adatok bevitele során azok a megfelelő tachográfkártyában rögzítésre kerülnek.

A kézi adatbevitel megszakad, ha:

— kiveszik a kártyát, vagy

— a jármű mozgásban van, és a kártya be van helyezve a járművezetői kártyaolvasó egységbe.

További megszakítás is megengedett, például ha a felhasználói bizonyos ideig inaktív volt, azt szünet követheti. Amennyiben a kézi bevitel félbeszakad, az adatrögzítő készüléknek meg kell erősítenie minden, a hellyel és a tevékenységgel kapcsolatban már hiánytalanul bevitt adatot (egyértelműen meghatározott hely és idő, illetve egyértelműen meghatározott tevékenységtípus, kezdési és befejezési idővel).

Amennyiben egy második járművezetői vagy műhelykártya behelyezésére kerül sor, miközben az előzőleg behelyezett kártyára irányuló kézi adatbevitel még folyamatban van, hagyni kell az előzőleg behelyezett kártyára történő kézi bevitel befejezését, mielőtt a második kártyára történő kézi bevitel megkezdődik.

A kártyatulajdonos számára lehetővé kell tenni, hogy a kézi adatbevitelt a következő minimumeljárásnak megfelelően végezhesse:

— Időrendi sorrendben kézzel viszi be a tevékenységeket az utolsó kártyakivétel és az aktuális behelyezés közötti időszakra vonatkozóan.

— Az első tevékenység időpontját a kártyakivétel időpontjához kell igazítani. Minden ezt követő adatbevitel kezdési időpontját úgy kell előre beállítani, hogy közvetlenül az előző bevitel befejezési időpontjára következzen. Minden egyes tevékenység esetében ki kell választani a tevékenységtípust és befejezési időt.

▼B

Az eljárás akkor fejeződik be, amikor a kézzel bevitt tevékenység befejezésének ideje azonos a kártyabehelyezés idejével. Az adatrögzítő készülék ezután még megengedheti, hogy a kártya tulajdonosa a kézzel bevitt tevékenységeket módosíthassa, mindaddig, amíg egy meghatározott parancs megadásával végérvényesen meg nem erősíti az adatokat. Ezután már semmilyen módosítás sem lehetséges.

3.6.3 *Különleges körülmények bevitele*

(62) Az adatrögzítő készülék lehetővé kell, hogy tegye a járművezető számára, hogy az alábbi két különleges körülményt valós időben vigye be:

— „MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES” (kezdet, vég)

— „KOMPON/VONATON MEGTETT ÚT” (kezdet, vég).

A „KOMPON/VONATON MEGTETT ÚT” nem fordulhat elő „MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES” körülmény esetén.

A megnyitott „MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES” körülményt az adatrögzítő készülék automatikusan bezárja járművezetői kártya behelyezése vagy kivétele esetén.

A megnyitott „MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES” körülmény letiltja a következő eseményeket és figyelmeztetéseket:

— járművezetés megfelelő kártya nélkül,

— a megszakítás nélküli járművezetési idővel kapcsolatos figyelmeztetések.

A „KOMPON/VONATON MEGTETT ÚT” kezdetét már azelőtt jelezni kell a rendszerben, hogy a járművezető leállítja a motort a kompon vagy a vonaton.

A megnyitott „KOMPON/VONATON MEGTETT ÚT” körülménynek véget kell érnie az alábbi lehetőségek bármelyike esetén:

— a járművezető kézzel befejezi a „KOMPON/VONATON MEGTETT ÚT” körülményt,

— a járművezető kiveszi a kártyáját.

A megnyitott „KOMPON/VONATON MEGTETT ÚT” körülménynek véget kell érnie, ha az 561/2006/EK rendeletben megállapított szabályok alapján megszűnik érvényessége.

3.7 **A vállalkozások általi lezárások kezelése**

(63) E funkció a vállalkozások általi lezárások kezelésében áll, amelyeket a vállalkozások azért végeznek, hogy vállalkozási üzemmódban csak ők maguk férhessenek hozzá az adataikhoz.

(64) A vállalkozások általi lezárások egy kezdő dátumból/időpontból (lezárás) és egy befejező dátumból/időpontból (feloldás) állnak, hozzárendelve a vállalkozáskártya (lezárási művelet során kijelzett) számával azonosított megfelelő vállalkozáshoz.

(65) A lezárásokat és a feloldásokat csak valós időben lehet végrehajtani.

(66) A feloldást csak ugyanaz a vállalkozás hajthatja végre, mint a lezárást (ezt a vállalkozáskártya számának első 13 számjegye tanúsítja), vagy

(67) a feloldás automatikusan megtörténik, amint egy másik vállalkozás lezárást hajt végre.

▼B

(68) Amennyiben egy vállalkozás lezárást hajt végre, és az előző lezárást is ugyanaz a vállalkozás végezte, ezt úgy kell tekinteni, hogy az előző lezárást nem oldották fel, és a lezárás még mindig tart.

3.8 **Az ellenőrzési tevékenység nyomon követése**

(69) E funkció a KIJELZÉSI, a KINYOMTATÁSI, a JÁRMŰEGYSÉGRŐL és a kártyáról való LETÖLTÉS, valamint KÖZÚTI KALIBRÁCIÓ tevékenységek nyomon követésére szolgál az ellenőrzési üzemmódban.

(70) E funkciónak a GYORSHAJTÁS ELLENŐRZÉSE tevékenységek nyomon követésére is ki kell terjednie az ellenőrzés üzemmódban. A gyorshajtás ellenőrzését megtörténtnek kell tekinteni, amennyiben ellenőrzési üzemmódban a „gyorshajtás” kinyomat a nyomtatóba vagy a kijelzőbe elküldésre került, vagy ha az „események és hibák” adatokat letöltötték a járműegység adatmemóriájából.

3.9 **Események és/vagy hibák észlelése**

(71) E funkció az alábbi események és/vagy hibák észlelésére szolgál:

3.9.1 *„Érvénytelen kártya behelyezése”*

(72) Ezt az eseményt az idézi elő, ha bármilyen érvénytelen kártyát, már lecserélt járművezetői kártyát és/vagy egy lejárt érvényességi idejű, de egyébként érvényes kártyát helyeznek a készülékbe.

3.9.2 *„Kártyaütközés”*

(73) Ezt az eseményt az idézi elő, amikor az érvényes kártyáknak a következő táblázatban X-szel jelölt alábbi kombinációja valósul meg:

Kártyaütközés		Járművezetői kártyaolvasó egység				
		Nincs kártya	Járművezetői kártya	Ellenőrzőkártya	Műhelykártya	Vállalkozáskártya
Járműkísérői kártyaolvasó egység	Nincs kártya					
	Járművezetői kártya				X	
	Ellenőrzőkártya			X	X	X
	Műhelykártya		X	X	X	X
	Vállalkozáskártya			X	X	X

3.9.3 *„Időátfedés”*

(74) Ezt az eseményt az idézi elő, amikor egy járművezetői kártyáról leolvasható utolsó kártyakivétel dátuma/időpontja későbbi, mint az azon adatrögzítő készülék által kijelzett aktuális dátum/időpont, amelybe a kártyát behelyezték.

3.9.4 *„Járművezetés megfelelő kártya nélkül”*

(75) Ezt az eseményt bármely érvényes tachográfkártya alábbi táblázatban X-szel jelölt kombinációja idézi elő, amikor a járművezető tevékenysége JÁRMŰVEZETÉS-re változik, vagy JÁRMŰVEZETÉS tevékenység közben változik az üzemmód.

▼B

Járművezetés megfelelő kártya nélkül		Járművezetői kártyaolvasó egység				
		Nincs (vagy érvénytelen) kártya	Járművezetői kártya	Ellenőrzőkártya	Műhelykártya	Vállalkozáskártya
Járműkísérői kártyaolvasó egység	Nincs (vagy érvénytelen) kártya	X		X		X
	Járművezetői kártya	X		X	X	X
	Ellenőrzőkártya	X	X	X	X	X
	Műhelykártya	X	X	X		X
	Vállalkozáskártya	X	X	X	X	X

3.9.5 *„Kártya behelyezése járművezetés közben”*

(76) Ezt az eseményt az idézi elő, amikor valamelyik tachográfkártyát behelyezik a kártyaolvasó egységbe, mialatt a járművezető tevékenysége JÁRMŰVEZETÉS.

3.9.6 *„Utolsó kártyakapcsolat nem megfelelő lezárása”*

(77) Ezt az eseményt az idézi elő, amikor egy kártyabehelyezésnél az adatrögzítő készülék megállapítja, hogy a 3.1. szakaszban foglaltak ellenére az előző kártyakapcsolat nem került helyesen lezárásra (a kártyát kivették, mielőtt a megfelelő adatok tárolásra kerültek volna a kártyán). Ezt az eseményt csak a járművezetői kártya és a műhelykártya válthatja ki.

3.9.7 *„Gyorshajtás”*

(78) Ezt az eseményt minden egyes gyorshajtás kiváltja.

3.9.8 *„Áramellátás megszakadása”*

(79) Ezt az eseményt az idézi elő, amikor – kalibrálási vagy ellenőrzési üzemmódon kívül – a mozgásérzékelő és/vagy a járműegység áramkimaradása meghaladja a 200 milliszekundumot. A megszakadási küszöbértéket a gyártó cégnek kell meghatározni. A jármű motorjának beindításából eredő áramellátás-csökkenés nem válthatja ki ezt az eseményt.

3.9.9. *„Kommunikációs hiba a távoli kommunikációs eszközzel”*

(80) Ezt az eseményt az idézi elő, amikor – **kalibrálási üzemmódon kívül** – a távoli kommunikációs eszköz több mint harmadszori próbálkozásra sem igazolja a járműegységből származó távoli kommunikációs adatok sikeres vételét.

3.9.10. *„A GNSS-vevőből származó helyzetmeghatározási információk hiánya”*

(81) Ezt az eseményt az idézi elő, amikor – **kalibrálási üzemmódon kívül** – a halmozott járművezetési időből eltelő több mint három órán keresztül nem jönnek helyzetmeghatározási információk a (belső vagy külső) GNSS-vevőből.

3.9.11. *„Kommunikációs hiba a külső GNSS-eszközzel”*

(82) Ezt az eseményt az idézi elő, amikor – **kalibrálási üzemmódon kívül** – a jármű mozgása közben több mint 20 folyamatos percen keresztül nem működik a kommunikáció a külső GNSS-eszköz és a járműegység között.

▼B

3.9.12. *A „mozgásadatok hibája”*

(83) Ezt az eseményt az idézi elő, amikor – **kalibrálási üzemmódon kívül** – megszakad a normál adatfolyam a mozgásérzékelő és a járműegység között, és/vagy hiba lép fel az adatintegritásban vagy adathitelesítésben a mozgásérzékelő és a járműegység közötti adatcsere alatt.

3.9.13 *„A jármű mozgásával kapcsolatos ellentmondás”*

(84) Ezt az eseményt az idézi elő, amikor – **kalibrálási üzemmódon kívül** – a mozgásérzékelő adatai alapján a jármű mozgására vonatkozóan kiszámított információk ellentmondanak a belső GNSS-vevőből vagy a külső GNSS-eszközből és lehetőség szerint egy vagy több további független, a 12. függelékben meghatározott adatforrásból származó adatok alapján kiszámított információknak. Ezt az eseményt sem a kompon/vonaton megtett út, sem a MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES körülmény, sem pedig a GNSS-vevőkből származó helyzetmeghatározási információk hiánya nem válthatja ki.

3.9.14. *A „biztonsági rendszer megsértésére irányuló kísérlet”*

(85) Ezt az eseményt minden olyan további, a mozgásérzékelő és/vagy a járműegység és/vagy a külső GNSS-eszköz 10. függelékben előírt biztonságát érintő esemény idézi elő, amely a kalibrálási üzemmódon kívül következik be.

3.9.15. *„Időütközés”*

(86) Ezt az eseményt az idézi elő, amikor a járműegység – **a kalibrálási üzemmódon kívül** – 1 percet meghaladó eltérést észlel a járműegység időmérő funkciója által kijelzett idő és a GNSS-vevőből származó időadatok között. Ez az esemény a járműegység belső időmérőjének értékével együtt rögzítésre kerül, és automatikus időbeállítást eredményez. Valamely „időütközés” esemény kiváltását követően a járműegység a következő 12 órában nem fog újabb „időütközés” eseményt generálni. Ez az esemény akkor nem idéződhet elő, ha a GNSS-vevő az utolsó 30 nap során nem észlelt érvényes GNSS-jelet. Amint azonban a GNSS-vevő ismét helyzetmeghatározási információkat szolgáltat, az automatikus időbeállításnak meg kell történnie.

3.9.16. *Kártyahiba*

(87) E hibát a tachográfkártya működés közben bekövetkező meghibásodása idézi elő.

3.9.17. *Az „adatrögzítő készülék” hibája*

(88) Ezt a hibát a kalibrálási üzemmódon kívül bekövetkező bármely alábbi meghibásodásnak elő kell idéznie:

— a járműegység belső hibája

— nyomtatóhiba

— kijelzőhiba

— letöltési hiba

— érzékelőhiba

— a GNSS-vevő vagy a külső GNSS-eszköz hibája

— a távoli kommunikációs eszköz hibája

▼B

3.10 **Beépített és önellenőrző tesztek**

(89) Az adatrögzítő készüléknek önellenőrző és beépített tesztek segítségével magától fel kell derítenie a hibákat az alábbi táblázat szerint:

Vizsgálandó készülékrész	Önellenőrzés	Beépített teszt
Szoftver		Integritás
Adatmemória	Hozzáférés	Hozzáférés, adatintegritás
Kártyainterfész-eszközök	Hozzáférés	Hozzáférés
Billentyűzet		Kézi ellenőrzés
Nyomtató	(A gyártótól függ)	Kinyomat
Kijelző		Szemrevételezés
Letöltés (végrehajtva csak a letöltés alatt)	Megfelelő működés	
Érzékelő	Megfelelő működés	Megfelelő működés
Távoli kommunikációs eszköz	Megfelelő működés	Megfelelő működés
GNSS-eszköz	Megfelelő működés	Megfelelő működés

3.11 **Az adatmemória leolvasása**

(90) Az adatrögzítő készüléknek képesnek kell lennie az adatmemóriájában tárolt minden adat leolvasására.

3.12 **Rögzítés és tárolás az adatmemóriában**

E szakasz alkalmazásában:

— „365 nap”: 365 naptári nap, amely időszakot egy járműben végzett átlagos járművezetői tevékenység jellemez. Egy járműben végzett átlagos napi járművezetői tevékenység a meghatározás szerint a következő: legalább hat járművezető, illetve járműkísérő, hat kártyabehelyezési és -kivételi ciklus és 256 tevékenységváltoztatás. Ezért a „365 nap” legalább 2 190 járművezetőt vagy járműkísérőt, 2 190 kártyabehelyezési és -kivételi ciklust, valamint 93 440 tevékenységváltoztatást foglal magában.

— A földrajzi helyek napi átlagos száma a meghatározás szerint a következő: 6 olyan hely, ahol a munkanap kezdődött, 6 olyan hely, ahol a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét, 6 olyan hely, ahol a munkanap befejeződik, tehát a „365 nap” legalább 6 570 helyet magában foglal.

— Eltérő utasítások hiányában az időt egyperces pontossággal kell rögzíteni.

— A kilométer-számláló értékeit egy kilométeres pontossággal kell rögzíteni.

— A sebességadatokat 1 km/h pontossággal kell rögzíteni.

— A földrajzi helyzetet (szélesség és hosszúság) fokban és percekben kell megadni, 1/10 perc pontossággal, a kapcsolódó GNSS-pontosságot és az adatfelvétel idejét is megadva.

▼B

(91) Az adatmemóriában tárolt adatokra típus-jóváhagyási körülmények között egy 12 hónapnál rövidebb külső áramkimaradás nem lehet hatással. Emellett a 14. függelék szerinti külső távoli kommunikációs eszközben tárolt adatokra egy 28 napnál rövidebb külső áramkimaradás nem lehet hatással.

(92) Az adatrögzítő készüléknek képesnek kell lennie arra, hogy implicit vagy explicit módon rögzítse és tárolja adatmemóriájában az alábbiakat:

3.12.1 *Készülékazonosítási adatok*

3.12.1.1 Járműegység-azonosítási adatok

(93) Az adatrögzítő készüléknek tárolnia kell adatmemóriájában az alábbi járműegység-azonosítási adatokat:

— a gyártó neve,

— a gyártó címe,

— alkatrészszám,

— sorozatszám,

— a járműegység generációja,

— képes-e a járműegység első generációs tachográfkártyák használatára,

— szoftververzió száma,

— szoftververzió telepítésének dátuma,

— gyártási év,

— jóváhagyási szám.

(94) A járműegység-azonosítási adatokat a járműegység gyártója rögzíti és véglegesen tárolja, kivéve a szoftverre vonatkozó adatokat és a jóváhagyási számot, amelyek a szoftver frissítése esetén változhatnak, valamint az első generációs tachográfkártyák használatára irányuló képességet.

3.12.1.2 A mozgásérzékelő azonosítási adatai

(95) A mozgásérzékelőnek tárolnia kell memóriájában az alábbi azonosítási adatokat:

— a gyártó neve,

— sorozatszám,

— jóváhagyási szám,

— a beépített biztonsági alkatrész azonosítója (például a belső chip/processzor alkatrészszáma),

— operációs rendszer azonosítója (például a szoftververzió száma).

(96) A mozgásérzékelő azonosítási adatait a mozgásérzékelő gyártója rögzíti és tárolja véglegesen a mozgásérzékelőben.

(97) A járműegységnek képesnek kell lennie arra, hogy adatmemóriájában rögzítse és tárolja a 20 legutóbbi mozgásérzékelő-párosítással kapcsolatos következő adatokat (ha ugyanazon a naptári napon több párosítás történt, csak az aznapi elsőt és utolsót kell tárolni):

▼B

Az egyes párosításokra vonatkozóan a következő adatokat kell rögzíteni:

— a mozgásérzékelő azonosítási adatai:

— sorozatszám

— jóváhagyási szám

— a mozgásérzékelő párosítási adatai:

— a párosítás dátuma.

3.12.1.3 A globális navigációs műholdrendszerek azonosítási adatai

(98) A külső GNSS-eszköznek tárolnia kell memóriájában az alábbi azonosítási adatokat:

— a gyártó neve,

— sorozatszám,

— jóváhagyási szám,

— a beépített biztonsági alkatrész azonosítója (például a belső chip/processzor alkatrészszáma),

— operációs rendszer azonosítója (például a szoftververzió száma).

(99) A külső GNSS-eszköz azonosítási adatait az eszköz gyártója rögzíti és tárolja véglegesen a külső GNSS-eszközben.

(100) A járműegységnek képesnek kell lennie arra, hogy adatmemóriájában rögzítse és tárolja a külső GNSS-eszközök 20 legutóbbi rákapcsolódásával kapcsolatos következő adatokat (ha ugyanazon a naptári napon több rákapcsolódás történt, csak az aznapi elsőt és utolsót kell tárolni).

Az egyes rákapcsolódásokra vonatkozóan a következő adatokat kell rögzíteni:

— a külső GNSS-eszköz azonosítási adatai:

— sorozatszám,

— jóváhagyási szám,

— a külső GNSS-eszköz rákapcsolódási adatai:

— a rákapcsolódás dátuma.

3.12.2 *Kulcsok és tanúsítványok*

(101) Az adatrögzítő készüléknek képesnek kell lennie egy sor, a 11. függelék A. és B. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

3.12.3 *A járművezetői vagy műhelykártya behelyezési és kivételi adatai*

(102) Az adatrögzítő készüléknek a járművezetői kártya és a műhelykártya minden egyes behelyezési és kivételi ciklusánál az alábbi adatokat rögzítenie és tárolnia kell adatmemóriájában:

— a kártyatulajdonos családi neve és utóneve(i) a kártyán tárolt formában,

— a kártya száma, kiállító tagállama és érvényességének ideje a kártyán tárolt formában,

— a kártya generációja,

▼B

— a behelyezés dátuma és időpontja,

— a jármű kilométer-számlálójának értéke kártyabehelyezéskor,

— azon kártyaolvasó egység, amelybe a kártyát behelyezték,

— a kivétel dátuma és időpontja,

— a jármű kilométer-számlálójának értéke kártyakivételkor,

— a járművezető által használt előző járművel kapcsolatos alábbi információk, a kártyán tárolt formában:

— a jármű rendszáma (VRN) és a nyilvántartásba vétel szerinti tagállam,

— a járműegység generációja (ha ismert),

— a kártyakivétel dátuma és időpontja,

— jelző, amely megmutatja, hogy a kártyabehelyezésnél a kártyatulajdonos kézzel vitt-e be tevékenységeket vagy sem.

(103) Az adatmemóriának legalább 365 napig meg kell őriznie ezen adatokat.

(104) Amennyiben a tárolóhely megtelik, az új adatok felülírják a régebbieket.

3.12.4 *A járművezető tevékenységére vonatkozó adatok*

(105) Az adatrögzítő készüléknek rögzítenie és adatmemóriájában tárolnia kell a járművezető és/vagy a járműkísérő tevékenységében és/vagy a járművezetési állapotban bekövetkező bármilyen változás esetén és/vagy a járművezetői vagy a műhelykártya valamennyi behelyezésekor vagy kivételekor a következőket:

— a járművezetési állapot (SZEMÉLYZET, EGYEDÜLI),

— a kártyaolvasó egység (JÁRMŰVEZETŐI, JÁRMŰKÍSÉRŐI),

— a kártyaállapot a megfelelő kártyaolvasó egységben (BEHELYEZVE, NINCS BEHELYEZVE),

— a tevékenység (JÁRMŰVEZETÉS, KÉSZENLÉT, MUNKA, SZÜNET/PIHENÉS),

— a változás dátuma és időpontja.

A BEHELYEZVE szó azt jelenti, hogy a kártyaolvasó egységbe érvényes járművezetői vagy műhelykártyát helyeztek be. A NINCS BEHELYEZVE szó ennek az ellenkezőjét jelenti, vagyis hogy érvénytelen járművezetői vagy műhelykártyát helyeztek be a kártyaolvasó egységbe (például vállalkozáskártyát, vagy egyáltalán nem került sor kártya behelyezésére).

A járművezető által kézzel bevitt tevékenységi adatokat az adatmemória nem rögzíti.

(106) Az adatmemóriának legalább 365 napig meg kell őriznie a járművezető tevékenységére vonatkozó adatokat.

(107) Amennyiben a tárolóhely megtelik, az új adatok felülírják a régebbieket.

▼B

3.12.5 *Azok a helyek (helységnév és földrajzi hely), ahol a munkanapok kezdődnek, végződnek és/vagy ahol a megszakítás nélküli járművezetési idő eléri a három óra többszörösét*

(108) Az adatrögzítő készüléknek az alábbi adatokat rögzítenie és tárolnia kell adatmemóriájában:

— azok a helyek (helységnév és földrajzi hely), ahol a járművezető és/vagy a járműkísérő megkezdi munkanapját,

— azok a helyek (helységnév és földrajzi hely), ahol a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét,

— azok a helyek (helységnév és földrajzi hely), ahol a járművezető és/vagy a járműkísérő befejezi munkanapját.

(109) Amennyiben ezekben az időpontokban a GNSS-vevők nem adnak információt a jármű helyzetéről, az adatrögzítő készüléknek a legutolsó rendelkezésre álló helyzetmeghatározási adatot kell használnia, a kapcsolódó dátummal és időponttal.

(110) Az adatrögzítő készüléknek minden egyes hellyel (helységnév és földrajzi hely) együtt az alábbi adatokat rögzítenie és tárolnia kell adatmemóriájában:

— a járművezetői vagy járműkísérői kártya száma és a kártyát kiállító tagállam,

— a kártya generációja,

— az adatbevitel dátuma és időpontja,

— a bevitt adat típusa (a munkanap kezdete, vége vagy 3 óra megszakítás nélküli járművezetési idő),

— a kapcsolódó GNSS-pontosság, valamint adott esetben a dátum és az időpont,

— a jármű kilométer-számlálójának értéke.

(111) Az adatmemóriának képesnek kell lennie arra, hogy legalább 365 napon át megőrizze azokat a helyeket (helységnév és földrajzi hely), ahol a munkanapok kezdődtek, végződtek, és/vagy a megszakítás nélküli járművezetési idő elérte a három órát.

(112) Amennyiben a tárolóhely megtelik, az új adatok felülírják a régebbieket.

3.12.6 *A kilométer-számláló adatai*

(113) Az adatrögzítő készüléknek a jármű kilométer-számlálójának értékét és az ezzel összefüggő dátumot minden naptári napon éjfélkor rögzíteni kell adatmemóriájában.

(114) Az adatmemóriának legalább 365 naptári napig tárolnia kell a kilométer-számláló éjféli értékeit.

(115) Amennyiben a tárolóhely megtelik, az új adatok felülírják a régebbieket.

3.12.7 *Részletes sebességadatok*

(116) Az adatrögzítő készüléknek rögzíteni és tárolnia kell adatmemóriájában a jármű pillanatnyi sebességét és az ezzel összefüggő dátumot és időpontot a megelőző legalább 24 órás időszak minden másodpercében, amikor a járművet vezették.

3.12.8 *Az eseményekkel kapcsolatos adatok*

E szakasz alkalmazásában az időt egy másodperces pontossággal kell rögzíteni.

(117) Az adatrögzítő készüléknek az alábbi adatokat minden egyes felderített eseménynél az alábbi tárolási szabályok szerint rögzíteni és tárolnia kell adatmemóriájában:

▼B

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Érvénytelen kártya behelyezése	— a 10 legutóbbi esemény.	— az esemény dátuma és időpontja, — az eseményt előidéző kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kártyaütközés	— a 10 legutóbbi esemény.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — a kártyaütközést előidéző két kártya típusa, száma, kiállító tagállama és generációja.
Járművezetés megfelelő kártya nélkül	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kártya behelyezése járművezetés közben	— az utolsó esemény az utolsó 10 előfordulási nap mindegyikén,	— az esemény dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Az utolsó kártyakapcsolat nem megfelelő lezárása	— a 10 legutóbbi esemény.	— a kártyabehelyezés dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — a kártyáról leolvasott utolsó kártyakapcsolat adatai: — a kártyabehelyezés dátuma és időpontja, — a jármű rendszáma (VRN), valamint a nyilvántartásba vétel és a járműegység előállítása szerinti tagállam.
Gyorshajtás (1)	— a legsúlyosabb esemény az utolsó 10 előfordulási nap mindegyikén (például az, amelynél a legmagasabb volt az átlagsebesség) — az öt legsúlyosabb esemény az utolsó 365 nap folyamán. — a legutóbbi kalibrálást követő első esemény,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény alatt mért legnagyobb sebesség, — az esemény alatt mért számtani átlagsebesség, — a járművezetői kártya típusa, száma, kiállító tagállama és generációja (adott esetben), — az ugyanazon a napon történt hasonló események száma.

▼B

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Az áramellátás megszakadása (2)	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kommunikációs hiba a távoli kommunikációs eszközzel	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A GNSS-vevőből származó helyzetmeghatározási információk hiánya	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A mozgásadatok hibája	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A jármű mozgásával kapcsolatos ellentmondás	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A biztonsági rendszer megsértésére irányuló kísérlet	— a 10 legutolsó esemény eseménytípusonként.	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja (ha lényeges), — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az esemény típusa.

▼B

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Időütközés	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán.	— az adatrögzítő készülék által rögzített dátum és időpont, — GNSS-dátum és -időpont, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.

(1) Az adatrögzítő készüléknek az alábbi adatokat is rögzítenie és tárolnia kell adatmemóriájában:

— az utolsó GYORSHAJTÁS-ELLENŐRZÉS dátuma és időpontja,

— az erre a GYORSHAJTÁS-ELLENŐRZÉS-re következő első gyorshajtás dátuma és időpontja,

— a gyorshajtási események száma az utolsó GYORSHAJTÁS-ELLENŐRZÉS óta.

(2) Ezek az adatok csak akkor kerülhetnek rögzítésre, ha az áramellátás helyreállt, az időmérés pontossága egy perc lehet.

3.12.9 *A hibákkal kapcsolatos adatok*

E szakasz alkalmazásában az időt egy másodperces pontossággal kell rögzíteni.

(118) Az adatrögzítő készüléknek a következő tárolási szabályok szerint meg kell kísérelnie rögzíteni és tárolni az adatmemóriájában az összes észlelt hibát:

Hiba	Tárolási szabályok	Az egyes hibákkal kapcsolatban rögzítendő adatok
Kártyahiba	— a 10 legutóbbi járművezetői kártyahiba.	— a hiba kezdetének dátuma és időpontja, — a hiba végének dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja.
Az adatrögzítő készülék hibái	— a 10 legutóbbi hiba minden egyes hibatípusra, — a legutóbbi kalibrálást követő első hiba.	— a hiba kezdetének dátuma és időpontja, — a hiba végének dátuma és időpontja, — a hiba típusa, — a hiba kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja.

3.12.10 *Kalibrálási adatok*

(119) Az adatrögzítő készüléknek az alábbiakkal kapcsolatos adatokat rögzítenie és tárolnia kell adatmemóriájában:

— az aktiválás pillanatában ismert kalibrálási paraméterek,

▼B

— a készülék aktiválást követő legelső kalibrálása,

— a készülék első kalibrálása az aktuális járműben (amelyet a jármű-azonosító szám [VIN] azonosít),

— a 20 legutóbbi kalibrálás (ha ugyanazon a naptári napon több kalibrálást végeztek, csak az aznapi elsőt és utolsót kell tárolni).

(120) Az egyes kalibrálásokra vonatkozóan a következő adatokat kell rögzíteni:

— a kalibrálás célja (aktiválás, első beépítés, beépítés, időszakos vizsgálat),

— a műhely neve és címe,

— a műhelykártya száma, a kártyát kiállító tagállam és a kártya érvényességi ideje,

— a jármű azonosítása,

— aktualizált vagy megerősített paraméterek: w, k, l, abroncsméret, a sebességkorlátozó készülék beállítása, kilométer-számláló (régi és új értékek), dátum és időpont (régi és új értékek),

— az összes elhelyezett plomba típusa és azonosítása.

(121) Ezenkívül az adatrögzítő készüléknek rögzíteni és tárolnia kell adatmemóriájában, hogy képes-e első generációs tachográfkártyák használatára (aktiválva van-e még ez a funkció, avagy sem).

(122) A mozgásérzékelőnek a következő adatokat kell rögzítenie és tárolnia a memóriájában a mozgásérzékelő beépítésével kapcsolatban:

— a járműegységgel való első párosítás (dátum, időpont, a járműegység jóváhagyási száma és sorozatszáma),

— a járműegységgel való utolsó párosítás (dátum, időpont, a járműegység jóváhagyási száma és sorozatszáma).

(123) A külső GNSS-eszköznek a következő adatokat kell rögzítenie és tárolnia a memóriájában a külső GNSS-eszköz beépítésével kapcsolatban:

— a járműegységre való első rákapcsolódás (dátum, időpont, a járműegység jóváhagyási száma és sorozatszáma),

— a járműegységre való utolsó rákapcsolódás (dátum, időpont, a járműegység jóváhagyási száma és sorozatszáma).

3.12.11 *Időbeállítási adatok*

(124) Az adatrögzítő készüléknek a rendszeres kalibrálások keretén kívül kalibrálási üzemmódban végzett időbeállításokkal kapcsolatos következő adatokat rögzítenie és tárolnia kell adatmemóriájában:

— a legutóbbi időbeállítás,

— az öt legnagyobb mértékű időbeállítás.

(125) Az egyes időbeállításokra vonatkozóan a következő adatokat kell rögzíteni:

— dátum és időpont, régi érték,

— dátum és időpont, új érték,

— a műhely neve és címe,

— a műhelykártya száma, a kártyát kiállító tagállam, a kártya generációja és a kártya érvényességi ideje.

▼B

3.12.12 *Az ellenőrzési tevékenységre vonatkozó adatok*

(126) Az adatrögzítő készüléknek a 20 legutóbbi ellenőrzési tevékenységgel kapcsolatos következő adatokat rögzítenie és tárolnia kell adatmemóriájában:

— az ellenőrzés dátuma és időpontja,

— az ellenőrzőkártya száma, a kártyát kiállító tagállam és a kártya generációja,

— az ellenőrzés típusa (kijelzés és/vagy nyomtatás és/vagy a járműegységről való letöltés és/vagy kártyaletöltés és/vagy közúti kalibrálási ellenőrzés).

(127) Letöltés esetén a legrégebbi és a legfrissebb letöltött napok dátumait is rögzíteni kell.

3.12.13 *A vállalkozások általi lezárások adatai*

(128) Az adatrögzítő készüléknek a 255 legutóbbi, vállalkozás általi lezárással kapcsolatban a következő adatokat kell rögzítenie és tárolnia adatmemóriájában:

— a lezárás dátuma és időpontja,

— a feloldás dátuma és időpontja,

— a vállalkozáskártya száma, a kártyát kiállító tagállam és a kártya generációja,

— a vállalkozás neve és címe.

Azokat a korábban lezárt adatokat, amelyek lezárását a fenti mennyiségi korlát miatt eltávolították a memóriából, nem lezártnak kell tekinteni.

3.12.14 *A letöltési tevékenységre vonatkozó adatok*

(129) Az adatrögzítő készüléknek vállalkozási vagy kalibrálási üzemmódban a külső adathordozóra történő utolsó adatmemória-letöltésre vonatkozóan a következő adatokat kell rögzítenie és tárolnia az adatmemóriájában:

— a letöltés dátuma és időpontja,

— a vállalkozáskártya vagy a műhelykártya száma, a kártyát kiállító tagállam és a kártya generációja,

— a vállalkozás vagy a műhely neve.

3.12.15 *A különleges körülményekre vonatkozó adatok*

(130) Az adatrögzítő készüléknek a különleges körülményekre vonatkozó következő adatokat kell rögzítenie adatmemóriájában:

— az adatbevitel dátuma és időpontja,

— a különleges körülmény típusa.

(131) Az adatmemóriának legalább 365 napon át meg kell őriznie a különleges körülményekre vonatkozó adatokat (abból kiindulva, hogy átlagosan egy nyitott és egy zárt állapot fordul elő naponta). Amennyiben a tárolóhely megtelik, az új adatok felülírják a régebbieket.

3.12.16 *A tachográfkártya adatai*

(132) Az adatrögzítő készüléknek a járműegységben használt különböző tachográfkártyákkal kapcsolatban a következő adatokat kell tárolnia:

— a tachográfkártya száma és sorozatszáma,

— a tachográfkártya gyártója,

▼B

— a tachográfkártya típusa,

— a tachográfkártya változata.

(133) Az adatrögzítő készüléknek legalább 88 ilyen rekord tárolására képesnek kell lennie.

3.13 **A tachográfkártyák leolvasása**

(134) Az adatrögzítő készüléknek képesnek kell lennie arra, hogy első vagy második generációs tachográfkártyákról leolvassa adott esetben az alábbiakhoz szükséges adatokat:

— a kártyatípus, a kártyatulajdonos, az előzőleg használt jármű, az utolsó kártyakivétel dátuma és időpontja és az ezen időpontban kiválasztott tevékenység azonosítása,

— annak ellenőrzése, hogy az utolsó kártyakapcsolatot megfelelően zárták-e le,

— a járművezető megszakítás nélküli járművezetési idejének, halmozott pihenőidejének és halmozott járművezetési idejének kiszámítása, a megelőző és a folyó hétre vonatkozóan,

— a járművezetői kártyán rögzített adatok kért kinyomatainak kinyomtatása,

— a járművezetői kártya letöltése külső adathordozóra.

Ez a követelmény csak azokra az első generációs tachográfkártyákra vonatkozik, melyek használatának lehetőségét nem szüntette be valamelyik műhely.

(135) Olvasási hiba esetén az adatrögzítő készüléknek legfeljebb három alkalommal, ugyanazzal az olvasóparanccsal ismételten próbálkoznia kell, és ha továbbra is sikertelennek bizonyul, a kártyát hibásnak és érvénytelennek kell nyilvánítania.

3.14 **Rögzítés és tárolás a tachográfkártyákon**

3.14.1 *Rögzítés és tárolás az első generációs tachográfkártyákon*

(136) Amennyiben az első generációs tachográfkártyák használatának lehetőségét nem szüntette be valamelyik műhely, az adatrögzítő készüléknek pontosan ugyanúgy kell rögzítenie és tárolnia az adatokat, mint egy első generációs adatrögzítő készüléknek.

(137) Az adatrögzítő készüléknek közvetlenül a kártyabehelyezés után be kell állítania a „kártyakapcsolati adatokat” a járművezetői vagy a műhelykártyán.

(138) Az adatrögzítő készüléknek aktualizálnia kell az érvényes járművezetői, műhely- és/vagy ellenőrzőkártyákon tárolt adatokat a kártyatulajdonosra és az arra az időszakra vonatkozó valamennyi szükséges adattal együtt, mialatt a kártya behelyezett állapotban van. Az e kártyákon tárolt adatokat a 4. fejezet határozza meg.

(139) Az adatrögzítő készüléknek aktualizálnia kell az érvényes járművezetői és/vagy műhelykártyákon tárolt, a járművezetői tevékenységre és a helyre vonatkozó adatokat (a 4.5.3.1.9. és a 4.5.3.1.11. pontban meghatározottak szerint) a kártyatulajdonos által kézzel bevitt, a tevékenységre és a helyre vonatkozó adatokkal.

(140) Azok az események, amelyek az első generációs adatrögzítő készülék vonatkozásában nem lettek meghatározva, nem kerülnek tárolásra a járművezetői és műhelykártyákon.

▼B

(141) A tachográfkártyákon tárolt adatok aktualizálása úgy történik, hogy amennyiben az tekintettel a kártya tényleges tárolókapacitására szükségessé válik, az újabb adatok felülírják a régieket.

(142) Íráshiba esetén az adatrögzítő készüléknek legfeljebb három alkalommal, ugyanazzal az írásparanccsal ismételten próbálkoznia kell, és ha továbbra is sikertelennek bizonyul, a kártyát hibásnak és érvénytelennek kell nyilvánítania.

(143) Miután a vonatkozó adatok a járművezetői kártyán tárolásra kerültek, de még a kártya kioldása előtt az adatrögzítő készüléknek le kell nulláznia a „kártyakapcsolati adatokat”.

3.14.2 *Rögzítés és tárolás a második generációs tachográfkártyákon*

(144) A második generációs tachográfkártyáknak két különböző kártyaalkalmazással kell rendelkezniük, melyek közül az első pontosan megegyezik a TACHO nevű, első generációs tachográfkártyák használatára szolgáló alkalmazással, a második pedig a 4. fejezet 2. függelékében leírt „TACHO_G2” alkalmazás.

(145) Az adatrögzítő készüléknek közvetlenül a kártyabehelyezés után be kell állítania a „kártyakapcsolati adatokat” a járművezetői vagy a műhelykártyán.

(146) Az adatrögzítő készüléknek aktualizálnia kell az érvényes járművezetői, műhely- és/vagy ellenőrzőkártyák két kártyaalkalmazásában tárolt adatokat a kártyatulajdonosra és az arra az időszakra vonatkozó valamennyi szükséges adattal együtt, mialatt a kártya behelyezett állapotban van. Az e kártyákon tárolt adatokat a 4. fejezet határozza meg.

(147) Az adatrögzítő készüléknek aktualizálnia kell az érvényes járművezetői és/vagy műhelykártyákon tárolt, a járművezetői tevékenységre és a helyre (helységnév és földrajzi hely) vonatkozó adatokat (a 4.5.3.1.9., 4.5.3.1.11, 4.5.3.2.9., és 4.5.3.2.11. pontban meghatározottak szerint) a kártyatulajdonos által kézzel bevitt, a tevékenységre és a helyre vonatkozó adatokkal.

(148) A tachográfkártyákon tárolt adatok aktualizálása úgy történik, hogy amennyiben az tekintettel a kártya tényleges tárolókapacitására szükségessé válik, az újabb adatok felülírják a régieket.

(149) Íráshiba esetén az adatrögzítő készüléknek legfeljebb három alkalommal, ugyanazzal az írásparanccsal ismételten próbálkoznia kell, és ha továbbra is sikertelennek bizonyul, a kártyát hibásnak és érvénytelennek kell nyilvánítania.

(150) Miután a vonatkozó adatok a járművezetői kártya két kártyaalkalmazásában tárolásra kerültek, de még a kártya kioldása előtt az adatrögzítő készüléknek le kell nulláznia a „kártyakapcsolati adatokat”.

3.15 **Kijelzés**

(151) A kijelzőnek legalább 20 karakter megjelenítésére alkalmasnak kell lennie.

(152) A karakterek magassága legalább 5 mm, szélessége legalább 3,5 mm.

(153) A kijelzőnek képesnek kell lennie az 1. függelék 4. fejezetében („Karakterkészletek”) meghatározott karakterek kijelzésére. A kijelzőn megengedett az egyszerűsített írásmód használata (például az ékezetes betűk ékezet nélkül vagy a kisbetűk nagybetűként való megjelenítése).

▼B

(154) A kijelző világítása nem vakíthat.

(155) A kijelzőn megjelenő jeleknek az adatrögzítő készüléken kívülről is jól kell látszaniuk.

(156) Az adatrögzítő készüléknek ki kell jeleznie a következőket:

— alapértelmezett adatok,

— figyelmeztetésekkel kapcsolatos adatok,

— a menü elérésével kapcsolatos adatok,

— a felhasználó által kért egyéb adatok.

Az adatrögzítő készülék kijelezhet további információkat is, amennyiben ezek világosan megkülönböztethetők a fenti információktól.

(157) Az adatrögzítő készülék kijelzőjének a 3. függelékben felsorolt piktogramokat vagy piktogram-kombinációkat kell alkalmaznia. Emellett további piktogramokat vagy piktogram-kombinációkat is kijelezhet, amennyiben ezek világosan megkülönböztethetők a fent említett piktogramoktól vagy piktogram-kombinációktól.

(158) Mialatt a jármű mozog, a kijelzőnek mindvégig bekapcsolt („ON”) állapotban kell lennie.

(159) Az adatrögzítő készülék magában foglalhat kézi vagy automatikus berendezést, amellyel a kijelzőt ki lehet kapcsolni („OFF”), amikor a jármű nem mozog.

A kijelzés formátumát az 5. függelék határozza meg.

3.15.1 *Az alapértelmezett adatok kijelzése*

(160) Amennyiben más információ kijelzésére nincs szükség, az adatrögzítő készüléknek alapértelmezetten a következőket kell kijeleznie:

— helyi idő (UTC idő + a járművezető által végzett beállítás),

— az üzemmód,

— a járművezető és a járműkísérő folyamatban lévő tevékenysége,

— a járművezetőre vonatkozó információk:

— amennyiben aktuális tevékenysége JÁRMŰVEZETÉS, úgy az aktuális, megszakítás nélküli járművezetési idő és tényleges halmozott pihenőidő,

— amennyiben aktuális tevékenysége nem JÁRMŰVEZETÉS, úgy a folyamatban lévő tevékenységének időtartama (a tevékenység kiválasztása óta), és tényleges halmozott pihenőideje.

(161) Az egyes járművezetőkre vonatkozó adatokat világosan, érthetően és egyértelműen kell kijelezni. Amennyiben a járművezetőre és a járműkísérőre vonatkozó információk nem jelezhetők ki egyidejűleg, úgy az adatrögzítő készülék alapértelmezetten a járművezetőre vonatkozó információkat jelzi ki, de a felhasználó részére lehetővé teszi a járműkísérőre vonatkozó információk kijelzését.

(162) Amennyiben a kijelző szélessége nem teszi lehetővé az üzemmód alapértelmezett kijelzését, úgy a készüléknek az új üzemmódra váltáskor röviden ki kell jeleznie az új üzemmódot.

▼B

(163) Az adatrögzítő készüléknek új kártya behelyezésekor röviden ki kell jeleznie a kártyatulajdonos nevét.

(164) Amennyiben a „MENETÍRÓ KÉSZÜLÉK NEM SZÜKSÉGES” vagy a „KOMPON/VONATON MEGTETT ÚT” körülmény nyitott, ezt az alapértelmezett kijelző a megfelelő piktogrammal jelzi (megengedett, hogy a járművezető folyamatban lévő tevékenysége ezzel egy időben ne legyen kijelezve).

3.15.2 *Figyelmeztető kijelzés*

(165) Az adatrögzítő készüléknek figyelmeztetésként elsősorban a 3. függelék piktogramjait kell használnia, szükség esetén numerikusan kódolt információkkal kiegészítve ezeket. A figyelmeztetést emellett a járművezető által választott nyelven szövegesen is le lehet írni.

3.15.3 *A menü elérése*

(166) Az adatrögzítő készülékben a szükséges parancsoknak egy megfelelő menüstruktúra segítségével kell lehívhatónak lenniük.

3.15.4 *Egyéb kijelzett információk*

(167) Kérésre az alábbi adatok kijelzését is lehetővé kell tenni:

— UTC dátum és idő, valamint a helyi idő,

— a hat kinyomat bármelyikének tartalma a kinyomatokkal megegyező formátumban,

— a járművezető megszakítás nélküli járművezetési ideje és halmozott pihenőideje,

— a járműkísérő megszakítás nélküli járművezetési ideje és halmozott pihenőideje,

— a járművezető halmozott járművezetési ideje az előző és a folyó hétre,

— a járműkísérő halmozott járművezetési ideje az előző és a folyó hétre,

opcionálisan:

— a járműkísérő folyamatban lévő tevékenységének időtartama (a tevékenység menüből való kiválasztása óta),

— a járművezető halmozott járművezetési ideje a folyó hétre,

— a járműkísérő halmozott járművezetési ideje a folyó munkanapra,

— a járművezető halmozott járművezetési ideje a folyó munkanapra.

(168) A kinyomat tartalmát szekvenciálisan, sorról sorra kell kijelezni. Amennyiben a kijelző szélessége nem éri el a 24 karaktert, gondoskodni kell arról, hogy a felhasználó a megfelelő módon az összes információt meg tudja jeleníteni (több sorban, sorgörgetéssel stb.).

A kinyomaton a kézzel írott információk számára fenntartott sorokat nem kell megjeleníteni.

▼B

3.16 **Nyomtatás**

(169) Az adatrögzítő készüléknek képesnek kell lennie arra, hogy adatmemóriájából és/vagy a tachográfkártyákról információkat nyomtasson ki a következő hét kinyomatnak megfelelően:

— a kártyán tárolt járművezetői tevékenységek napi kinyomata,

— a járműegységen tárolt járművezetői tevékenységek napi kinyomata,

— a kártyán tárolt események és hibák kinyomata,

— a járműegységen tárolt események és hibák kinyomata,

— a műszaki adatok kinyomata,

— a gyorshajtások kinyomata,

— egy adott járműegység tachográfkártyájának adattörténete (lásd a 3.12.16. szakaszt).

E kinyomatok részletes formátumát és tartalmát a 4. függelék határozza meg.

A kinyomatok végén kiegészítő adatokat is fel lehet tüntetni.

Az adatrögzítő készülék emellett további kinyomatokat is készíthet, amennyiben ezek világosan megkülönböztethetők a fent említett hét kinyomattól.

(170) A „kártyán tárolt járművezetői tevékenységek napi kinyomata” és a „kártyán tárolt események és hibák kinyomata” csak az adatrögzítő készülékbe behelyezett járművezetői kártya vagy műhelykártya esetében állhatnak rendelkezésre. Az adatrögzítő készüléknek a nyomtatás megkezdése előtt aktualizálnia kell a megfelelő kártyán tárolt adatokat.

(171) A „kártyán tárolt járművezetői tevékenységek napi kinyomata” vagy a „kártyán tárolt események és hibák kinyomata” előállításához az adatrögzítő készüléknek:

— vagy automatikusan ki kell választania a járművezetői vagy a műhelykártyát, amennyiben e kártyák egyike került csak behelyezésre,

— vagy parancsot kell adnia a forráskártya kiválasztására, vagy a járművezetői kártyaolvasó egységben lévő kártya kiválasztására, amennyiben mindkét kártya be van helyezve az adatrögzítő készülékbe.

(172) A nyomtatónak képesnek kell soronként 24 karakter kinyomtatására.

(173) A karakterek magassága legalább 2,1 mm, szélessége legalább 1,5 mm.

(174) A nyomtatónak képesnek kell lennie az 1. függelék 4. fejezetében („Karakterkészletek”) meghatározott karakterek kinyomtatására.

(175) A nyomtatóknak az említett kinyomatokat olyan felbontásban kell előállítaniuk, hogy azok félreértések nélkül olvashatók legyenek.

(176) A kinyomatoknak rendes páratartalom mellett (10–90 %) és rendes hőmérsékleti körülmények között meg kell tartaniuk méretüket és meg kell őrizniük tartalmukat.

(177) Az adatrögzítő készülék által használt, típusjóváhagyással rendelkező papíron szerepelnie kell a megfelelő típus-jóváhagyási jelnek és annak/azoknak a készüléktípus(ok)nak, amelylyel/amelyekkel a papír felhasználható.

▼B

(178) A kinyomatoknak legalább két éven keresztül tisztán olvashatónak és azonosíthatónak kell maradniuk a szokásos tárolási feltételekre jellemző fényerősség, páratartalom és hőmérsékletviszonyok mellett.

(179) A kinyomatoknak legalább a 9. függelékben a tesztekre vonatkozóan meghatározott előírásoknak meg kell felelniük.

(180) Lehetővé kell tenni, hogy e dokumentumokra kézzel is írni lehessen, azaz például a járművezető alá tudja írni.

(181) Ha nyomtatás közben kifogy a papír, az adatrögzítő készüléknek a papír újratöltése után vagy elölről kell kezdenie a nyomtatást, vagy a megszakítás pontjától folytatnia kell, félreérthetetlenül megjelölve, hogy melyik volt az előzőleg kinyomtatott rész.

3.17 **Figyelmeztetések**

(182) Az adatrögzítő készüléknek figyelmeztetnie kell a járművezetőt bármilyen esemény és/vagy hiba észlelésekor.

(183) Az áramellátás megszakadására vonatkozó figyelmeztetés visszatartható az áramellátás helyreállításáig.

(184) Az adatrögzítő készüléknek 15 perccel a megszakítás nélkül legfeljebb megengedett járművezetési idő letelte előtt és ezen idő túllépése pillanatában figyelmeztetnie kell a járművezetőt.

(185) A figyelmeztető jelzéseknek vizuálisan kell megjelenniük. A látható figyelmeztetések hangjelzésekkel is kiegészíthetők.

(186) A látható figyelmeztetéseknek a felhasználó számára világosan felismerhetőnek kell lenniük, a járművezető látóterében kell megjelenniük, és tisztán olvashatónak kell lenniük mind nappal, mind éjjel.

(187) A látható figyelmeztetések jöhetnek az adatrögzítő készülékből és/vagy az adatrögzítő készüléken kívülről is.

(188) Az utóbbi esetben a figyelmeztetéseket „T” jellel kell ellátni.

(189) A figyelmeztetéseket legalább 30 másodpercen keresztül ki kell jelezni, hacsak a felhasználó hamarabb vissza nem igazolja őket az adatrögzítő készülék egy vagy több meghatározott gombjának lenyomásával. Ez az első visszaigazolás nem oldhatja fel a figyelmeztetés okára vonatkozó kijelzést, amelyet a következő szakasz említ.

(190) Az adatrögzítő készüléknek a figyelmeztetés okát is ki kell jelezni, és e figyelmeztetésnek mindaddig láthatónak kell maradnia, amíg a felhasználó nem igazolja vissza az adatrögzítő készülék egy meghatározott gombjának vagy parancsának alkalmazásával.

(191) Emellett további figyelmeztetések is adhatók, amennyiben azok nem téveszthetők össze az előző figyelmeztetésekkel.

3.18 **Adatletöltés külső adathordozókra**

(192) Az adatrögzítő készüléknek képesnek kell lennie arra, hogy adatmemóriájából vagy a járművezetői kártyáról kérésre adatokat töltsön le egy külső adathordozóra a kalibrálási/letöltő csatlakozón keresztül. Az adatrögzítő készüléknek a letöltés megkezdése előtt aktualizálnia kell a megfelelő kártyán tárolt adatokat.

▼B

(193) Emellett opcionális lehetőségként az adatrögzítő készülék – bármely üzemmódban – bármilyen más eszközön keresztül adatokat tölthet le az ezen eszközön keresztül hitelesített vállalkozás részére. Ilyen esetben e letöltésre a vállalkozási üzemmód adathozzáférési jogai vonatkoznak.

(194) A letöltés nem eredményezheti a tárolt adatok módosulását vagy törlését.

(195) A kalibrálási/letöltő csatlakozó elektromos interfészét a 6. függelék határozza meg.

(196) A letöltési protokollokat a 7. függelék határozza meg.

3.19 **Távoli kommunikáció a célzott közúti ellenőrzések céljára**

(197) Bekapcsolt gyújtás mellett a járműegységnek 60 másodpercenként el kell mentenie a távoli kommunikációs eszközben a célzott közúti ellenőrzésekhez szükséges legfrissebb adatokat. Ezeket az adatokat a 11. és 14. függelék szerint kell titkosítani és aláírni.

(198) A távészleléssel ellenőrizendő adatokat vezeték nélküli kommunikáció révén kell a távoli kommunikációs leolvasók számára elérhetővé tenni, amint azt a 14. függelék meghatározza.

(199) A célzott közúti ellenőrzések céljára a következő adatok szükségesek:

— a biztonsági rendszer megsértésére irányuló legutóbbi kísérlet,

— az áramellátás leghosszabb megszakadása,

— érzékelőhiba,

— a mozgásadatok hibája,

— a jármű mozgásával kapcsolatos ellentmondás,

— érvényes kártya nélküli járművezetés,

— kártyabehelyezés menet közben,

— időbeállítási adatok,

— kalibrálási adatok, beleértve a két legutóbbi kalibrálás elmentett adatait,

— a jármű rendszáma,

— az adatrögzítő készülék által rögzített sebesség.

3.20 **Külső kiegészítő eszközök számára kiadott adatok**

(200) Az adatrögzítő készüléket el lehet látni szabványosított interfészekkel, amelyek lehetővé teszik, hogy egy külső eszköz a menetíró készülék által rögzített vagy előállított adatokat működési vagy kalibrálási üzemmódban használni tudja.

A 13. függelék meghatározza szabványosított formában, hogy milyen opcionális ITS-interfészt lehet használni. A készüléknek emellett más hasonló interfészei is lehetnek, amennyiben azok teljes mértékben megfelelnek a 13. függelék követelményeinek a minimális adatlistát, a biztonságot és a járművezető hozzájárulását illetően.

Az említett interfészen keresztül rendelkezésre bocsátott ITS-adatokra a következő követelmények vonatkoznak:

— a menetíró adatszótárában meglévő adatokból kiválasztott adathalmazról van szó (1. függelék),

▼B

— e kiválasztott adatok egy részhalmaza a „személyes adat” jelölést kapta,

— a „személyes adatok” részhalmaz csak akkor hívható le, ha a járművezető igazolható módon hozzájárulását adta ahhoz, hogy személyes adatai elhagyják a járműhálózatot, és a hozzájárulási funkciót aktiválták,

— a járművezető hozzájárulása bármikor aktiválható vagy kikapcsolható a menüben szereplő parancsok segítségével, ha a járművezetői kártya be van helyezve,

— az adathalmazt és -részhalmazt vezeték nélküli Bluetooth protokollal továbbítják a jármű vezetőfülkéjének sugarán belül, 1 perces frissítési gyakorisággal,

— a külső eszköz és az ITS-interfész párosítását egy külön erre a célra szolgáló, véletlenszerűen megválasztott, 4 számból álló PIN kód védi, amelyet a járműegységben rögzítenek, és amely a kijelzőn keresztül megjeleníthető,

— az ITS-interfész jelenléte semmi esetre sem zavarhatja vagy befolyásolhatja a járműegység megfelelő működését és biztonságát.

Egyéb adatok is kiadhatók a meglévő adatokból kiválasztott, minimális listának tekintett adathalmazon kívül, feltéve, hogy nem minősülnek személyes adatoknak.

Az adatrögzítő készüléknek értesítést kell küldenie a többi külső eszközre a járművezető hozzájárulásáról.

Bekapcsolt gyújtás mellett ezeket az adatokat folyamatosan közvetíteni kell.

(201) A visszamenőleges kompatibilitásra tekintettel a menetíró készülékeket továbbra is fel lehet szerelni a 3281/85/EGK rendelet legutóbb módosított változatának 1.B. mellékletében meghatározott kapcsolatsor interfészével. A járművezető hozzájárulására azonban mindenképpen szükség van személyes adatok továbbítása esetén.

3.21 **Kalibrálás**

(202) A kalibrálási funkciónak a következőket kell lehetővé tenni:

— a mozgásérzékelő automatikus párosítása a járműegységgel,

— a külső GNSS-eszköz automatikus rákapcsolása a járműegységre adott esetben,

— az adatrögzítő készülék állandójának (k) digitális adaptálása a jármű jellemző együtthatójához (w),

— az aktuális idő beállítása a behelyezett műhelykártya érvényességi idején belül,

— a kilométer-számláló aktuális értékének beállítása,

— a mozgásérzékelő adatmemóriában tárolt azonosító adatainak aktualizálása,

— a külső GNSS-eszköz adatmemóriában tárolt azonosító adatainak aktualizálása adott esetben,

▼B

— az összes elhelyezett plomba típusának és azonosításának aktualizálása,

— az adatrögzítő készülék által ismert egyéb paraméterek aktualizálása vagy megerősítése: a jármű azonosítása, w, l, abroncsméret és adott esetben a sebességkorlátozó készülék beállítása.

(203) Emellett a kalibrálási funkciónak lehetővé kell tennie az első generációs tachográfkártyáknak az adatrögzítő készülékben való használatának beszüntetését, amennyiben a 15. függelékben meghatározott feltételek teljesülnek.

(204) A mozgásérzékelő és járműegység párosítása során legalább a következő műveleteknek végbe kell menniük:

— a mozgásérzékelő által tárolt, a mozgásérzékelő beépítésével kapcsolatos adatok aktualizálása (szükség szerint),

— a mozgásérzékelő azonosításához szükséges adatok átmásolása a mozgásérzékelőből a járműegység adatmemóriájába.

(205) A külső GNSS-eszköznek a járműegységre való rákapcsolódása során legalább a következő műveleteknek végbe kell menniük:

— a külső GNSS-eszköz által tárolt, a külső GNSS-eszköz beépítésével kapcsolatos adatok aktualizálása (szükség szerint),

— a külső GNSS-eszköz azonosításához szükséges adatok, köztük a külső GNSS-eszköz sorozatszámának átmásolása a külső GNSS-eszközből a járműegység adatmemóriájába.

A rákapcsolódást követően ellenőrizni kell a GNSS helyzetmeghatározási információit.

(206) A kalibrálási funkciónak lehetővé kell tennie a szükséges adatok betáplálását a kalibrálási/letöltő csatlakozó segítségével, a 8. függelékben meghatározott kalibrálási protokollal összhangban. A szükséges adatok kalibrálási funkción keresztüli betáplálása más eszközzel is történhet.

3.22 **Közúti kalibrálási ellenőrzés**

(207) A közúti kalibrálási ellenőrzési funkciónak lehetővé kell tennie az adapter részét képező mozgásérzékelő sorozatszámának és adott esetben a járműegységhez csatlakoztatott külső GNSS-eszköz sorozatszámának leolvasását az erre irányuló kérés időpontjában.

(208) A leolvasásnak legalább a járműegység kijelzőjén keresztül a menüben szereplő megfelelő parancsok kiválasztásával lehetségesnek kell lennie.

(209) A közúti kalibrálási ellenőrzési funkciónak lehetővé kell tennie továbbá a 6. függelékben meghatározott kalibrálási I/O jelvonal I/O üzemmódjának kiválasztását a K vonal interfészén keresztül. Ez az „ECUAdjustmentSession” szakaszban végezhető el, amint azt a 8. függelék 7. szakasza („Vizsgálati impulzusok vezérlése – input/output vezérlési funkcionális egység”) meghatározza.

3.23 **Időbeállítás**

(210) Az időbeállítási funkció lehetővé teszi az aktuális idő beállítását. Az adatrögzítő készülék két forrást használ az időbeállításhoz, melyek: 1) a járműegység beépített órája, 2) a GNSS-vevő.

▼B

(211) A járműegység beépített órájának időbeállítását legkésőbb 12 óránként automatikusan kiigazítják. Ha letelt ez az időintervallum, de nincsen GNSS-jel, az időbeállításnak a lehető leghamarabb meg kell történnie, amint a járműegység – attól függően, hogy a jármű mikor kap gyújtást – ismét érvényes időadatokhoz jut a GNSS-vevőből. A járműegységbe épített óra automatikus beállításához a GNSS-vevőből jövő időjelzést kell használni. Ha az aktuális idő több mint egy (1) perccel eltér a GNSS-vevő által szolgáltatott időadattól, annak „időütközés” eseményt kell kiváltania.

(212) Az időbeállítási funkciónak az aktuális idő kalibrálási üzemmódban történő, külső körülmény által kiváltott beállítását is lehetővé kell tennie.

3.24 **Teljesítményjellemzők**

(213) A járműegységnek a – 20 °C-tól 70 °C-ig, a külső GNSS-eszköznek – 20 °C-tól 70 °C-ig, a mozgásérzékelőnek pedig a – 40 °C-tól 135 °C-ig terjedő hőmérséklet-tartományban teljes mértékben működőképesnek kell lennie. Az adatmemória tartalmának – 40 °C-ig sérülésmentesnek kell maradnia.

(214) A menetíró készüléknek a 10 %-tól a 90 %-ig terjedő páratartalom-tartományban teljes mértékben működőképesnek kell maradnia.

(215) Az intelligens menetíró készülékben használt plombáknak ugyanazon körülményekkel szemben ellenállónak kell lenniük, mint a menetíró készülékek azon alkatrészei, amelyekre felerősítették őket.

(216) Az adatrögzítő készüléket óvni kell a túlfeszültségtől, az energiaellátás polaritásának felcserélésétől és a rövidzárlatoktól.

(217) A mozgásérzékelőknek:

— vagy reagálniuk kell a jármű mozgásának érzékelését zavaró mágneses terekre. Ilyen körülmények esetén a járműegység érzékelőhibát jegyez fel és tárol (88. követelmény),

— vagy olyan érzékelő elemmel kell rendelkezniük, amely védett a mágneses terekkel szemben.

(218) Az adatrögzítő készüléknek és a külső GNSS-eszköznek meg kell felelniük az ENSZ EGB 10. számú nemzetközi előírásának, és az elektrosztatikus kisülések és tranziens áramok elleni védelemmel kell rendelkezniük.

3.25 **Anyagok**

(219) Az adatrögzítő készülék valamennyi alkotóelemének megfelelő ellenálló képességgel és mechanikai szilárdsággal, továbbá állandó elektromos és mágneses jellemzőkkel rendelkező anyagokból kell készülnie.

(220) A szokásos használati körülményekre tekintettel a készülék valamennyi belső részét védeni kell a nedvességtől és a portól.

(221) A járműegységnek és a külső GNSS-eszköznek meg kell felelniük az IP 40 érintésvédelmi osztálynak, a mozgásérzékelőnek pedig az IP 64 érintésvédelmi osztálynak, amint azt az A1:1999 és az A2:2013 módosítást is magában foglaló IEC 60529:1989 szabvány előírja.

(222) Az adatrögzítő készüléknek meg kell felelnie az ergonómiai tervezésre vonatkozó érvényes műszaki rendelkezéseknek.

▼B

(223) Az adatrögzítő készüléket óvni kell a véletlenül bekövetkező sérülésektől.

3.26 **Jelölések**

(224) Amikor az adatrögzítő készülék kijelzi a jármű kilométerszámlálójának értékét és sebességét, a kijelzőn a következő adatoknak kell megjelenniük:

— a megtett távolságot mutató szám mellett a távolságmérés „km” rövidítéssel jelölt mértékegysége,

— a sebességet mutató szám mellett a „km/h” rövidítés.

Lehetővé kell tenni, hogy az adatrögzítő készüléket úgy is be lehessen állítani, hogy a sebességet mérföld per órában jelezze ki, ekkor a sebesség mértékegységét az „mph” rövidítéssel kell megadni. Lehetővé kell tenni, hogy az adatrögzítő készüléket úgy is be lehessen állítani, hogy a távolságot mérföldben jelezze ki, ekkor a távolság mértékegységét a „mi” rövidítéssel kell megadni.

(225) Az adatrögzítő készülék minden különálló alkatrészén ismertető címkét kell helyezni, amelyen a következő adatoknak kell szerepelniük:

— a berendezés gyártójának neve és címe,

— a gyártó által adott alkatrészszám és a berendezés gyártási éve,

— a berendezés sorozatszáma,

— a berendezés típus-jóváhagyási jele.

(226) Az ismertető címkén az alábbiaknak mindenképpen szerepelnie kell, akkor is, ha nincs elég hely az összes fent említett adat feltüntetésére: a gyártó neve vagy logója és a berendezés sorozatszáma.

4 A TACHOGRÁFKÁRTYÁK KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

4.1 **Látható adatok**

Az elülső oldalon a következőket kell feltüntetni:

(227) a kártya típusának megfelelően a „Járművezetői kártya” vagy „Ellenőrzőkártya” vagy „Műhelykártya” vagy „Vállalkozáskártya” szavak nagybetűvel szedve a kártyát kiállító tagállam hivatalos nyelvén vagy nyelvein,

(228) a kártyát kiállító tagállam neve (opcionális),

(229) a kártyát kiállító tagállam megkülönböztető jele, kék négyszögben, negatívan nyomtatva, 12 sárga csillaggal körülvéve. A megkülönböztető jelek a következők:

B	Belgium	LV	Lettország
BG	Bulgária	L	Luxemburg
CZ	Cseh Köztársaság	LT	Litvánia
CY	Ciprus	M	Málta
DK	Dánia	NL	Hollandia
D	Németország	A	Ausztria
EST	Észtország	PL	Lengyelország

▼B

GR	Görögország	P RO SK SLO	Portugália Románia Szlovákia Szlovénia
E	Spanyolország	FIN	Finnország
F HR H	Franciaország Horvátország Magyarország	S	Svédország
IRL	Írország	UK	Egyesült Királyság
I	Olaszország		

(230) a kiállított kártyára vonatkozó információk a következőképpen számozva:

	Járművezetői kártya	Ellenőrzőkártya	Vállalkozáskártya vagy műhelykártya
1.	a járművezető családi neve	az ellenőrző szerv neve	a vállalkozás vagy a műhely neve
2.	a járművezető utóneve(i)	az ellenőrző személy családi neve (adott esetben)	a kártyatulajdonos családi neve (adott esetben)
3.	a járművezető születési dátuma	az ellenőrző személy utóneve(i) (adott esetben)	a kártyatulajdonos utóneve(i) (adott esetben)
4.a	a kártya érvényességi idejének kezdete		
4.b	a kártya érvényességi idejének lejárata		
4.c	a kiállító hatóság neve (nyomtatható a hátoldalra is)		
4.d	az 5. pont alatt megadottól különböző szám adminisztratív célokra (opcionális)		
5. a	A vezetői engedély száma: (a járművezetői kártya kiállításának időpontjában)	—	—
5. b	Kártyaszám		
6.	A járművezető fényképe	az ellenőrző személy fényképe (opcionális)	a szerelő fényképe (opcionális)
7.	A tulajdonos aláírása (opcionális)		
8.	A tulajdonos lakóhelye vagy postacíme (opcionális).	Az ellenőrző szerve postacíme	a vállalkozás vagy műhely postacíme

(231) A dátumokat „nn/hh/éééé” vagy „nn.hh.éééé” (nap, hónap, év) formátumban kell megadni.

A hátoldalnak a következőket kell tartalmaznia:

(232) a kártya elülső oldalán feltüntetett számozott adatok magyarázata,

▼B

(233) adott esetben és a tulajdonos kifejezett, írásbeli beleegyezésével olyan adatok, amelyek nem kapcsolatosak a járművezetői kártya adminisztrációjával, amennyiben nem nehezítik meg a modell tachográfkártyaként történő használatát.

(234) A tachográfkártyákat a következő fő háttérszínekkel kell nyomtatni:

— járművezetői kártya: fehér,

— ellenőrzőkártya: kék,

— műhelykártya: piros,

— vállalkozáskártya: sárga.

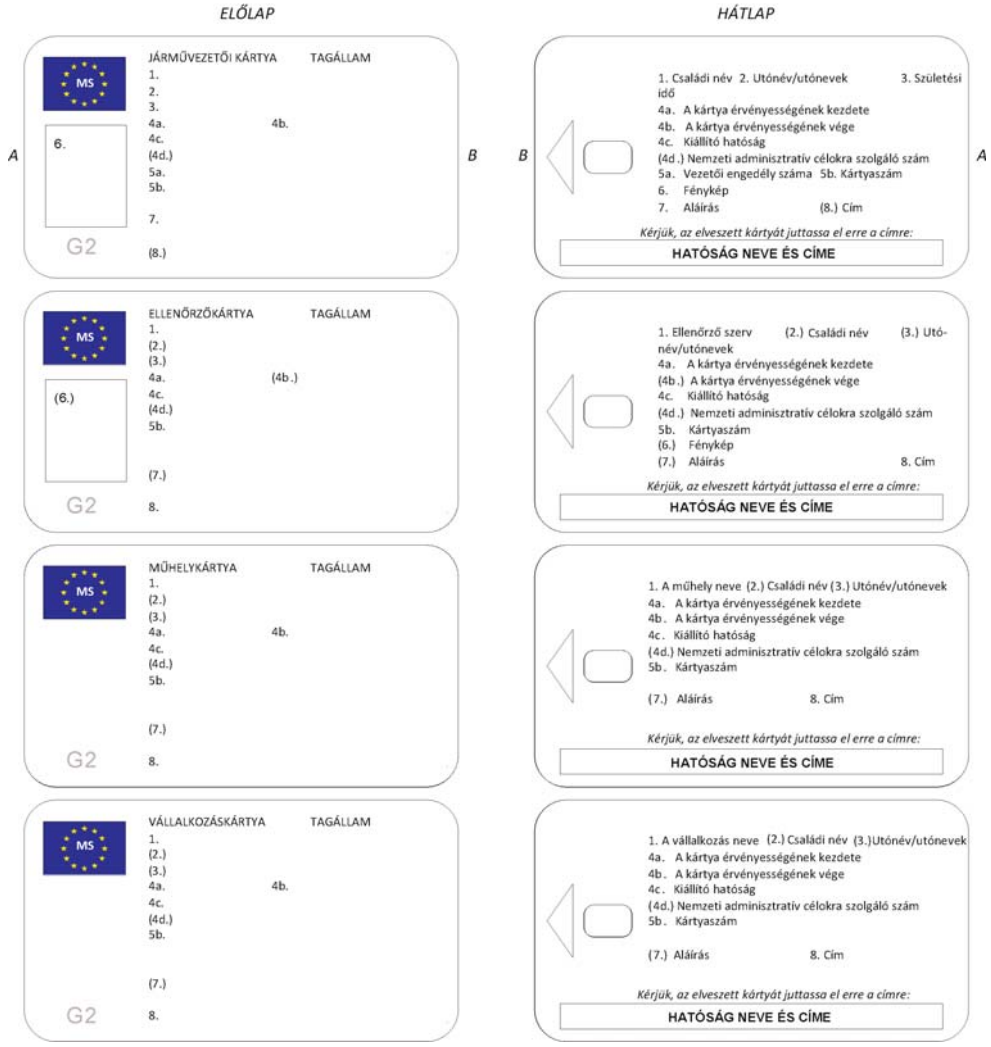
(235) A tachográfkártyákat a hamisítás és a manipulálás ellen legalább a következőkkel kell ellátni:

— biztonsági háttérnyomtatás, finom gilosmintával és írisznyomtatással,

— a fénykép helyén a biztonsági háttérnyomtatás és a fénykép közötti átfedés,

— legalább egy kétszínű mikronyomtatású vonal.

A TACHOGRÁFKÁRTYÁK KÖZÖSSÉGI MODELLJE



▼B

(236) A Bizottsággal folyatott megfelelő egyeztetés után e melléklet egyéb rendelkezéseinek sérelme nélkül a tagállamok más színeket vagy jelöléseket is használhatnak, például nemzeti szimbólumokat vagy biztonsági elemeket.

(237) A 165/2014/EU rendelet 26. cikkének (4) bekezdésében említett ideiglenes kártyáknak is meg kell felelniük e melléklet rendelkezéseinek.

4.2 **Biztonság**

A rendszerbiztonság célja a kártyák és az adatrögzítő készülék között kicserélt adatok integritásának és hitelességének, valamint a kártyákról letöltött adatok integritásának és hitelességének védelme, amely cél érdekében bizonyos kártyabeírási műveletek elvégzését kizárólag az adatrögzítő készülékre korlátozza, és bizonyos adatokat titkosít, kizárva a kártyákon tárolt adatok bármiféle hamisítását, megakadályozva a manipulálást és feltárva minden ilyen kísérletet.

(238) A rendszerbiztonság elérése céljából a tachográfkártyáknak meg kell felelniük a 10. és 11. függelékben meghatározott biztonsági követelményeknek.

(239) A tachográfkártyák leolvasását más berendezésekkel is lehetővé kell tenni, például személyi számítógépekkel.

4.3 **Szabványok**

(240) A tachográfkártyáknak a következő szabványoknak kell megfelelniük:

— ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők,

— ISO IEC/7816 Azonosító kártyák – Integrált áramkörös kártyák:

— 1. rész: Fizikai jellemzők,

— 2. rész: Az érintkezők méretei és elhelyezkedése (ISO/IEC 7816-2:2007),

— 3. rész: Elektromos interfész és átviteli protokollok (ISO/IEC 7816-3:2006),

— 4. rész: Az adatcsere megszervezése, biztonsága és vezérlése (ISO/IEC 7816-4:2013 + 1:2014 helyesbítés),

— 6. rész: Ágazatközi adatelemek az adatcseréhez (ISO/IEC 7816-6:2004 + 1:2006 helyesbítés),

— 8. rész: A biztonsági műveletekre vonatkozó parancsok (ISO/IEC 7816-8:2004).

— A tachográfkártyák vizsgálatát az ISO/IEC 10373-3:2010 „Azonosító kártyák – Vizsgálati módszerek – 3. rész: Integrált áramkörös kártyák érintkezőkkel és a kapcsolódó interfészberendezések” szabvány szerint kell végezni.

4.4 **Környezeti és elektromos előírások**

(241) A tachográfkártyáknak rendeltetésszerűen kell működniük a Közösség területén rendesen előforduló éghajlati viszonyok között, és legalább a – 25 °C-tól + 70 °C-ig terjedő hőmérséklet-tartományban, + 85 °C-os esetenkénti csúcsokkal; ahol az „esetenkénti” kifejezés legfeljebb 4 órás időtartamot és a kártya élettartama alatt legfeljebb 100 alkalmat jelent.

(242) A tachográfkártyáknak a 10 %-tól 90 %-ig terjedő páratartalom-tartományban rendeltetésszerűen kell működniük.

▼B

(243) A tachográfkártyáknak öt éven át rendeltetésszerűen kell működniük, amennyiben a környezeti és elektromos előírásoknak megfelelően használják őket.

(244) A tachográfkártyáknak a működésük során meg kell felelniük az elektromágneses kompatibilitásra vonatkozó, 10. számú ENSZ EGB-előírásnak, és az elektrosztatikus kisülések elleni védelemmel kell rendelkezniük.

4.5 **Adattárolás**

E szakasz alkalmazásában:

— Eltérő utasítások hiányában az időt egyperces pontossággal kell rögzíteni.

— A kilométer-számláló értékeit egy kilométeres pontossággal kell rögzíteni.

— A sebességadatokat 1 km/h pontossággal kell rögzíteni.

— A földrajzi helyzetet (szélesség és hosszúság) fokban és percekben kell megadni, 1/10 perc pontossággal.

A tachográfkártyáknak az adattárolási követelményeknek megfelelő funkcióit, parancsait és logikai szerkezetét a 2. függelék határozza meg.

Ellenkező rendelkezések hiányában a tachográfkártyákon való adattárolás szervezési elve, hogy az új adatok felülírják a régebb óta tárolt adatokat, amennyiben a meghatározott adatrekordok számára fenntartott tárolóhely megtelik.

(245) E szakasz meghatározza a különféle alkalmazások adatfájljai számára fenntartott minimális tárolóhelyet. A tachográfkártyáknak jelezniük kell az adatrögzítő készülék felé, hogy az egyes adatfájlok számára aktuálisan mekkora tárolóhely van még.

(246) A tachográfkártyákon tárolható minden további, az esetleges egyéb kártyaalkalmazásokkal összefüggő adat tárolásának a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 95/46/EK irányelvnek, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002/58/EK irányelvnek, valamint a 165/2014/EU rendelet 7. cikkének megfelelően kell történnie.

(247) Minden tachográfkártya valamennyi törzsállománya (MF) legfeljebb öt, a kártya kezelését, a kártyaalkalmazásokat és a chipazonosítást szolgáló elemi fájlból (EF) és két meghatározott célra rendelt fájlból (DF) áll:

— DF Tachograph, amely az első generációs járműegységek számára elérhető alkalmazást tartalmazza, amely az első generációs tachográfkártyákban is jelen van,

— DF Tachograph_G2, amely a csak második generációs járműegységek számára elérhető alkalmazást tartalmazza, amely csak a második generációs tachográfkártyákban van jelen.

A tachográfkártyák szerkezetét teljes részletességben a 2. függelék határozza meg.

4.5.1 *Az azonosítást és a kártya kezelését szolgáló elemi fájlok*

4.5.2 *Az integrált áramkörös kártyák azonosítása*

(248) A tachográfkártyáknak az intelligens kártyák azonosítására a következő adatokat kell tárolniuk:

— stopperóra,

▼B

— a kártya sorozatszáma (beleértve a gyártási referenciákat),

— a kártya típus-jóváhagyási száma,

— a kártyához kapcsolt személyi azonosító (ID),

— a kártyába chipet beépítő gyártó azonosítója (ID),

— IC-azonosító.

4.5.2.1 Chipazonosítás

(249) A tachográfkártyáknak az integrált áramkörök (IC) azonosítására a következő adatokat kell tárolniuk:

— IC-sorozatszám,

— IC-gyártási referenciák.

4.5.2.2 DIR (csak második generációs tachográfkártyákban van jelen)

(250) A tachográfkártyáknak tárolniuk kell a 2. függelékben meghatározott alkalmazásazonosító adatobjektumokat.

4.5.2.3 ATR-információ (korlátozott, csak második generációs tachográfkártyákban van jelen)

(251) A tachográfkártyáknak a következő kiterjesztett hosszúságú adatobjektumot kell tárolniuk:

— abban az esetben, ha a tachográfkártya támogatja a kiterjesztett hosszúságú adatmezőket, a 2. függelékben meghatározott, kiterjesztett hosszúságú adatobjektum.

4.5.2.4 Kiterjesztett hosszúságú információk (korlátozott, csak második generációs tachográfkártyákban van jelen)

(252) A tachográfkártyáknak a következő kiterjesztett hosszúságú adatobjektumokat kell tárolniuk:

— abban az esetben, ha a tachográfkártya támogatja a kiterjesztett hosszúságú adatmezőket, a 2. függelékben meghatározott, kiterjesztett hosszúságú adatobjektumok.

4.5.3 *Járművezetői kártya*

4.5.3.1 Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.3.1.1 Alkalmazásazonosító

(253) A járművezetői kártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.3.1.2 Kulcsok és tanúsítványok

(254) A járművezetői kártyának képesnek kell lennie egy sor, a 11. függelék A. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

▼B

4.5.3.1.3 A kártya azonosítása

(255) A járművezetői kártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata.

4.5.3.1.4 A kártyatulajdonos azonosítása

(256) A járművezetői kártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— születési dátum,

— választott nyelv.

4.5.3.1.5 Kártyaletöltés

(257) A járművezetői kártyának a kártyaletöltéssel kapcsolatos következő adatokat kell tárolnia:

— azt utolsó kártyaletöltés dátuma és időpontja (az ellenőrzéstől eltérő célokra).

(258) A járművezetői kártyának egy ilyen rekord tárolására képesnek kell lennie.

4.5.3.1.6 Információk a vezetői engedélyről

(259) A járművezetői kártyának a vezetői engedéllyel kapcsolatos következő adatokat kell tárolnia:

— a kiállító tagállam, a kiállító hatóság neve,

— a vezetői engedély száma (a kártya kiállításának időpontjában).

4.5.3.1.7 Az eseményekkel kapcsolatos adatok

E szakasz alkalmazásában az időadatokat egy másodperces pontossággal kell tárolni.

(260) A járművezetői kártyának képesnek kell lennie tárolni az adatrögzítő készülék által a kártya behelyezett állapota alatt észlelt következő eseményekkel kapcsolatos adatokat:

— időátfedés (amennyiben az eseményt ez a kártya váltotta ki),

— kártya behelyezése járművezetés közben (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az utolsó kártyakapcsolat nem megfelelő lezárása (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az áramellátás megszakadása,

— a mozgásadatok hibája,

— a biztonsági rendszer megsértésére irányuló kísérletek,

(261) A járművezetői kártyának az említett eseményekkel kapcsolatban a következő adatokat kell tárolnia:

— az esemény kódja,

— az esemény kezdetének dátuma és időpontja (vagy a kártyabehelyezés dátuma és időpontja, ha az esemény már folyamatban volt ezen időpontban),

▼B

— az esemény végének dátuma és időpontja (vagy a kártyakivétel dátuma és időpontja, ha az esemény már folyamatban volt ezen időpontban),

— a jármű rendszáma (VRN) és azon jármű nyilvántartásba vétele szerinti tagállam, amelyben az esemény történt.

Megjegyzés: az „időátfedés” eseményre vonatkozóan:

— az esemény kezdetének dátuma és időpontja meg kell, hogy egyezzen az előző járműből történő kártyakivétel dátumával és időpontjával,

— az esemény végének dátuma és időpontja meg kell, hogy egyezzen az aktuális járműbe történő kártyabehelyezés dátumával és időpontjával,

— a jármű adatainak meg kell egyezniük az eseményt előidéző aktuális jármű adataival.

Megjegyzés: Az „utolsó kártyakapcsolat nem megfelelő lezárása” eseményre vonatkozóan:

— az esemény kezdetének dátuma és időpontja meg kell, hogy egyezzen azon kártyabehelyezés dátumával és időpontjával, amelynél a kártyakapcsolat nem került megfelelően lezárásra,

— az esemény végének dátuma és időpontja meg kell, hogy egyezzen azon kártyabehelyezés dátumával és időpontjával, amikor a kártyakapcsolat folyamán az eseményt észlelték (aktuális kártyakapcsolat),

— a jármű adatainak meg kell egyezniük azon jármű adataival, amelyben a kapcsolat nem került megfelelően lezárásra.

(262) A járművezetői kártyának minden egyes típussal összefüggésben tárolnia kell a hat legutóbbi eseményre vonatkozó adatokat (azaz 36 eseményt).

4.5.3.1.8 A hibákkal kapcsolatos adatok

E szakasz alkalmazásában az időt egy másodperces pontossággal kell rögzíteni.

(263) A járművezetői kártyának képesnek kell lennie tárolni az adatrögzítő készülék által a kártya behelyezett állapota alatt észlelt következő hibákkal kapcsolatos adatokat:

— kártyahiba (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az adatrögzítő készülék hibája.

(264) A járművezetői kártyának az említett hibákkal kapcsolatban a következő adatokat kell tárolnia:

— hibakód,

— a hiba kezdetének dátuma és időpontja (vagy a kártyabehelyezés dátuma és időpontja, ha a hiba már folyamatban volt ezen időpontban),

— a hiba végének dátuma és időpontja (vagy a kártyakivétel dátuma és időpontja, ha a hiba már folyamatban volt ezen időpontban),

— a jármű rendszáma (VRN) és azon jármű nyilvántartásba vétele szerinti tagállam, amelyben a hiba történt.

(265) A járművezetői kártyának minden egyes típussal összefüggésben tárolnia kell a 12 legutóbbi hibára vonatkozó adatokat (azaz 24 hibát).

▼B

4.5.3.1.9 A járművezető tevékenységére vonatkozó adatok

(266) A járművezetői kártyának minden olyan naptári napra vonatkozóan, amelyen a kártyát használták, vagy amelyen a járművezető kézzel vitt be tevékenységeket, tárolnia kell a következő adatokat:

— a dátum,

— a napi jelenlét számlálója (egy egységgel megnövelve minden egyes naptári napra),

— a járművezető által e napon megtett teljes távolság,

— a járművezető állapota 00.00-kor,

— minden egyes alkalommal, amikor a járművezető megváltoztatta tevékenységét és/vagy járművezetési állapotát és/vagy behelyezte vagy kivette kártyáját:

— a járművezetési állapot (SZEMÉLYZET, EGYEDÜLI),

— a kártyaolvasó egység (JÁRMŰVEZETŐI, JÁRMŰKÍSÉRŐI),

— a kártyaállapot (BEHELYEZVE, NINCS BEHELYEZVE)

— a tevékenység (JÁRMŰVEZETÉS, KÉSZENLÉT, MUNKA, SZÜNET/PIHENÉS),

— a változás időpontja.

(267) A járművezetői kártya memóriájának a járművezető tevékenységére vonatkozó adatokat legalább 28 napon át tárolnia kell (egy járművezető átlagos tevékenysége a meghatározás szerint napi 93 tevékenységváltozás).

(268) A 261., 264. és 266. követelményben felsorolt adatokat úgy kell tárolni, hogy a tevékenységeket előfordulásuk sorrendjében vissza lehessen keresni, időátfedés esetén is.

4.5.3.1.10 Az üzemeltetett járművek adatai

(269) A járművezetői kártyának minden olyan naptári napra vonatkozóan, amelyen a kártyát használták, valamint e napokon belül az adott jármű minden egyes használati időszakára vonatkozóan tárolnia kell a következő adatokat (egy használati időszak magában foglalja e kártya tekintetében az összes egymást követő kártyabehelyezési/-kivételi ciklust a járműben):

— a jármű első használatának dátuma és időpontja (tehát az első kártyabehelyezés a jármű e használati időszakára vonatkozóan, vagy 00.00 óra, amennyiben a használati időszak éppen folyamatban van),

— a jármű kilométer-számlálójának értéke ezen időpontban,

— a jármű utolsó használatának dátuma és időpontja (tehát az utolsó kártyakivétel a jármű e használati időszakában, vagy 23.59, amennyiben a használati időszak éppen folyamatban van),

▼B

— a jármű kilométer-számlálójának értéke ezen időpontban,

— a jármű rendszáma (VRN) és a jármű nyilvántartásba vétele szerinti tagállam.

(270) A járművezetői kártyának legalább 84 ilyen rekord tárolására képesnek kell lennie.

4.5.3.1.11 A munkanap kezdő és/vagy végső helye

(271) A járművezetői kártyának azokkal a helyekkel kapcsolatban, amelyeket a járművezető a munkanapok kezdetének és/vagy végének helyeként bevitt a készülékbe, a következő adatokat kell tárolnia:

— az adatbevitel dátuma és időpontja (vagy a bevitt adatra vonatkozó dátum/idő, amennyiben azt kézzel vitték be),

— a bevitt adat típusa (kezdés vagy befejezés, az adatbevitel feltétele),

— a bevitt ország és régió,

— a jármű kilométer-számlálójának értéke.

(272) A járművezetői kártya memóriájának legalább 42 ilyen rekordpár tárolására képesnek kell lennie.

4.5.3.1.12 Kártyakapcsolati adatok

(273) A járművezetői kártyának képesnek kell lennie azon járműre vonatkozó adatokat tárolni, amely az aktuális kártyakapcsolatot megnyitotta:

— a kapcsolat megnyitásának (kártyabehelyezés) dátuma és időpontja, egy másodperces pontossággal,

— a jármű rendszáma (VRN) és a nyilvántartásba vétel szerinti tagállam.

4.5.3.1.13 Az ellenőrzési tevékenységre vonatkozó adatok

(274) A járművezetői kártyának az ellenőrzési tevékenységekkel kapcsolatban a következő adatokat kell tárolnia:

— az ellenőrzés dátuma és időpontja,

— az ellenőrzőkártya száma és a kártyát kiállító tagállam,

— az ellenőrzés típusa (kijelzés és/vagy nyomtatás és/vagy a járműegységről való letöltés és/vagy kártyaletöltés [lásd megjegyzés]),

— a letöltött időszak letöltés esetén,

— a jármű rendszáma (VRN) és az ellenőrzött jármű nyilvántartásba vétele szerinti tagállam.

Megjegyzés: a kártya letöltése csak akkor kerül rögzítésre, ha ezt egy adatrögzítő készülék hajtja végre.

(275) A járművezetői kártyának egy ilyen rekord tárolására képesnek kell lennie.

4.5.3.1.14 A különleges körülményekre vonatkozó adatok

(276) A járművezetői kártyának tárolnia kell a különleges körülményekre vonatkozóan a kártya behelyezett állapotában bevitt adatokat (bármely kártyaolvasó egység esetében):

— az adatbevitel dátuma és időpontja,

— a különleges körülmény típusa.

▼B

(277) A járművezetői kártyának legalább 56 ilyen rekord tárolására képesnek kell lennie.

4.5.3.2 Második generációs tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.3.2.1 Alkalmazásazonosító

(278) A járművezetői kártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.3.2.2 Kulcsok és tanúsítványok

(279) A járművezetői kártyának képesnek kell lennie egy sor, a 11. függelék B. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

4.5.3.2.3 A kártya azonosítása

(280) A járművezetői kártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata.

4.5.3.2.4 A kártyatulajdonos azonosítása

(281) A járművezetői kártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— születési dátum,

— választott nyelv.

4.5.3.2.5 Kártyaletöltés

(282) A járművezetői kártyának a kártyaletöltéssel kapcsolatos következő adatokat kell tárolnia:

— azt utolsó kártyaletöltés dátuma és időpontja (az ellenőrzéstől eltérő célokra).

(283) A járművezetői kártyának egy ilyen rekord tárolására képesnek kell lennie.

4.5.3.2.6 Információk a vezetői engedélyről

(284) A járművezetői kártyának a vezetői engedéllyel kapcsolatos következő adatokat kell tárolnia:

— a kiállító tagállam, a kiállító hatóság neve,

— a vezetői engedély száma (a kártya kiállításának időpontjában).

4.5.3.2.7 Az eseményekkel kapcsolatos adatok

E szakasz alkalmazásában az időadatokat egy másodperces pontossággal kell tárolni.

▼B

(285) A járművezetői kártyának képesnek kell lennie tárolni az adatrögzítő készülék által a kártya behelyezett állapota alatt észlelt következő eseményekkel kapcsolatos adatokat:

— időátfedés (amennyiben az eseményt ez a kártya váltotta ki),

— a kártya behelyezése járművezetés közben (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az utolsó kártyakapcsolat nem megfelelő lezárása (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az áramellátás megszakadása,

— kommunikációs hiba a távoli kommunikációs eszközzel,

— a GNSS-vevőből származó helyzetmeghatározási információk hiánya,

— kommunikációs hiba a külső GNSS-eszközzel,

— a mozgásadatok hibája,

— a jármű mozgásával kapcsolatos ellentmondás,

— a biztonsági rendszer megsértésére irányuló kísérletek,

— időütközés.

(286) A járművezetői kártyának az említett eseményekkel kapcsolatban a következő adatokat kell tárolnia:

— az esemény kódja,

— az esemény kezdetének dátuma és időpontja (vagy a kártyabehelyezés dátuma és időpontja, ha az esemény már folyamatban volt ezen időpontban),

— az esemény végének dátuma és időpontja (vagy a kártyakivétel dátuma és időpontja, ha az esemény már folyamatban volt ezen időpontban),

— a jármű rendszáma (VRN) és azon jármű nyilvántartásba vétele szerinti tagállam, amelyben az esemény történt.

Megjegyzés: az „időátfedés” eseményre vonatkozóan:

— az esemény kezdetének dátuma és időpontja meg kell, hogy egyezzen az előző járműből történő kártyakivétel dátumával és időpontjával,

— az esemény végének dátuma és időpontja meg kell, hogy egyezzen az aktuális járműbe történő kártyabehelyezés dátumával és időpontjával,

— a jármű adatainak meg kell egyezniük az eseményt előidéző aktuális jármű adataival.

Megjegyzés: Az „utolsó kártyakapcsolat nem megfelelő lezárása” eseményre vonatkozóan:

— az esemény kezdetének dátuma és időpontja meg kell, hogy egyezzen azon kártyabehelyezés dátumával és időpontjával, amelynél a kártyakapcsolat nem került megfelelően lezárásra,

— az esemény végének dátuma és időpontja meg kell, hogy egyezzen azon kártyabehelyezés dátumával és időpontjával, amikor a kártyakapcsolat folyamán az eseményt észlelték (aktuális kártyakapcsolat),

▼B

— a jármű adatainak meg kell egyezniük azon jármű adataival, amelyben a kapcsolat nem került megfelelően lezárásra.

(287) A járművezetői kártyának minden egyes típussal összefüggésben tárolnia kell a hat legutóbbi eseményre vonatkozó adatokat (azaz 66 eseményt).

4.5.3.2.8 A hibákkal kapcsolatos adatok

E szakasz alkalmazásában az időt egy másodperces pontossággal kell rögzíteni.

(288) A járművezetői kártyának képesnek kell lennie tárolni az adatrögzítő készülék által a kártya behelyezett állapota alatt észlelt következő hibákkal kapcsolatos adatokat:

— kártyahiba (amennyiben az esemény ehhez a kártyához kapcsolódik),

— az adatrögzítő készülék hibája.

(289) A járművezetői kártyának az említett hibákkal kapcsolatban a következő adatokat kell tárolnia:

— hibakód,

— a hiba kezdetének dátuma és időpontja (vagy a kártyabehelyezés dátuma és időpontja, ha a hiba már folyamatban volt ezen időpontban),

— a hiba végének dátuma és időpontja (vagy a kártyakivétel dátuma és időpontja, ha a hiba már folyamatban volt ezen időpontban),

— a jármű rendszáma (VRN) és azon jármű nyilvántartásba vétele szerinti tagállam, amelyben a hiba történt.

(290) A járművezetői kártyának minden egyes típussal összefüggésben tárolnia kell a 12 legutóbbi hibára vonatkozó adatokat (azaz 24 hibát).

4.5.3.2.9 A járművezető tevékenységére vonatkozó adatok

(291) A járművezetői kártyának minden olyan naptári napra vonatkozóan, amelyen a kártyát használták, vagy amelyen a járművezető kézzel vitt be tevékenységeket, tárolnia kell a következő adatokat:

— a dátum,

— a napi jelenlét számlálója (egy egységgel megnövelve minden egyes naptári napra),

— a járművezető által e napon megtett teljes távolság,

— a járművezető állapota 00.00-kor,

— minden egyes alkalommal, amikor a járművezető megváltoztatta tevékenységét és/vagy járművezetési állapotát és/vagy behelyezte vagy kivette kártyáját:

— a járművezetési állapot (SZEMÉLYZET, EGYEDÜLI),

— a kártyaolvasó egység (JÁRMŰVEZETŐI, JÁRMŰKÍSÉRŐI),

— a kártyaállapot (BEHELYEZVE, NINCS BEHELYEZVE)

— a tevékenység (JÁRMŰVEZETÉS, KÉSZENLÉT, MUNKA, SZÜNET/PIHENÉS),

▼B

— a változás időpontja.

(292) A járművezetői kártya memóriájának a járművezető tevékenységére vonatkozó adatokat legalább 28 napon át tárolnia kell (egy járművezető átlagos tevékenysége a meghatározás szerint napi 93 tevékenységváltozás).

(293) A 286., 289. és 291. követelményben felsorolt adatokat úgy kell tárolni, hogy a tevékenységeket előfordulásuk sorrendjében vissza lehessen keresni, időátfedés esetén is.

4.5.3.2.10 Az üzemeltetett járművek adatai

(294) A járművezetői kártyának minden olyan naptári napra vonatkozóan, amelyen a kártyát használták, valamint e napokon belül az adott jármű minden egyes használati időszakára vonatkozóan tárolnia kell a következő adatokat (egy használati időszak magában foglalja e kártya tekintetében az összes egymást követő kártyabehelyezési/kivételi ciklust a járműben):

— a jármű első használatának dátuma és időpontja (tehát az első kártyabehelyezés a jármű e használati időszakára vonatkozóan vagy 00.00 óra, amennyiben a használati időszak éppen folyamatban van),

— a jármű kilométer-számlálójának értéke az első használat időpontjában,

— a jármű utolsó használatának dátuma és időpontja (tehát az utolsó kártyakivétel a jármű e használati időszakában, vagy 23.59, amennyiben a használati időszak éppen folyamatban van),

— a jármű kilométer-számlálójának értéke az utolsó használat időpontjában,

— a jármű rendszáma (VRN) és a jármű nyilvántartásba vétele szerinti tagállam,

— a jármű jármű-azonosító száma (VIN).

(295) A járművezetői kártyának legalább 84 ilyen rekord tárolására képesnek kell lennie.

4.5.3.2.11 A munkanap kezdő és/vagy végső helye (helységnév és földrajzi hely)

(296) A járművezetői kártyának azokkal a helyekkel kapcsolatban, amelyeket a járművezető a munkanapok kezdetének és/vagy végének helyeként bevitt a készülékbe, a következő adatokat kell tárolnia:

— az adatbevitel dátuma és időpontja (vagy a bevitt adatra vonatkozó dátum/idő, amennyiben azt kézzel vitték be),

— a bevitt adat típusa (kezdés vagy befejezés, az adatbevitel feltétele),

— a bevitt ország és régió,

— a jármű kilométer-számlálójának értéke,

— a jármű helyzete,

— a GNSS pontossága és a helyzet meghatározásának dátuma és időpontja.

(297) A járművezetői kártya memóriájának legalább 84 ilyen rekordpár tárolására képesnek kell lennie.

▼B

4.5.3.2.12 Kártyakapcsolati adatok

(298) A járművezetői kártyának képesnek kell lennie azon járműre vonatkozó adatokat tárolni, amely az aktuális kártyakapcsolatot megnyitotta:

— a kapcsolat megnyitásának (kártyabehelyezés) dátuma és időpontja, egy másodperces pontossággal,

— a jármű rendszáma (VRN) és a nyilvántartásba vétel szerinti tagállam.

4.5.3.2.13 Az ellenőrzési tevékenységre vonatkozó adatok

(299) A járművezetői kártyának az ellenőrzési tevékenységekkel kapcsolatban a következő adatokat kell tárolnia:

— az ellenőrzés dátuma és időpontja,

— az ellenőrzőkártya száma és a kártyát kiállító tagállam,

— az ellenőrzés típusa (kijelzés és/vagy nyomtatás és/vagy a járműegységről való letöltés és/vagy kártyaletöltés [lásd megjegyzés]),

— a letöltött időszak letöltés esetén,

— a jármű rendszáma (VRN) és az ellenőrzött jármű nyilvántartásba vétele szerinti tagállam.

Megjegyzés: a biztonsági követelményekből eredően a kártya letöltése csak akkor kerül rögzítésre, ha ezt egy adatrögzítő készülék hajtja végre.

(300) A járművezetői kártyának egy ilyen rekord tárolására képesnek kell lennie.

4.5.3.2.14 A különleges körülményekre vonatkozó adatok

(301) A járművezetői kártyának tárolnia kell a különleges körülményekre vonatkozóan a kártya behelyezett állapotában bevitt adatokat (bármely kártyaolvasó egység esetében):

— az adatbevitel dátuma és időpontja,

— a különleges körülmény típusa.

(302) A járművezetői kártyának legalább 56 ilyen rekord tárolására képesnek kell lennie.

4.5.3.2.15 Az üzemeltetett járműegységek adatai

(303) A járművezetői kártyának az alábbi adatokat kell tárolnia a különböző olyan járműegységekkel kapcsolatban, amelyekben a kártyát használták:

— az a dátum és időpont, amikor a járműegység használati időszaka megkezdődött (azaz a járműegységbe való első kártyabehelyezés az adott időszakban),

— a járműegység gyártója,

— a járműegység típusa,

— a járműegység szoftververziójának száma,

(304) A járművezetői kártyának legalább 84 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.3.2.16 Azon helyek adatai, ahol a megszakítás nélküli járművezetési idő elérte a három órát

(305) A járművezetői kártyának az alábbi adatokat kell tárolnia a jármű azokban az időpontokban elért helyzetével kapcsolatban, amikor a járművezető megszakítás nélküli járművezetési ideje elérte a három óra többszörösét:

— az a dátum és időpont, amikor a kártyatulajdonos megszakítás nélküli járművezetési ideje eléri a három óra többszörösét,

— a jármű helyzete,

— a GNSS pontossága és a helyzet meghatározásának dátuma és időpontja.

(306) A járművezetői kártyának legalább 252 ilyen rekord tárolására képesnek kell lennie.

4.5.4 *Műhelykártya*

4.5.4.1 Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.4.1.1 Alkalmazásazonosító

(307) A műhelykártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.4.1.2 Kulcsok és tanúsítványok

(308) A műhelykártyának képesnek kell lennie egy sor, a 11. függelék A. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

(309) A műhelykártyának alkalmas kell lennie személyi azonosító szám tárolására (PIN kód).

4.5.4.1.3 A kártya azonosítása

(310) A műhelykártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata.

4.5.4.1.4 A kártyatulajdonos azonosítása

(311) A műhelykártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a műhely neve,

— a műhely címe,

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— választott nyelv.

4.5.4.1.5 Kártyaletöltés

(312) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a kártyaletöltési adatokat.

▼B

4.5.4.1.6 Kalibrálási és időbeállítási adatok

(313) A műhelykártyának meg kell őriznie a kalibrálási és/vagy időbeállítási rekordokat, mialatt a kártya be van helyezve az adatrögzítő készülékbe.

(314) Valamennyi kalibrálási rekordnak a következő adatokat kell magában foglalnia:

— a kalibrálás célja (aktiválás, első beépítés, beépítés, időszakos vizsgálat),

— a jármű azonosítása,

— aktualizált vagy megerősített paraméterek (w, k, l, abroncsméret, sebességkorlátozó készülék beállítása, kilométer-számláló [új és régi értékek], dátum és idő [új és régi értékek]),

— az adatrögzítő készülék azonosítása (a járműegység alkatrészeinek száma, a járműegység sorozatszáma, a mozgásérzékelő sorozatszáma).

(315) A műhelykártyának legalább 88 ilyen rekord tárolására képesnek kell lennie.

(316) A műhelykártyában lennie kell egy olyan számlálónak, amely jelzi a kártyával elvégzett kalibrálások számát.

(317) A műhelykártyában lennie kell egy olyan számlálónak, amely jelzi az utolsó letöltés óta elvégzett kalibrálások számát.

4.5.4.1.7 Az eseményekkel és a hibákkal kapcsolatos adatok

(318) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az eseményekkel és a hibákkal kapcsolatos adatrekordokat.

(319) A műhelykártyának minden eseménytípussal összefüggésben tárolnia kell a három legutóbbi eseményt (18 esemény), az egyes hibatípusok esetében pedig a hat legutóbbi hibát (12 hiba).

4.5.4.1.8 A járművezető tevékenységére vonatkozó adatok

(320) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a járművezető tevékenységére vonatkozó adatokat.

(321) A műhelykártyának a járművezető tevékenységére vonatkozó adatokat legalább egy napig tárolnia kell, átlagos járművezetői tevékenység mellett.

4.5.4.1.9 Az üzemeltetett járművek adatai

(322) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az üzemeltetett járművekre vonatkozó adatokat.

(323) A műhelykártyának legalább 4 ilyen rekord tárolására képesnek kell lennie.

4.5.4.1.10 A munkanapok kezdetére és/vagy végére vonatkozó adatok

(324) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a munkanapok kezdetére és/vagy végére vonatkozó adatokat.

(325) A műhelykártyának legalább 3 ilyen rekordpár tárolására képesnek kell lennie.

▼B

4.5.4.1.11 Kártyakapcsolati adatok

(326) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a kártyakapcsolati adatokat.

4.5.4.1.12 Az ellenőrzési tevékenységre vonatkozó adatok

(327) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az ellenőrző tevékenységi adatrekordokat.

4.5.4.1.13 A különleges körülményekre vonatkozó adatok

(328) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a különleges körülményekre vonatkozó adatokat.

(329) A műhelykártyának legalább 2 ilyen rekord tárolására képesnek kell lennie.

4.5.4.2 Második generációs tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.4.2.1 Alkalmazásazonosító

(330) A műhelykártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.4.2.2 Kulcsok és tanúsítványok

(331) A műhelykártyának képesnek kell lennie egy sor, a 11. függelék B. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

(332) A műhelykártyának alkalmas kell lennie személyi azonosító szám tárolására (PIN kód).

4.5.4.2.3 A kártya azonosítása

(333) A műhelykártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata.

4.5.4.2.4 A kártyatulajdonos azonosítása

(334) A műhelykártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a műhely neve,

— a műhely címe,

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— választott nyelv.

4.5.4.2.5 Kártyaletöltés

(335) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a kártyaletöltési adatokat.

▼B

4.5.4.2.6 Kalibrálási és időbeállítási adatok

(336) A műhelykártyának meg kell őriznie a kalibrálási és/vagy időbeállítási rekordokat, mialatt a kártya be van helyezve az adatrögzítő készülékbe.

(337) Valamennyi kalibrálási rekordnak a következő adatokat kell magában foglalnia:

— a kalibrálás célja (aktiválás, első beépítés, beépítés, időszakos vizsgálat),

— a jármű azonosítása,

— aktualizált vagy megerősített paraméterek (w, k, l, abroncsméret, sebességkorlátozó készülék beállítása, kilométer-számláló [új és régi értékek], dátum és idő [új és régi értékek]),

— az adatrögzítő készülék azonosítása (a járműegység alkatrészeinek száma, a járműegység sorozatszáma, a mozgásérzékelő sorozatszáma, a távoli kommunikációs eszköz sorozatszáma és a külső GNSS-eszköz sorozatszáma adott esetben),

— az összes elhelyezett plomba típusa és azonosítása,

— képes-e a járműegység első generációs tachográfkártyák használatára (aktiválva van-e ez a funkció, avagy sem).

(338) A műhelykártyának legalább 88 ilyen rekord tárolására képesnek kell lennie.

(339) A műhelykártyában lennie kell egy olyan számlálónak, amely jelzi a kártyával elvégzett kalibrálások számát.

(340) A műhelykártyában lennie kell egy olyan számlálónak, amely jelzi az utolsó letöltés óta elvégzett kalibrálások számát.

4.5.4.2.7 Az eseményekkel és a hibákkal kapcsolatos adatok

(341) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az eseményekkel és a hibákkal kapcsolatos adatrekordokat.

(342) A műhelykártyának minden eseménytípussal összefüggésben tárolnia kell a három legutóbbi eseményt (33 esemény), az egyes hibatípusok esetében pedig a hat legutóbbi hibát (12 hiba).

4.5.4.2.8 A járművezető tevékenységére vonatkozó adatok

(343) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a járművezető tevékenységére vonatkozó adatokat.

(344) A műhelykártyának a járművezető tevékenységére vonatkozó adatokat legalább egy napig tárolnia kell, átlagos járművezetői tevékenység mellett.

4.5.4.2.9 Az üzemeltetett járművek adatai

(345) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az üzemeltetett járművekre vonatkozó adatokat.

(346) A műhelykártyának legalább 4 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.4.2.10 A munkanapok kezdetére és/vagy végére vonatkozó adatok

(347) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a munkanapok kezdetére és/vagy végére vonatkozó adatokat.

(348) A műhelykártyának legalább 3 ilyen rekordpár tárolására képesnek kell lennie.

4.5.4.2.11 Kártyakapcsolati adatok

(349) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a kártyakapcsolati adatokat.

4.5.4.2.12 Az ellenőrzési tevékenységre vonatkozó adatok

(350) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia az ellenőrző tevékenységi adatrekordokat.

4.5.4.2.13 Az üzemeltetett járműegységek adatai

(351) A műhelykártyának az alábbi adatokat kell tárolnia a különböző olyan járműegységekkel kapcsolatban, amelyekben a kártyát használták:

— az a dátum és időpont, amikor a járműegység használati időszaka megkezdődött (azaz a járműegységbe való első kártyabehelyezés az adott időszakban),

— a járműegység gyártója,

— a járműegység típusa,

— a járműegység szoftververziójának száma,

(352) A műhelykártyának legalább 4 ilyen rekord tárolására képesnek kell lennie.

4.5.4.2.14 Azon helyek adatai, ahol a megszakítás nélküli járművezetési idő elérte a három órát

(353) A műhelykártyának az alábbi adatokat kell tárolnia a jármű azokban az időpontokban elért helyzetével kapcsolatban, amikor a járművezető megszakítás nélküli járművezetési ideje elérte a három óra többszörösét:

— az a dátum és időpont, amikor a kártyatulajdonos megszakítás nélküli járművezetési ideje eléri a három óra többszörösét,

— a jármű helyzete,

— a GNSS pontossága és a helyzet meghatározásának dátuma és időpontja.

(354) A műhelykártyának legalább 18 ilyen rekord tárolására képesnek kell lennie.

4.5.4.2.15 A különleges körülményekre vonatkozó adatok

(355) A műhelykártyának a járművezetői kártyával azonos módon kell tárolnia a különleges körülményekre vonatkozó adatokat.

(356) A műhelykártyának legalább 2 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.5 *Ellenőrzőkártya*

4.5.5.1 Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.5.1.1 Alkalmazásazonosító

(357) Az ellenőrzőkártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.5.1.2 Kulcsok és tanúsítványok

(358) Az ellenőrzőkártyának képesnek kell lennie egy sor, a 11. függelék A. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

4.5.5.1.3 A kártya azonosítása

(359) Az ellenőrzőkártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata (adott esetben).

4.5.5.1.4 A kártyatulajdonos azonosítása

(360) Az ellenőrzőkártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— ellenőrző szerv neve,

— az ellenőrző szerv címe,

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— választott nyelv.

4.5.5.1.5 Az ellenőrzési tevékenységre vonatkozó adatok

(361) Az ellenőrzőkártyának tárolnia kell az ellenőrző tevékenységre vonatkozó következő adatokat:

— az ellenőrzés dátuma és időpontja,

— az ellenőrzés típusa (kijelzés és/vagy nyomtatás és/vagy a járműegységről való letöltés és/vagy kártyaletöltés és/vagy közúti kalibrálási ellenőrzés),

— letöltött időszak (adott esetben),

— a jármű rendszáma (VRN) és az ellenőrzött jármű nyilvántartásba vétele szerinti tagállam hatósága,

— kártyaszám és az ellenőrzött járművezetői kártyát kiállító tagállam.

(362) Az ellenőrzőkártyának legalább 230 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.5.2 Második generációs (G2) tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.5.2.1 Alkalmazásazonosító

(363) Az ellenőrzőkártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.5.2.2 Kulcsok és tanúsítványok

(364) Az ellenőrzőkártyának képesnek kell lennie egy sor, a 11. függelék B. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

4.5.5.2.3 A kártya azonosítása

(365) Az ellenőrzőkártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata (adott esetben).

4.5.5.2.4 A kártyatulajdonos azonosítása

(366) Az ellenőrzőkártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— ellenőrző szerv neve,

— az ellenőrző szerv címe,

— a tulajdonos családi neve,

— a tulajdonos utóneve(i),

— választott nyelv.

4.5.5.2.5 Az ellenőrzési tevékenységre vonatkozó adatok

(367) Az ellenőrzőkártyának tárolnia kell az ellenőrző tevékenységre vonatkozó következő adatokat:

— az ellenőrzés dátuma és időpontja,

— az ellenőrzés típusa (kijelzés és/vagy nyomtatás és/vagy a járműegységről való letöltés és/vagy kártyaletöltés és/vagy közúti kalibrálási ellenőrzés),

— letöltött időszak (adott esetben),

— a jármű rendszáma (VRN) és az ellenőrzött jármű nyilvántartásba vétele szerinti tagállam hatósága,

— kártyaszám és az ellenőrzött járművezetői kártyát kiállító tagállam.

(368) Az ellenőrzőkártyának legalább 230 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.6 *Vállalkozáskártya*

4.5.6.1 Tachográf-alkalmazás (az első és második generációs járműegységek számára)

4.5.6.1.1 Alkalmazásazonosító

(369) A vállalkozáskártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.6.1.2 Kulcsok és tanúsítványok

(370) A vállalkozáskártyának képesnek kell lennie egy sor, a 11. függelék A. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

4.5.6.1.3 A kártya azonosítása

(371) A vállalkozáskártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata (adott esetben).

4.5.6.1.4 A kártyatulajdonos azonosítása

(372) A vállalkozáskártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a vállalkozás neve,

— a vállalkozás címe.

4.5.6.1.5 A vállalkozás tevékenységére vonatkozó adatok

(373) A vállalkozáskártyának tárolnia kell a vállalkozás tevékenységére vonatkozó következő adatokat:

— a tevékenység dátuma és időpontja,

— a tevékenység típusa (járműegység lezárása és/vagy kioldása és/vagy a járműegységről való letöltés és/vagy kártyaletöltés),

— letöltött időszak (adott esetben),

— a jármű rendszáma (VRN) és a jármű nyilvántartásba vétele szerinti tagállam hatósága,

— kártyaszám és a kártyát kiállító tagállam (kártyaletöltés esetén).

(374) A vállalkozáskártyának legalább 230 ilyen rekord tárolására képesnek kell lennie.

▼B

4.5.6.2 Második generációs (G2) tachográf-alkalmazás (az első generációs járműegységek számára nem elérhető)

4.5.6.2.1 Alkalmazásazonosító

(375) A vállalkozáskártyának a következő alkalmazásazonosító adatokat kell tárolnia:

— tachográfalkalmazás-azonosító,

— tachográfkártyatípus-azonosító.

4.5.6.2.2 Kulcsok és tanúsítványok

(376) A vállalkozáskártyának képesnek kell lennie egy sor, a 11. függelék B. részében meghatározott titkosítási kulcs és tanúsítvány tárolására.

4.5.6.2.3 A kártya azonosítása

(377) A vállalkozáskártyának a következő kártyaazonosító adatokat kell tárolnia:

— kártyaszám,

— a kiállító tagállam, a kiállító hatóság neve, a kiállítás dátuma,

— a kártya érvényességi idejének kezdete és lejárata (adott esetben).

4.5.6.2.4 A kártyatulajdonos azonosítása

(378) A vállalkozáskártyának a következő kártyatulajdonos-azonosító adatokat kell tárolnia:

— a vállalkozás neve,

— a vállalkozás címe.

4.5.6.2.5 A vállalkozás tevékenységére vonatkozó adatok

(379) A vállalkozáskártyának tárolnia kell a vállalkozás tevékenységére vonatkozó következő adatokat:

— a tevékenység dátuma és időpontja,

— a tevékenység típusa (járműegység lezárása és/vagy kioldása és/vagy a járműegységről való letöltés és/vagy kártyaletöltés),

— letöltött időszak (adott esetben),

— a jármű rendszáma (VRN) és a jármű nyilvántartásba vétele szerinti tagállam hatósága,

— kártyaszám és a kártyát kiállító tagállam (kártyaletöltés esetén).

(380) A vállalkozáskártyának legalább 230 ilyen rekord tárolására képesnek kell lennie.

5 AZ ADATRÖGZÍTŐ KÉSZÜLÉK BEÉPÍTÉSE

5.1 **Beépítés**

(381) Az új adatrögzítő készüléket nem aktivált állapotban kell a szerelők vagy a járműgyártók részére leszállítani, úgy, hogy a 3.21. szakaszban felsorolt összes kalibrálási paraméter a megfelelő és érvényes alapértelmezett értékre legyen beállítva. Ha nincsen meghatározott érték, a betűkkel leírt paramétereket „?” karakterláncokba kell rendezni, a numerikus paramétereket pedig „0”-ra kell állítani. Amennyiben a biztonsági tanúsítás során kérelmezik, az adatrögzítő készülék biztonsági vonatkozású részeinek átadása korlátozható.

▼B

(382) Aktiválása előtt az adatrögzítő készüléknek akkor is hozzáférést kell biztosítania a kalibrálási funkcióhoz, ha a készülék nem kalibrálási üzemmódban van.

(383) Az adatrögzítő készülék aktiválása előtt se nem rögzíti, se nem tárolja a 3.12.3., 3.12.9. és 3.12.12–3.12.15. szakaszban említett adatokat.

(384) A beépítés során a járműgyártónak valamennyi ismert paramétert előre be kell állítania.

(385) A járműgyártóknak vagy -szerelőknek a beépített adatrögzítő készüléket legkésőbb a jármű 561/2006/EK rendelet alkalmazási körében történő használatba vétele előtt aktiválniuk kell.

(386) Az adatrögzítő készülék automatikusan aktiválódik, amikor valamelyik kártyainterfész-eszközbe első alkalommal érvényes műhelykártyát helyeznek.

(387) A mozgásérzékelő és a járműegység között adott esetben szükséges egyedi párosítási műveletek elvégzésének automatikusan meg kell történnie az aktiválás előtt vagy ennek során.

(388) A külső GNSS-eszköz és a járműegység között adott esetben szükséges egyedi kapcsolódási műveletek elvégzésének hasonlóképpen automatikusan meg kell történnie az aktiválás előtt vagy ennek során.

(389) Az adatrögzítő készüléknek aktiválása után biztosítania kell, hogy funkciói működjenek, és az adathozzáférési jogok teljes mértékben érvényesüljenek.

(390) Az adatrögzítő készüléknek aktiválása után a célzott közúti ellenőrzésekhez szükséges biztosított adatokat továbbítania kell a távoli kommunikációs eszközhöz.

(391) Az adatrögzítő készülék rögzítő és tároló funkcióinak teljes mértékben működőképeseknek kell lenniük az aktiválás után.

(392) A beépítést követően kalibrálást kell végezni. Az első kalibrálás nem feltétlenül foglalja magában a rendszám (VRN) bevitelét, ha azt a kalibrálással megbízott jóváhagyott műhely nem ismeri. Ilyen esetben és csakis ekkor lehetséges, hogy a járműtulajdonos a járműnek az 561/2006/EK rendelet alkalmazási körében történő használatát megelőzően vállalkozáskártyáját használva (például a járműegység felhasználói/gépi interfész megfelelő menüstruktúrájában a megfelelő parancsok megadásával) vigye be a rendszámot (VRN) ([1]). A bevitt adat aktualizálása vagy megerősítése csak a műhelykártya felhasználásával lehetséges.

(393) A külső GNSS-eszköz beépítéséhez az eszközt csatlakoztatni a járműegységre, majd ellenőrizni kell a GNSS helyzetmeghatározási információit.

(394) Az adatrögzítő készüléket úgy kell elhelyezni a járműben, hogy a járművezető a vezetői ülésből hozzá tudjon férni a szükséges funkciókhoz.

([1]) HL L 102., 2006.4.11., 1. o.

▼B

5.2 **Illesztési címke**

(395) Miután az adatrögzítő készülék ellenőrzése a beépítés során megtörtént, egy gravírozással vagy tartós nyomtatással feliratozott illesztési címkét kell elhelyezni a készüléken, jól látható és könnyen hozzáférhető helyre. Amennyiben ez nem lehetséges, a címkét a jármű „B” oszlopán kell elhelyezni, jól látható helyre. Azokban a járművekben, amelyeknek nincsen „B” oszlopa, az illesztési címkét az ajtókereten kell elhelyezni a járművezetői oldalon, minden esetben jól látható helyre.

Jóváhagyott szerelő vagy műhely által végzett minden egyes ellenőrzés után új címkét kell elhelyezni az előző címke helyén

(396) A címkén legalább a következő adatokat fel kell tüntetni:

— az elismert szerelő vagy műhely neve, címe vagy kereskedelmi neve,

— a jármű jellemző együtthatója, „w = … imp/km” formában,

— az adatrögzítő készülék állandója, „k = … imp/km” formában,

— a gumiabroncsok tényleges kerülete, „l = … mm” formában,

— abroncsméret,

— az a dátum, amikor meghatározták jármű jellemző együtthatóját, és lemérték a gumiabroncsok kerületét,

— a jármű jármű-azonosító száma,

— külső GNSS-eszköz jelenléte vagy hiánya,

— a külső GNSS-eszköz sorozatszáma,

— a távoli kommunikációs eszköz sorozatszáma,

— az összes elhelyezett plomba sorozatszáma,

— a jármű azon része, amelybe adott esetben az adaptert beépítették,

— a jármű azon része, amelybe a mozgásérzékelőt beépítették, ha az nincs összekötve a sebességváltóval, illetve nem alkalmaznak adaptert,

— az adaptert és a járműnek az adapter bejövő impulzusait továbbító részét összekötő kábel színe,

— az adapterbe épített mozgásérzékelő sorozatszáma.

(397) Kizárólag az M1 és az N1 kategóriába tartozó, valamint a 68/2009/EK bizottsági rendelet ([1]) legutóbb módosított változatával összhangban adapterrel felszerelt járművek esetében, valamint amennyiben nem lehetséges minden szükséges, a 396. követelményben ismertetett információ feltüntetése, egy második, kiegészítő címke is alkalmazható. Ilyen esetekben a kiegészítő címkének a 396. követelmény legalább négy utolsó francia bekezdésben szereplő információkat tartalmaznia kell.

([1]) A Bizottság 2009. január 23-i 68/2009/EK rendelete a közúti közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendeletnek a műszaki fejlődésre figyelemmel történő kilencedik kiigazításáról (HL L 21., 2009.1.24., 3. o.).

▼B

Ha használnak ilyen második, kiegészítő címkét, akkor azt a 396. követelményben ismertetett első címke közvetlen közelében vagy mellett kell elhelyezni, és ugyanolyan védelemmel kell ellátni. A beépítést elvégző jóváhagyott szerelő vagy műhely nevét, címét vagy kereskedelmi nevét, valamint a beépítés dátumát a második címkén is fel kell tüntetni.

5.3 **Plombák**

(398) A következő alkatrészeket kell leplombálni:

— minden olyan csatlakozás, amely szétkapcsoláskor észlelhetetlen változásokat vagy észrevehetetlen adatvesztést okoz (ez például érvényes lehet a sebességváltóműre csatlakoztatott mozgásérzékelőre, az M1/N1 kategóriájú járművek adapterére, a külső GNSS-eszközre vagy a járműegységre),

— az illesztési címke, kivéve, ha az úgy van felerősítve, hogy a rajta lévő jelölések megrongálása nélkül nem távolítható el.

(399) A fent említett plombák a következő esetekben távolíthatók el:

— veszélyhelyzetben,

— a sebességkorlátozó készülék vagy bármely más, az útbiztonságot szolgáló eszköz beépítése, beállítása vagy javítása esetén, feltéve, hogy az adatrögzítő készülék megbízhatóan és pontosan működik továbbra is, és azt egy jóváhagyott szerelő vagy műhely (a 6. fejezettel összhangban) a sebességkorlátozó készülék vagy bármely más, az útbiztonságot szolgáló eszköz beépítése után közvetlenül, illetve más esetekben hét napon belül újra leplombálja.

(400) A plombák eltávolításakor minden egyes alkalommal írásbeli nyilatkozatot kell tenni arról, hogy miért került erre sor, amelyet az illetékes hatóságnak át kell adni.

(401) A plombáknak a gyártó által kiutalt azonosító számot kell viselniük. Ennek a számnak egyedinek és minden más plombagyártó által kiutalt plombaszámtól különbözőnek kell lennie.

Ezen egyedi azonosító szám formátuma a következő: MMNNNNNN eltávolíthatatlan módon feltüntetve; MM a gyártó egyedi azonosítója (a nyilvántartás kezelése az Európai Bizottság illetékességi körébe tartozik), az NNNNNN pedig a plomba alfanumerikus, a gyártó által kiadott számok körében egyedi szám.

(402) A plombákon helyet kell hagyni, ahová a jóváhagyott szerelők, műhelyek vagy járműgyártók a 165/2014/EU rendelet 22. cikkének (3) bekezdése szerinti speciális jelet helyezhetnek el.

Ez a jel nem takarhatja ki a plomba azonosító számát.

(403) A plombagyártókat nyilvántartásba kell venni egy külön erre a célra fenntartott adatbázisban, és plombaazonosító számaikat pedig közzé kell tenni egy olyan eljárással, amelyet az Európai Bizottság határoz meg.

(404) A jóváhagyott műhelyek és járműgyártók a 165/2014/EU rendelet keretében csak olyan plombákat használhatnak, amelyek a fent említett adatbázisban bejegyzett plombagyártóktól származnak.

▼B

(405) A plombák gyártóinak és forgalmazóinak hiánytalan nyomonkövethetőségi nyilvántartást kell vezetniük a 165/2014/EU rendelet keretében történő felhasználás céljára eladott plombákról, és készen kell állniuk arra, hogy szükség esetén bármikor bemutassák ezt az illetékes nemzeti hatóságnak.

(406) A plomba egyedi azonosító számának láthatónak kell lennie az illesztési címkén.

6 ELLENŐRZÉSEK, VIZSGÁLATOK ÉS JAVÍTÁSOK

E melléklet 5.3. szakasza meghatározza azokat a követelményeket, amelyek a plombák eltávolításának azon körülményeire vonatkoznak, melyeket a 165/2014/EU rendelet 22. cikkének (5) bekezdése említ.

6.1 **Szerelők, műhelyek és járműgyártók jóváhagyása**

A tagállamoknak jóvá kell hagyniuk, rendszeresen ellenőrizniük kell és tanúsítaniuk kell a következő feladatokért felelős szerveket:

— beépítések,

— ellenőrzések,

— vizsgálatok,

— javítások.

Műhelykártyák megfelelő indoklás hiányában e melléklet szerint csak az adatrögzítő készülékek aktiválására, illetve kalibrálására feljogosított olyan szerelőknek és/vagy műhelyeknek adhatók ki:

— akik nem jogosultak vállalkozáskártya használatára,

— és akik egyéb szakmai tevékenysége nem jelent potenciális veszélyt a rendszer 10. függelékben előírt általános biztonságára.

6.2 **Új vagy javított készülékek ellenőrzése**

(407) Minden egyes eszköz esetében – akár új, akár javított – ellenőrizni kell az 5.3. szakasz szerinti plombázás és kalibrálás révén, hogy a 3.2.1., 3.2.2., 3.2.3. és 3.3. szakaszban megállapított határokon belül megfelelően működik-e, és leolvasásai és a rögzített adatok tekintetében pontos-e.

6.3 **A beépítés vizsgálata**

(408) A járműbe beépítve a berendezés egészének (beleértve az adatrögzítő készüléket) meg kell felelnie a 3.2.1., 3.2.2., 3.2.3. és 3.3. szakaszban megállapított megengedhető tűréshatárokra vonatkozó előírásoknak.

6.4 **Időszakos vizsgálatok**

(409) A járműbe szerelt berendezések bármilyen javítását követően, a jármű jellemző együtthatójának vagy a gumiabroncsok tényleges kerületének megváltozása után, valamint ha a berendezés UTC ideje több mint 20 perccel eltér a pontos időtől, vagy ha a rendszám megváltozott, de az utolsó vizsgálattól számítva legalább kétévenként (24 hónap) egyszer a járművekbe beépített berendezések időszakos vizsgálatára kerül sor.

(410) E vizsgálatok a következők ellenőrzését foglalják magukban:

— az adatrögzítő készülék megfelelő működése, ideértve az adattárolási funkciót a tachográfkártyákon és a távoli kommunikációs leolvasókkal való kommunikációt,

▼B

— a 3.2.1. és 3.2.2. szakasz rendelkezéseit betartják a beépítésre vonatkozó megengedhető tűréshatár tekintetében,

— a 3.2.3. és 3.3. szakasz rendelkezéseit betartják,

— az adatrögzítő készüléken szerepel-e a típus-jóváhagyási jel,

— a 396. követelményben meghatározott illesztési címke, valamint a 225. követelményben meghatározott ismertető címke fel van erősítve,

— az abroncsok mérete és tényleges kerülete,

— a készülékhez nem csatlakozik manipulációs eszköz,

— a plombák a megfelelő helyen és jó állapotban vannak, és érvényes azonosító számmal rendelkeznek (a plombagyártó szerepel a Bizottság nyilvántartásában), valamint azonosító számaik megfelelnek az illesztési címkén olvasható jelöléseknek (lásd a 401. követelményt).

(411) Amennyiben megállapítást nyer, hogy a 3.9. szakaszban („Események és/vagy hibák észlelése”) felsorolt események valamelyike előfordult az utolsó ellenőrzés óta, és a menetíró készülék gyártója és/vagy a nemzeti hatóságok úgy vélik, hogy ez potenciális kockázatot jelenthet a készülék biztonsága szempontjából, a műhely köteles a következő tevékenységeket elvégezni:

a. összehasonlítja a sebességváltóhoz csatlakoztatott mozgásérzékelő azonosításai adatait a párosított mozgásérzékelőnek a járműegységben feljegyzett azonosítási adataival,

b. ellenőrzi, hogy az illesztési címkén feltüntetett információ egyezik-e a járműegység adatrekordjában szereplő információval,

c. ellenőrzi, hogy a mozgásérzékelő sorozatszáma és jóváhagyási száma – amennyiben ezek rá vannak nyomtatva a mozgásérzékelőre – megegyezik-e az adatrögzítő készülék adatmemóriájában tárolt információkkal,

d. összehasonlítja adott esetben a külső GNSS-eszköz ismertető címkéjén feltüntetett azonosítási adatokat a járműegység adatmemóriájában tárolt adatokkal.

(412) A műhelyeknek a vizsgálati jelentéseikben nyilván kell tartaniuk, ha sérült plombákat találtak, vagy manipulációs eszközöket fedeztek fel. E jelentéseket legalább két évig meg kell őrizniük, és kérésre bármikor az illetékes hatóság rendelkezésére kell bocsátaniuk őket.

(413) A vizsgálatok során kalibrálást is kell végezni, és megelőző jelleggel le kell cserélni azokat a plombákat, amelyek elhelyezéséért az adott műhely felel..

6.5 **A hibák mérése**

(414) A hibamérést a beépítés alatt és a használat folyamán az alábbi feltételek mellett kell végrehajtani, mely feltételeket szabványosított tesztfeltételeknek kell tekintetni:

— terheletlen jármű a szokásos menetkész állapotban,

— gumiabroncsnyomás a gyártó előírásai szerint,

▼B

— gumiabroncskopás a nemzeti jog által megengedett határokon belül,

— a jármű mozgása:

— a járműnek saját motorerejével egyenes vonalban, sík terepen, 50 ± 5 km/h sebességgel kell előrehaladnia. A mérési távolság legalább 1 km.

— a vizsgálat alternatív módszerekkel, azaz például egy megfelelő próbapadon is elvégezhető, ha e módszer összevethető pontosságot nyújt.

6.6 **Javítások**

(415) A műhelyeknek képesnek kell lenniük arra, hogy az adatrögzítő készülékről adatokat töltsenek le, hogy azután azokat visszaszolgáltassák az érintett fuvarozási vállalkozásnak.

(416) Amennyiben a korábban rögzített adatok letöltése nem lehetséges, mégpedig annak ellenére sem, hogy a műhely megjavította az adatrögzítő készüléket, a jóváhagyott műhelynek igazolást kell kiállítania a fuvarozási vállalkozások részére az adatok letölthetetlenségéről. A műhelyek minden kiállított igazolás egy másolatát kötelesek legalább egy évig megőrizni.

7 KÁRTYAKIBOCSÁTÁS

A tagállamok által bevezetett kártyakibocsátási eljárásoknak meg kell felelniük az alábbiaknak:

(417) A valamely kérelmező részére első alkalommal kibocsátott tachográfkártya száma egy konszekutív indexszel (adott esetben), egy csereindexszel és egy „0”-ról induló megújítási indexszel rendelkezik.

(418) Az ugyanazon ellenőrző szerv, ugyanazon műhely vagy ugyanazon fuvarozási vállalkozás számára kibocsátott, nem személyhez kötött tachográfkártyák kártyaszámai ugyanazzal a 13 számjeggyel kezdődnek, de különböző konszekutív indexszel rendelkeznek.

(419) A meglévő tachográfkártya cseréjeként kibocsátott tachográfkártya számának meg kell egyeznie a lecserélt kártya számával, a csereindex kivételével, amelyet egy egységgel kell megnövelni (sorrendben 0, …, 9, A, …, Z).

(420) A meglévő tachográfkártya cseréjeként kibocsátott tachográfkártya érvényességi idejének meg kell egyeznie a lecserélt kártya érvényességi idejével.

(421) Egy meglévő tachográfkártya megújításaként kibocsátott tachográfkártya számának meg kell egyeznie a megújított kártya számával, a csereindex kivételével, amelyet „0”-ra kell visszaállítani, és a megújítási index kivételével, amelyet egy egységgel kell megnövelni (sorrendben 0, …, 9, A, …, Z).

(422) Egy meglévő tachográfkártya adminisztratív adatok módosítása céljából történő cseréje a megújítás szabályait követi, ha a csere ugyanabban a tagállamban történik, vagy az első kibocsátás szabályait követi, ha a cserére egy másik tagállamban kerül sor.

(423) A nem személyre szóló műhely- vagy ellenőrzőkártyákon „A kártyatulajdonos családi neve” rovatot a műhely vagy az ellenőrző szerv nevével, illetve ha a tagállamok úgy döntenek, a szerelő vagy az ellenőrző tisztviselő nevével kell kitölteni.

▼B

(424) A tagállamoknak a 165/2014/EU rendelet 31. cikkének megfelelően elektronikus adatcserét kell folytatniuk annak érdekében, hogy az általuk kibocsátott járművezetői kártyák egyedisége biztosított legyen.

8 AZ ADATRÖGZÍTŐ KÉSZÜLÉKEK ÉS A TACHOGRÁFKÁRTYÁK TÍPUSJÓVÁHAGYÁSA

8.1 **Általános szempontok**

E szakasz alkalmazásában az „adatrögzítő készülék” meghatározás az „adatrögzítő készülék vagy alkatrészei” fogalmát jelenti. A mozgásérzékelőt a járműegységgel, a külső GNSS-eszközt a járműegységgel, valamint a távoli kommunikációs eszközt a járműegységgel összekötő kábel(ek) típusjóváhagyása nem szükséges. Az adatrögzítő készülék által használt papírt az adatrögzítő készülék alkatrészének kell tekinteni.

A gyártók kérhetik, hogy az általuk gyártott alkatrészek jóváhagyása a mozgásérzékelők vagy a külső GNSS-eszközök bármilyen típusával együtt történjen, és fordítva, feltéve, hogy minden egyes alkatrész megfelel e melléklet követelményeinek. A gyártók az adatrögzítő készülék típusjóváhagyását is kérelmezhetik.

(425) Az adatrögzítő készüléket valamennyi integrált kiegészítő készülékével együtt kell jóváhagyásra benyújtani.

(426) Az adatrögzítő készülék és a tachográfkártyák típusjóváhagyása során biztonsági, működési és interoperabilitási teszteket is végeznek. Ha e vizsgálatok kedvező eredménnyel zárulnak, arról megfelelő tanúsítványt kell kiállítani.

(427) A tagállamok típusjóváhagyó hatóságai mindaddig nem adnak ki típusbizonyítványt, amíg számukra át nem nyújtják az azon adatrögzítő készülékre és tachográfkártyára vonatkozó:

— biztonsági tanúsítványt,

— működési tanúsítványt,

— valamint interoperabilitási tanúsítványt,

amelyre a típus-jóváhagyási kérelmet benyújtották.

(428) A készülék szoftverében, hardverében és a gyártásához felhasznált anyagok jellegét illetően végzett minden módosítást még a felhasználás előtt be kell jelenteni azon hatóságnak, amely a készüléket típusjóváhagyásban részesítette. E hatóság visszaigazolja a gyártó felé a típusjóváhagyás kiterjesztését, vagy kérheti a vonatkozó működési, biztonsági és/vagy interoperabilitási aktualizálását vagy megerősítését.

(429) A már beépített adatrögzítő készülék szoftverfrissítési eljárásait azon hatósághoz kell jóváhagyásra benyújtani, amely a készüléket típusjóváhagyásban részesítette. A szoftverfrissítés nem módosíthat vagy törölhet az adatrögzítő készülékben a járművezetői tevékenységre vonatkozóan tárolt egyetlen adatot sem. A szoftvert csak a készülék gyártójának felelősségére lehet frissíteni.

(430) Az előzőleg típusjóváhagyásban részesített adatrögzítő készülék frissítésére irányuló szoftvermódosítások típusjóváhagyása nem utasítható el, ha a szóban forgó módosítások csakis olyan funkciókat érintenek, amelyekre e melléklet nem tér ki. Az adatrögzítő készülék szoftverfrissítése kizárhatja új karakterkészletek bevezetését, amennyiben ez technikailag kivitelezhetetlen.

▼B

8.2 **Biztonsági tanúsítvány**

(431) A biztonsági tanúsítványt e melléklet 10. függelékének rendelkezéseivel összhangban kell kiállítani. Az adatrögzítő készülékek tanúsítandó alkatrészei a járműegység, a mozgásérzékelő, a külső GNSS-eszköz és a tachográfkártyák.

(432) Kivételes körülmények között, amikor a biztonsági tanúsítást végző hatóságok a biztonsági mechanizmusok elavultsága miatt megtagadják az új készülék tanúsítását, a típusjóváhagyást kizárólag ebben a konkrét és kivételes esetben továbbra is megadják, amennyiben nincs a rendeletnek megfelelő alternatív megoldás.

(433) Ebben az esetben az érintett tagállamnak haladéktalanul tájékoztatnia kell az Európai Bizottságot, amely a típusjóváhagyás megadásától számított tizenkét naptári hónapon belül intézkedni kezd annak érdekében, hogy az eredeti biztonsági szint helyreálljon.

8.3 **Működési tanúsítvány**

(434) Minden típusjóváhagyást kérelmező személynek a tagállami jóváhagyó hatóságok rendelkezésére kell bocsátania minden olyan anyagot és dokumentumot, amelyet a hatóság szükségesnek talál.

(435) A gyártóknak a kérelem benyújtásától számított egy hónapon belül át kell adniuk a működési tesztek elvégzésére kijelölt laboratóriumok által kért, a típusjóváhagyásra jelölt termékek megfelelő mintáit és a kapcsolódó dokumentációt. A kérelemmel kapcsolatos minden költséget a kérelmezőnek kell viselnie. A laboratóriumoknak az üzleti szempontból érzékeny információkat bizalmasan kell kezelniük.

(436) A működési tanúsítványt csak a legalább a 9. függelékben meghatározott valamennyi működési teszt sikeres elvégzése után lehet kiadni a gyártónak.

(437) A működési tanúsítványt a típusjóváhagyó hatóság állítja ki. E tanúsítványnak – a kedvezményezett neve és a modell azonosítása mellett – részletesen fel kell sorolnia az elvégzett teszteket azok eredményeivel együtt.

(438) Az adatrögzítő készülékek bármely alkatrészének működési tanúsítványában fel kell tüntetni az adatrögzítő készülék összes többi, típusjóváhagyással rendelkező kompatibilis alkatrészének típus-jóváhagyási számát is, amelyeket szintén teszteltek a tanúsítás céljára.

(439) Minden adatrögzítő készülék működési tanúsítványában meg kell adni azt az ISO- vagy CEN-szabványt is, amely alapján a működési interfészt tanúsították.

8.4 **Interoperabilitási tanúsítvány**

(440) Az interoperabilitási teszteket egyetlen, az Európai Bizottság hatáskörébe és felelőssége alá tartozó laboratórium végzi.

(441) A laboratóriumnak a gyártók által benyújtott, interoperabilitási tesztekre irányuló kérelmeket beérkezésük sorrendjében kell nyilvántartásba vennie.

(442) A kérelem csak akkor kerül be hivatalosan a nyilvántartásba, ha a laboratórium birtokába kerül:

— az említett interoperabilitási tesztek végrehajtásához szükséges összes anyag és dokumentáció,

▼B

— a megfelelő biztonsági tanúsítvány,

— a megfelelő működési tanúsítvány.

A kérelem nyilvántartásba vételének dátumáról a gyártót értesíteni kell.

(443) A laboratórium nem végezhet interoperabilitási teszteket azon adatrögzítő készülékeken és tachográfkártyákon, amelyek részére nem adtak ki biztonsági tanúsítványt és működési tanúsítványt, kivéve a 432. követelményben ismertetett kivételes körülmények között.

(444) Az interoperabilitási tesztek végzését kérelmező gyártóknak vállalniuk kell, hogy az ezeket a teszteket végző laboratóriumnak hiánytalanul átadják az összes anyagot és dokumentációt, amelyet a tesztek elvégzéséhez rendelkezésre bocsátottak.

(445) Az interoperabilitási teszteket e melléklet 9. függelékének rendelkezéseivel összhangban kell végrehajtani valamennyi olyan típusú adatrögzítő készülék és tachográfkártya tekintetében:

— amelyek típusjóváhagyása még érvényben van, vagy

— amelyek típusjóváhagyása már folyamatban van, és érvényes interoperabilitási tanúsítvánnyal rendelkeznek.

(446) Az interoperabilitási teszteknek ki kell terjedniük a használatban lévő adatrögzítő készülékek és tachográfkártyák valamennyi generációjára.

(447) A laboratórium csak akkor állítja ki a gyártó részére az interoperabilitási tanúsítványt, ha a megkívánt interoperabilitási tesztek mindegyike sikeresen zárult.

(448) Ha az interoperabilitási tesztek egy vagy több adatrögzítő készülék vagy tachográfkártya esetében sikertelenek, az interoperabilitási tanúsítvány nem állítható ki mindaddig, amíg a kérelmező gyártó nem hajtotta végre a szükséges módosításokat, és az interoperabilitási tesztek sikerrel nem zárulnak. A laboratórium az interoperabilitási hiba által érintett gyártók segítségével felderíti a probléma okát, és segíti a kérelmező gyártónak megtalálni a megfelelő műszaki megoldást. Amennyiben a gyártó módosította a terméket, az ő felelőssége tisztázni az illetékes hatóságokkal, hogy a biztonsági tanúsítvány és a működési tanúsítvány még érvényes-e.

(449) Az interoperabilitási tanúsítvány hat hónapig érvényes. Ezen időszak lejártával vissza kell vonni, ha a gyártó nem kapta meg a megfelelő típusbizonyítványt. Az interoperabilitási tanúsítványt a gyártó továbbítja a tagállam azon jóváhagyó hatóságának, amelyik a működési tanúsítványt kiállította.

(450) Azokat az elemeket, amelyek esetleg az interoperabilitási hiba hátterében állnak, tilos profitszerzésre vagy erőfölényes helyzet kialakítására felhasználni.

8.5 **Típusbizonyítvány**

(451) Amint a tagállam típusjóváhagyó hatósága kézhez vette a három szükséges tanúsítványt, kiállíthatja típusbizonyítványt.

▼B

(452) Az adatrögzítő készülék bármely alkatrészének típusbizonyítványában fel kell tüntetni az adatrögzítő készülék összes többi, típusjóváhagyással rendelkező interoperábilis alkatrészének típus-jóváhagyási számát is.

(453) A típusjóváhagyó hatóság a típusbizonyítvány gyártó részére történő kiállításával egyidejűleg köteles másolatot küldeni az interoperabilitási tesztek végrehajtásával megbízott laboratóriumnak.

(454) Az interoperabilitási tesztek elvégzéséért felelős laboratóriumnak nyilvános weboldalt kell fenntartania, amelyen folyamatosan frissíti azon adatrögzítőkészülék- és tachográfkártya-modellek listáját:

— amelyek tekintetében már nyilvántartásba vették az interoperabilitási tesztek elvégzésére irányuló kérelmet,

— amelyek interoperabilitási tanúsítványt kaptak (akár ideiglenes tanúsítványt is),

— amelyek típusbizonyítványt kaptak.

8.6 **Különleges eljárás: első interoperabilitási tanúsítványok második generációs adatrögzítő készülékek és tachográfkártyák számára**

(455) Egy második generációs adatrögzítő készülékből és egy második generációs tachográfkártyából (járművezetői, műhely-, ellenőrző-, és vállalkozáskártyák) álló első páros interoperábilissá nyilvánítását követő négy hónapban bármely ezen időszakban nyilvántartásba vett kérelemre kiállított interoperabilitási tanúsítványt (az első tanúsítványokat is) ideiglenesnek kell tekinteni.

(456) Ha ezen időszak végén valamennyi érintett termék interoperábilisnak bizonyul, az összes vonatkozó interoperabilitási tanúsítvány véglegessé válik.

(457) Ha az időszak alatt interoperabilitási hibák merülnek fel, az interoperabilitási tesztekkel megbízott laboratóriumnak azonosítania kell a problémák okait az összes érintett gyártó segítségével, és fel kell szólítania őket a szükséges módosítások végrehajtására.

(458) Ha ezen időszak végén továbbra is interoperabilitási problémák állnak fenn, az interoperabilitási tesztekkel megbízott laboratóriumnak az érintett gyártók és a típusjóváhagyó hatóságok közreműködésével fel kell derítenie az interoperabilitási hibák okait, és meg kell állapítania, hogy az érintett gyártóknak milyen módosításokat kell végrehajtaniuk. A műszaki megoldások keresése legfeljebb két hónapig tarthat, mely időszak lejárta után közös megoldás hiányában a Bizottság az interoperabilitási tesztekkel megbízott laboratóriummal való konzultációt követően eldönti, hogy mely készülék(ek) és kártyák kapnak végleges interoperabilitási tanúsítványt, és megindokolja döntését.

(459) Minden olyan interoperabilitási tesztre irányuló kérelmet, amelyet a laboratórium az első ideiglenes interoperabilitási tanúsítvány kiadása utáni négy hónapos időszak vége és a 455. követelményben említett bizottsági határozat dátuma között vett nyilvántartásba, félre kell tenni mindaddig, amíg az eredeti interoperabilitási problémák meg nem oldódnak. A kérelmeket a későbbiekben nyilvántartásba vételük sorrendjében kell feldolgozni.

▼B

1. függelék

ADATSZÓTÁR

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. Az adattípusok meghatározásának megközelítése

1.2. Hivatkozások

2. AZ ADATTÍPUSOK MEGHATÁROZÁSAI

2.1. ActivityChangeInfo

2.2. Address

2.3. AESKey

2.4. AES128Key

2.5. AES192Key

2.6. AES256Key

2.7. BCDString

2.8. CalibrationPurpose

2.9. CardActivityDailyRecord

2.10. CardActivityLengthRange

2.11. CardApprovalNumber

2.12. CardCertificate

2.13. CardChipIdentification

2.14. CardConsecutiveIndex

2.15. CardControlActivityDataRecord

2.16. CardCurrentUse

2.17. CardDriverActivity

2.18. CardDrivingLicenceInformation

2.19. CardEventData

2.20. CardEventRecord

2.21. CardFaultData

2.22. CardFaultRecord

2.23. CardIccIdentification

2.24. CardIdentification

2.25. CardMACertificate

2.26. CardNumber

2.27. CardPlaceDailyWorkPeriod

2.28. CardPrivateKey

2.29. CardPublicKey

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificate

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distance

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Name

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Speed

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

2.241. VuPowerSupplyInterruptionRecordArray

2.242. VuSensorExternalGNSSCoupledRecordArray

2.243. VuSensorPairedRecordArray

3. ÉRTÉK- ÉS MÉRETTARTOMÁNY-MEGHATÁROZÁSOK

4. KARAKTERKÉSZLETEK

5. KÓDOLÁS

6. OBJEKTUMAZONOSÍTÓK ÉS ALKALMAZÁSAZONOSÍTÓK

6.1. Objektumazonosítók

6.2. Alkalmazásazonosítók

1. BEVEZETÉS

Ez a függelék az adatrögzítő készülékben és a tachográfkártyákon alkalmazandó adatformátumokat, adatelemeket és adatszerkezeteket határozza meg.

1.1. **Az adattípusok meghatározásának megközelítése**

Ez a függelék az adattípusok meghatározásához az 1. számú absztrakt szintaxisjelölést alkalmazza. Ez egyszerű és strukturált adatok definiálását teszi lehetővé anélkül, hogy maga után vonna valamilyen meghatározott átviteli szintaxist (kódolási szabályt), amely szükségszerűen alkalmazás- és környezetfüggő lenne.

Az ASN.1 típusú elnevezési szabályok összhangban vannak az ISO/IEC 8824-1 szabvánnyal. Ebből adódóan:

— amennyiben lehetséges, az adattípus jelentését magukban foglalják a kiválasztott nevek,

— amennyiben az adattípus egyéb adattípusokból tevődik össze, az adattípus elnevezése még mindig egyetlen alfabetikus karaktersorozat, amely nagybetűvel kezdődik, ugyanakkor a megfelelő jelentés megadása érdekében a néven belül alkalmaznak nagybetűket,

— általános szabályként az adattípusok elnevezései összefüggnek azon adattípusok nevével, amelyekből felépülnek, azon készülékkel, amelyben az adatokat tárolják, illetve az adatokkal összefüggő funkcióval.

Amennyiben egy ASN.1 típust egy másik szabvány részeként már meghatároztak, és az lényeges az adatrögzítő készülékben való felhasználás szempontjából, úgy ezen ASN.1 típust ebben a függelékben definiálni kell.

Annak érdekében, hogy a különböző kódolási szabályokat lehessen alkalmazni, ebben a függelékben néhány ASN.1 típust értéktartomány-azonosítóval kell korlátozni. Az értéktartomány-azonosítók meghatározását a 3. szakasz és a 2. függelék tartalmazza.

1.2. **Hivatkozások**

Ebben a függelékben a következő hivatkozások jelennek meg:

ISO 639	A nyelvek neveinek jelölésére alkalmazott kód. Első kiadás: 1988.

▼B

ISO 3166	Országok és igazgatási egységeik nevének kódjai. 1. rész: Országkódok, 2013.
ISO 3779	Közúti járművek. A jármű alvázszáma (VIN). Tartalom és felépítés. 2009.
ISO/IEC 7816-5	Azonosító kártyák. Integrált áramkörös kártyák. 5. rész: Az alkalmazásszolgáltatók nyilvántartásba vétele. Második kiadás: 2004.
ISO/IEC 7816-6	Azonosító kártyák. Integrált áramkörös kártyák. 6. rész: Ágazatközi adatelemek a cseréhez, 2004 + 1. technikai helyesbítés: 2006.
ISO/IEC 8824-1	Információtechnológia. Az 1. számú absztrakt szintaxisjelölés (ASN.1): Az alapvető jelölési rendszer meghatározása. 2008 + 1. technikai helyesbítés: 2012 és 2. technikai helyesbítés: 2014.
ISO/IEC 8825-2	Információtechnológia. ASN.1 kódolási szabályok: A csomagolt kódolási szabályok (PER) meghatározása. 2008.
ISO/IEC 8859-1	Információtechnológia. 8 bites egyetlen bájtos kódolt grafikus karakterkészletek. 1. rész: 1. latin ábécé. Első kiadás: 1998.
ISO/IEC 8859-7	Információtechnológia. 8 bites egyetlen bájtos kódolt grafikus karakterkészletek. 7. rész: Latin/görög ábécé. 2003.
ISO 16844-3	Közúti járművek. Tachográf rendszerek. Mozgásérzékelő-interfész. 2004 + 1. technikai helyesbítés: 2006.
TR-03110-3	BSI / ANSSI TR-03110-3 számú műszaki iránymutatás: Fejlett biztonsági mechanizmusok géppel olvasható úti okmányokhoz és eIDAS-tokenhez. 3. rész: Egységes előírások, 2.20. verzió, 2015. február. 3.

2. AZ ADATTÍPUSOK MEGHATÁROZÁSAI

A következő adattípusok bármelyike esetében egy „ismeretlen” vagy „nem alkalmazható” tartalomnak megfelelő alapértelmezett érték az adatelem „FF” bájtokkal történő kitöltéséből áll.

Ellenkező értelmű jelzés hiányában valamennyi adattípus felhasználásra kerül mind az 1. generációs, mind a 2. generációs alkalmazásokban.

2.1. **ActivityChangeInfo**

Ezzel az adattípussal egy kétbájtos szóba be lehet kódolni a kártyaolvasó egység 00 óra 00 perckori állapotát és/vagy a járművezető 00 óra 00 perckori állapotát és/vagy egy járművezető vagy járműkísérő tevékenységváltásait és/vagy járművezetésiállapot-váltásait és/vagy kártyaállapot-váltásait. Ez az adattípus az 1C melléklet 105., 266., 291., 320., 321., 343. és 344. követelményével függ össze.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Érték-hozzárendelés – Rendezett oktett: ‘scpaatttttttttt’B (16 bit)

Az adatmemória-rögzítések (vagy a kártyaolvasó egység állapota) esetében:

‘s’B	Kártyaolvasó egység: ‘0’B: JÁRMŰVEZETŐ, ‘1’B: JÁRMŰKÍSÉRŐ,

▼B

‘c’B	Járművezetési állapot:
	‘0’B: EGYEDÜLI,
	‘1’B: SZEMÉLYZET,
‘p’B	Járművezetői (vagy műhely-) kártya állapota a megfelelő kártyaolvasó egységben:
	‘0’B: BEHELYEZVE, egy kártyát behelyeztek,
	‘1’B: NINCS BEHELYEZVE, nem helyeztek be kártyát (vagy a kártyát kivették),
‘aa’B	Tevékenység:
	‘00’B: SZÜNET/PIHENÉS,
	‘01’B: KÉSZENLÉT,
	‘10’B: MUNKA,
	‘11’B: JÁRMŰVEZETÉS,
‘ttttttttttt’B	A váltás ideje: Az adott napon 00 óra 00 perc óta eltelt percek száma.

A járművezetői (vagy műhely-) kártya rögzítései (és a járművezető állapota) esetében:

‘s’B	Kártyaolvasó egység (nem lényeges, ha ‘p’ = 1, kivéve az alábbi megjegyzésben szereplő esetben):
	‘0’B: JÁRMŰVEZETŐ,
	‘1’B: JÁRMŰKÍSÉRŐ,
‘c’B	Járművezetési állapot (‘p’ = 0 esete) vagy
	Következő tevékenység állapota (‘p’ = 1 esete):
	‘0’B: EGYEDÜLI,
	‘0’B: ISMERETLEN
	‘1’B: SZEMÉLYZET,
	‘1’B: ISMERT (= kézi betáplálás)
‘p’B	Kártyaállapot:
	‘0’B: BEHELYEZVE, a kártyát behelyezték az adatrögzítő készülékbe,
	‘1’B: NINCS BEHELYEZVE, a kártyát nem helyezték be (vagy a kártyát kivették),
‘aa’B	Tevékenység (nem lényeges, ha ‘p’ = 1 és ‘c’ = 0, kivéve az alábbi megjegyzésben szereplő esetben):
	‘00’B: SZÜNET/PIHENÉS,
	‘01’B: KÉSZENLÉT,
	‘10’B: MUNKA,
	‘11’B: JÁRMŰVEZETÉS,
‘ttttttttttt’B	A váltás ideje: Az adott napon 00 óra 00 perc óta eltelt percek száma.

▼B

Megjegyzés a „kártyakivétel” esetére:

A kártya kivételekor:

— ‘s’ alkalmazható és azon kártyaolvasó egységet jelzi, amelyből a kártyát kivették,

— ‘c’-t 0-ra kell beállítani,

— ‘p’-t 1-re kell beállítani,

— ‘aa’ az ekkor kiválasztott folyó tevékenység kódját kell, hogy tartalmazza,

Kézi betáplálás eredményeként a (kártyán eltárolt) szó ‘c’ és ‘aa’ bitjei később a betáplálásra tekintettel átírásra kerülhetnek.

2.2. **Address**

Egy cím.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage a 4. fejezetben meghatározott karakterkészletet adja meg,

address a meghatározott karakterkészlet felhasználásával kódolt cím.

2.3. **AESKey**

2. generáció:

Egy 128, 192 vagy 256 bit hosszúságú AES kulcs.

```
AESKey ::= CHOICE {
   aes128Key                             AES128Key,
   aes192Key                             AES192Key,
   aes256Key                             AES256Key
}
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.4. **AES128Key**

2. generáció:

Egy AES128 kulcs.

```
AES128Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes128Key                             OCTET STRING (SIZE(16))
}
```

length az AES128 kulcs hosszát jelöli oktettben.

aes128Key egy 128 bit hosszúságú AES kulcs.

Érték-hozzárendelés:

A hosszúság értékének 16-nak kell lennie.

▼B

2.5. **AES192Key**

2. generáció:

Egy AES192 kulcs.

```
AES192Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes192Key                           OCTET STRING (SIZE(24))
}
```

length az AES192 kulcs hosszát jelöli oktettben.

aes192Key egy 192 bit hosszúságú AES kulcs.

Érték-hozzárendelés:

A hosszúság értékének 24-nek kell lennie.

2.6. **AES256Key**

2. generáció:

Egy AES256 kulcs.

```
AES256Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes256Key                           OCTET STRING (SIZE(32))
}
```

length az AES256 kulcs hosszát jelöli oktettben.

aes256Key egy 256 bit hosszúságú AES kulcs.

Érték-hozzárendelés:

A hosszúság értékének 32-nek kell lennie.

2.7. **BCDString**

A BCDString-et (BCD karaktersorozat) a binárisan kódolt decimális szám – Binary Code Decimal (BCD) – megjelenítésére kell alkalmazni. Ez az adattípus egy decimális számjegynek egy fél oktettel (4 bittel) való megjelenítésére szolgál. A BCDString az ISO/IEC 8824-1 „CharacterStringType” karaktersorozat-típusán alapul.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

A BCDString „hstring” jelölést használ. A balról a legszélső hexadecimális számjegy az első oktett legjelentősebb féloktettje. Az oktettek többszörösének előállításához nulla vezető fél oktetteket kell beszúrni – szükség szerint – a balról a legszélső fél oktettől kezdve, az első oktettbe.

A megengedett számjegyek a következők: 0, 1 … 9.

2.8. **CalibrationPurpose**

Ez a kód annak magyarázatát tartalmazza, hogy a kalibrálási paraméterek egy meghatározott sorozata miért került rögzítésre. Ez az adattípus az 1B melléklet 097. és 098. követelményével, valamint az 1C melléklet 119. követelményével függ össze.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Érték-hozzárendelés:

1. generáció:

‘00’H	tartalék érték,
‘01’H	aktiválás: az ismert kalibrálási paraméterek rögzítése a járműegység aktiválásának pillanatában,
‘02’H	első beépítés: a járműegység aktiválása utáni első kalibrálás,
‘03’H	beépítés: a járműegység első kalibrálása az aktuális járműben,
‘04’H	időszakos vizsgálat.

2. generáció:

Az 1. generáció értékein túlmenően a következő értékeket kell alkalmazni:

‘05’H	a vállalkozás által betáplált rendszám,
‘06’H	időbeállítás kalibrálás nélkül,
‘07’H-tól ‘7F’H-ig	RFU,
‘80’H-tól ‘FF’H-ig	Gyártóspecifikus.

2.9. **CardActivityDailyRecord**

Olyan, kártyán tárolt információ, amely a járművezető adott naptári napon végzett tevékenységeire vonatkozik. Ez az adattípus az 1C melléklet 266., 291., 320. és 343. követelményével függ össze.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength az előző napi rekord teljes hossza, bájtokban kifejezve. A maximális értéket az e rekordokat tartalmazó OCTET STRING hossza adja meg (lásd: CardActivityLengthRange a 2. függelék 4. bekezdésében). Amennyiben ez a rekord a legrégebbi napi rekord, az activityPreviousRecordLength értékét 0-ra kell beállítani.

activityRecordLength e rekord teljes hossza, bájtokban kifejezve. A maximális értéket az e rekordokat tartalmazó OCTET STRING hossza adja meg.

activityRecordDate a rekord dátuma.

▼B

activityDailyPresenceCounter a kártya napijelenlét-számlálójának állása az adott napon.

activityDayDistance az adott napon megtett teljes távolság.

activityChangeInfo a járművezetőre vonatkozó ActivityChangeInfo adatsorozat az adott napon. Ez maximálisan 1440 értéket tartalmazhat (percenként egy tevékenységváltás). Ez az adatsorozat mindig magában foglalja a járművezető 00 óra 00 perckori állapotára vonatkozó activityChangeInfo kódot.

2.10. **CardActivityLengthRange**

Egy járművezetői vagy műhelykártyán a járművezető tevékenységi rekordjainak eltárolására rendelkezésre álló bájtok száma.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.11. **CardApprovalNumber**

A kártya típus-jóváhagyási száma.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Érték-hozzárendelés:

A jóváhagyási számot az Európai Bizottság megfelelő honlapján közzétett formában, azaz adott esetben például kötőjelekkel együtt kell megadni. A jóváhagyási számot balra kell igazítani.

2.12. **CardCertificate**

1. generáció:

Egy kártya nyilvános kulcsának tanúsítványa.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Olyan, kártyán tárolt információ, amely a kártya integrált áramkörének (IC) azonosítására vonatkozik (1C melléklet, 249. követelmény). Az icSerialNumber, valamint az icManufacturingReferences egyedileg azonosítják a kártya processzorlapkáját. Az icSerialNumber önmagában nem azonosítja egyedileg a kártya processzorlapkáját.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber az integrált áramkör sorozatszáma.

icManufacturingReferences az integrált áramkör gyártóspecifikus azonosítója.

2.14. **CardConsecutiveIndex**

Egy kártya konszekutív indexe [h) definíció].

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Érték-hozzárendelés: (lásd: 1C melléklet 7. fejezete)

A növekedés sorrendje: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely azon ellenőrzésre vonatkozik, amelyen a járművezető utoljára átesett (1C melléklet, 274., 299., 327. és 350. követelmény).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType az ellenőrzés típusa.

controlTime az ellenőrzés dátuma és ideje.

controlCardNumber az ellenőrzést végző ellenőrző tisztviselőhöz tartozó FullCardNumber.

controlVehicleRegistration az ellenőrzött jármű rendszáma és a nyilvántartásba vétele szerinti tagállam.

controlDownloadPeriodBegin és **controlDownloadPeriodEnd** az adott esetben letöltött időtartam.

2.16. **CardCurrentUse**

A kártya aktuális használatával kapcsolatos információ (1C melléklet, 273., 298., 326. és 349. követelmény).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime az az idő, amikor a kártyát az aktuális használat céljából behelyezik. Ez az elem a kártya eltávolításakor nulla értéket kap.

sessionOpenVehicle az aktuálisan használt jármű azonosítása, amelynek beállítása a kártya behelyezésekor történik meg. Ez az elem a kártya eltávolításakor nulla értéket kap.

2.17. **CardDriverActivity**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a járművezető tevékenységeire vonatkozik (1C melléklet, 267., 268., 292., 293., 321. és 344. követelmény).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord a legrégebbi teljes napi rekord tárolási helye kezdetének meghatározása (a bájtok száma a karakterlánc kezdetétől számítva) az activityDailyRecords karakterláncban. A maximális értéket a karakterlánc hossza adja meg.

▼B

activityPointerNewestRecord a legújabb napi rekord tárolási helye kezdetének meghatározása (a bájtok száma a karakterlánc kezdetétől számítva) az activityDailyRecords karakterláncban. A maximális értéket a karakterlánc hossza adja meg.

activityDailyRecords a járművezető tevékenységére vonatkozó adatok eltárolására rendelkezésre álló hely (adatstruktúra: CardActivityDailyRecord) minden olyan naptári napra, amikor a kártyát használták.

Érték-hozzárendelés: ez az oktettsorozat ciklikusan feltöltődik a CardActivityDailyRecord rekordjaival. Az első felhasználáskor az eltárolás a karakterlánc első bájtjánál kezdődik. Az összes új rekord hozzáfűződik az előző végéhez. Ha a karakterlánc megtelik, az eltárolás a karakterlánc első bájtjánál folytatódik, tekintet nélkül arra, hogy van-e szünet az adatelemeken belül. Mielőtt (az aktuális activityDailyRecord-ot megnövelve vagy új activityDailyRecord-ot felvéve) olyan új tevékenységadat kerülne a karakterláncba, amely régebbi tevékenységadatot vált fel, aktualizálni kell az activityPointerOldestDayRecord-ot, hogy a legrégebbi teljes napi rekord új helyét tükrözze, és ezen (új) legrégebbi teljes napi rekord activityPreviousRecordLength értékét 0-ra kell visszaállítani.

2.18. **CardDrivingLicenceInformation**

Olyan, járművezetői kártyán tárolt információ, amely a kártyatulajdonos járművezetői jogosítványának adataira vonatkozik (1C melléklet, 259. és 284. követelmény).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority a vezetői engedély kiállításáért felelős hatóság.

drivingLicenceIssuingNation azon hatóság helye szerinti ország, amely kiállította a vezetői engedélyt.

drivingLicenceNumber a vezetői engedély száma.

2.19. **CardEventData**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonossal kapcsolatos eseményekre vonatkozik (1C melléklet, 260., 285., 318. és 341. követelmény).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData egy, az EventFaultType emelkedő értéke szerint rendezett cardEventRecords sorozat (kivéve a biztonság megsértésére tett kísérletekkel kapcsolatos rekordokat, amelyek a sorozat utolsó részében kerülnek összegyűjtésre).

cardEventRecords egy adott eseménytípus (vagy a biztonság megsértésére tett kísérletek eseményeire vonatkozó kategória) eseményrekordjainak sorozata.

▼B

2.20. **CardEventRecord**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonossal kapcsolatos eseményre vonatkozik (1C melléklet, 261., 286., 318. és 341. követelmény).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType az esemény típusa.

eventBeginTime az esemény kezdetének dátuma és ideje.

eventEndTime az esemény befejeződésének dátuma és ideje.

eventVehicleRegistration azon jármű rendszáma (VRN) és nyilvántartásba vétele szerinti tagállam, amelyben az esemény történt.

2.21. **CardFaultData**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonossal összefüggő hibákra vonatkozik (1C melléklet, 263., 288., 318. és 341. követelmény).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData az adatrögzítő készülék hibáira vonatkozó rekordok sorozata, amelyet a kártyahibák rekordjainak sorozata követ.

cardFaultRecords egy adott hibakategória (adatrögzítő készülék vagy kártya) hibarekordjainak sorozata.

2.22. **CardFaultRecord**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonossal kapcsolatos hibára vonatkozik (1C melléklet, 264., 289., 318. és 341. követelmény).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType a hiba típusa.

faultBeginTime a hiba kezdetének dátuma és ideje.

faultEndTime a hiba befejeződésének dátuma és ideje.

faultVehicleRegistration azon jármű rendszáma (VRN) és nyilvántartásba vétele szerinti tagállam, amelyben a hiba történt.

▼B

2.23. **CardIccIdentification**

Olyan, kártyán tárolt információ, amely az integrált áramkörös kártya (IC-kártya) kártya azonosítására vonatkozik (1C melléklet, 248. követelmény).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop az óraleállítási üzemmód a 2. függelék definíciója szerint.

cardExtendedSerialNumber az IC-kártya egyedi sorozatszáma az ExtendedSerialNumber adattípus további meghatározása szerint.

cardApprovalNumber a kártya típus-jóváhagyási száma.

cardPersonaliserID a ManufacturerCode-ként kódolt kártyamegszemélyesítési azonosító.

embedderIcAssemblerId a beépítőről/IC-szerelőről szolgáltat információt.

icIdentifier a kártyán elhelyezett IC és az IC gyártójának azonosítója, az ISO/IEC 7816-6 szabvány meghatározása szerint.

2.24. **CardIdentification**

Olyan, kártyán tárolt információ, amely a kártya azonosítására vonatkozik (1C melléklet, 255., 280., 310., 333., 359., 365., 371. és 377. követelmény).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState a kártyát kiállító tagállam kódja.

cardNumber a kártya kártyaszáma.

cardIssuingAuthorityName a kártyát kiállító hatóság neve.

cardIssueDate az a dátum, amikor a kártyát kiállították az aktuális tulajdonosnak.

cardValidityBegin a kártya érvényessége kezdetének első napja.

cardExpiryDate az a dátum, amikor a kártya érvényessége lejár.

▼B

2.25. **CardMACertificate**

2. generáció:

A kártya nyilvános kulcsának tanúsítványa egy járműegységgel való kölcsönös hitelesítéshez. E tanúsítvány struktúráját a 11. függelék határozza meg.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Egy kártyaszám a g) definíció szerint.

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification a járművezető egyedi azonosítója egy tagállamban.

ownerIdentification egy vállalkozás, egy műhely vagy egy ellenőrző szerv egyedi azonosítója egy tagállamban.

cardConsecutiveIndex a kártya konszekutív indexe.

cardReplacementIndex a kártyacsere-index.

cardRenewalIndex a kártya megújítási indexe.

A választás első sorozata a járművezetői kártya számának kódolására, a választás második sorozata pedig a műhely-, az ellenőrző- és a vállalkozáskártya számának kódolására alkalmas.

2.27. **CardPlaceDailyWorkPeriod**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely arra a helyre vonatkozik, ahol a munkanap kezdődik, illetve végződik (1C melléklet, 272., 297., 325. és 348. követelmény).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord az utoljára aktualizált helyrekord indexe.

Érték-hozzárendelés: A helyrekord számlálójának megfelelő szám, amely a helyrekordoknak a szerkezetben való első előfordulásakor „0”-val kezdődik.

placeRecords a betáplált helyekre vonatkozó információkat tartalmazó rekordok sorozata.

▼B

2.28. **CardPrivateKey**

1. generáció:

A kártya privát kulcsa.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

A kártya nyilvános kulcsa.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

A kártya megújítási indexe [i) definíció].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Érték-hozzárendelés: (lásd: e melléklet VII. fejezete).

‘0’ Első kiadás.

A növekedés sorrendje: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

A kártya csereindexe [j) definíció].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Érték-hozzárendelés: (lásd: e melléklet VII. fejezete).

‘0’ Eredeti kártya.

A növekedés sorrendje: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

2. generáció:

A kártya nyilvános kulcsának tanúsítványa aláíráshoz. E tanúsítvány struktúráját a 11. függelék határozza meg.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Ez a kód egy járműegység két kártyaolvasó egységét különbözteti meg.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.34. **CardSlotsStatus**

Ez a kód a járműegység két kártyaolvasó egységébe behelyezett kártyák típusát jelzi.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Érték-hozzárendelés – Rendezett oktett: ‘ccccdddd’B

‘cccc’B A járműkísérői kártyaolvasó egységbe behelyezett kártya típusának azonosítása,

‘dddd’B A járművezetői kártyaolvasó egységbe behelyezett kártya típusának azonosítása

a következő azonosító kódokkal:

‘0000’B nem helyeztek be kártyát,

‘0001’B járművezetői kártyát helyeztek be,

‘0010’B műhelykártyát helyeztek be,

‘0011’B ellenőrzőkártyát helyeztek be,

‘0100’B vállalkozáskártyát helyeztek be.

2.35. **CardSlotsStatusRecordArray**

2. generáció:

A CardSlotsStatus plusz a letöltési protokollban használt metaadatok.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType a rekord (CardSlotsStatus) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a CardSlotsStatus mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a CardSlotsStatus rekordok sorozata.

2.36. **CardStructureVersion**

Ez a kód a tachográfkártyán alkalmazott struktúra verzióját jelzi.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Érték-hozzárendelés: ‘aabb’H:

‘aa’H A struktúraváltásokra vonatkozó index.

‘00’H az 1. generációs alkalmazások esetében

‘01’H a 2. generációs alkalmazások esetében

‘bb’H A magasabb helyértékű bájttal megadott struktúrához meghatározott adatelemek használatára vonatkozó váltások indexe.

‘00’H az 1. generációs alkalmazások e verziója esetében

‘00’H a 2. generációs alkalmazások e verziója esetében

▼B

2.37. **CardVehicleRecord**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a jármű egy naptári nap alatti használati periódusára vonatkozik (1C melléklet, 269., 294., 322. és 345. követelmény).

1. generáció:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin a jármű kilométer-számlálójának értéke a jármű használati időszakának kezdetén.

vehicleOdometerEnd a jármű kilométer-számlálójának értéke a jármű használati időszakának befejeződésekor.

vehicleFirstUse a járműhasználat időszaka kezdetének dátuma és ideje.

vehicleLastUse a járműhasználat időszaka befejeződésének dátuma és ideje.

vehicleRegistration a jármű rendszáma és a nyilvántartásba vétele szerinti tagállam.

vuDataBlockCounter a VuDataBlockCounter értéke a járműhasználat időszaka utolsó kivonásának alkalmával.

2. generáció:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemet kell alkalmazni:

VehicleIdentificationNumber a jármű egészére vonatkozó alvázszám.

2.38. **CardVehiclesUsed**

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonos által használt járművekre vonatkozik (1C melléklet, 270., 295., 323. és 346. követelmény).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord az utoljára aktualizált járműrekord indexe.

▼B

Érték-hozzárendelés: A járműrekord számlálójának megfelelő szám, amely a járműrekordoknak a szerkezetben való első előfordulásakor „0”-val kezdődik.

cardVehicleRecords a használt járművekre vonatkozó információkat tartalmazó rekordok sorozata.

2.39. **CardVehicleUnitRecord**

2. generáció:

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely egy használatban lévő járműegységre vonatkozik (1C melléklet, 303. és 351. követelmény).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp a járműegység használati időszakának kezdete (azaz a járműegységbe való első kártyabehelyezés az adott időszakban).

manufacturerCode a járműegység gyártóját azonosítja.

deviceID egy gyártó járműegységtípusát azonosítja. Az érték gyártóspecifikus.

vuSoftwareVersion a járműegység szoftververziójának száma.

2.40. **CardVehicleUnitsUsed**

2. generáció:

Olyan, járművezetői vagy műhelykártyán tárolt információ, amely a kártyatulajdonos által használt járműegységekre vonatkozik (1C melléklet, 306. és 352. követelmény).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord az utoljára aktualizált járműegységrekord indexe.

Érték-hozzárendelés: A járműegységrekord számlálójának megfelelő szám, amely a járműegységrekordoknak a szerkezetben való első előfordulásakor „0”-val kezdődik.

cardVehicleUnitRecords a használt járműegységekre vonatkozó információkat tartalmazó rekordok sorozata.

2.41. **Certificate**

Nyilvános kulcs tanúsító hatóság által kiállított tanúsítványa.

1. generáció:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Érték-hozzárendelés: digitális aláírás a CertificateContent részleges visszanyerésével, a 11. függelékben meghatározott általános biztonsági mechanizmusoknak megfelelően: Aláírás (128 bájt) || nyilvános kulcs fennmaradó része (58 bájt) || tanúsító hatósági hivatkozás (8 bájt).

2. generáció:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Érték-hozzárendelés: Lásd: 11. függelék.

2.42. **CertificateContent**

1. generáció:

Nyilvános kulcs tanúsítványának (érthető) tartalma a 11. függelékben meghatározott általános biztonsági mechanizmusoknak megfelelően.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier a megfelelő tanúsítvány verziója.

Érték-hozzárendelés: ‘01h’ e verzió esetében.

certificationAuthorityReference a tanúsítványt kiállító tanúsító hatóságot azonosítja. Emellett utal e tanúsító hatóság nyilvános kulcsára.

certificateHolderAuthorisation a tanúsítványtulajdonos jogait azonosítja.

certificateEndOfValidity az a dátum, amikor a tanúsítvány hivatalosan lejár.

certificateHolderReference a tanúsítványtulajdonost azonosítja. Emellett utal a tulajdonos nyilvános kulcsára.

publicKey az a nyilvános kulcs, amelyet e tanúsítvány tanúsít.

2.43. **CertificateHolderAuthorisation**

A tanúsítványtulajdonos jogainak azonosítása.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

1. generáció:

tachographApplicationID a tachográf-alkalmazás alkalmazásazonosítója.

Érték-hozzárendelés: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Ezen AID egy tulajdonosi, nem regisztrált alkalmazásazonosító, amely megfelel az ISO/IEC 7816-5 szabványnak.

equipmentType azon készüléktípus azonosítója, amelyhez a tanúsítvány kiadását tervezik.

Érték-hozzárendelés: az EquipmentType adattípussal összhangban. Értéke 0, ha a tanúsítvány a tagállamok egyikéből származik.

▼B

2. generáció:

tachographApplicationID a 2. generációs tachográfkártya alkalmazásazonosítójának (AID) 6 legfontosabb bájtját jelöli. A tachográfkártya-alkalmazás AID-ját a 6.2. fejezet határozza meg.

Érték-hozzárendelés: ‘FF 53 4D 52 44 54’.

equipmentType a 2. generáció esetében megadott, azon készüléktípus azonosítója, amelyhez a tanúsítvány kiadását tervezik.

Érték-hozzárendelés: az EquipmentType adattípussal összhangban.

2.44. **CertificateRequestID**

Tanúsítási kérelem egyedi azonosítója. Ez egy járműegység nyilvános kulcsának azonosítójaként is felhasználható, amennyiben a tanúsítvány előállításának idején nem ismert azon járműegység sorozatszáma, amelyhez a kulcsot szánják.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber a tanúsítási kérelemre vonatkozó sorozatszám, amely a gyártó és az alábbiakban megadott hónap tekintetében egyedi.

requestMonthYear a tanúsítási kérelem hónapjának és évének azonosítója.

Érték-hozzárendelés: A hónap (két számjegy) és az év (az utolsó két számjegy) BCD kódolása.

crIdentifier: azonosító a tanúsítási kérelem bővített sorozatszámtól való megkülönböztetésére.

Érték-hozzárendelés: ‘FFh’.

manufacturerCode: a tanúsítványt kérő gyártó numerikus kódja.

2.45. **CertificationAuthorityKID**

Egy tanúsító hatóság (egy tagállam vagy az európai tanúsító hatóság) nyilvános kulcsának azonosítója.

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric a tanúsító hatóság numerikus nemzeti kódja.

nationAlpha a tanúsító hatóság alfanumerikus nemzeti kódja.

▼B

keySerialNumber sorozatszám a tanúsító hatóság különböző kulcsainak megkülönböztetésére, amennyiben bizonyos kulcsokat megváltoztatnak.

additionalInfo egy kétbájtos mező a további kódolás céljára (mindig az adott tanúsító hatóság szerint).

caIdentifier azonosító a tanúsító hatóság kulcsazonosítójának egyéb kulcsazonosítóktól való megkülönböztetésére.

Érték-hozzárendelés: ‘01h’.

2.46. **CompanyActivityData**

Olyan, vállalkozáskártyán tárolt információ, amely a kártyával végrehajtott tevékenységekre vonatkozik (1C melléklet, 373. és 379. követelmény).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord        INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords            SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord             SEQUENCE {
     companyActivityType               CompanyActivityType,
     companyActivityTime               TimeReal,
     cardNumberInformation             FullCardNumber,
     vehicleRegistrationInformation    VehicleRegistrationIdentification,
     downloadPeriodBegin               TimeReal,
     downloadPeriodEnd                 TimeReal
    }
}
```

companyPointerNewestRecord az utoljára aktualizált companyActivityRecord indexe.

Érték-hozzárendelés: A vállalkozási tevékenységi rekord számlálójának megfelelő szám, amely a vállalkozási tevékenységi rekordnak a szerkezetben való első előfordulásakor „0”-val kezdődik.

companyActivityRecords az összes vállalkozási tevékenységi rekord sorozata.

companyActivityRecord az egy vállalkozási tevékenységre vonatkozó információk sorozata.

companyActivityType a vállalkozási tevékenység típusa.

companyActivityTime a vállalkozási tevékenység dátuma és ideje.

cardNumberInformation adott esetben a letöltött kártya kártyaszáma és a kártyát kiállító tagállam.

vehicleRegistrationInformation a letöltött, bezárt vagy kioldott jármű rendszáma és a nyilvántartásba vétele szerinti tagállam.

downloadPeriodBegin és **downloadPeriodEnd** a járműegységből adott esetben letöltött időszak.

2.47. **CompanyActivityType**

Ez a kód egy vállalkozás által a vállalkozáskártyája használatával végrehajtott tevékenységet jelzi.

```
CompanyActivityType ::= INTEGER {
   card downloading                  (1),
   VU downloading                    (2),
   VU lock-in                        (3),
   VU lock-out                       (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Olyan, vállalkozáskártyán tárolt információ, amely a kártya alkalmazásának azonosítására vonatkozik (1C melléklet, 369. és 375. követelmény).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId meghatározza az alkalmazott kártyatípust.

cardStructureVersion a kártyán alkalmazott struktúra verzióját határozza meg.

noOfCompanyActivityRecords a kártyán tárolható vállalkozási tevékenységi rekordok száma.

2.49. **CompanyCardHolderIdentification**

Olyan, vállalkozáskártyán tárolt információ, amely a kártyatulajdonos azonosítására vonatkozik (1C melléklet, 372. és 378. követelmény).

```
 CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                        Name,
    companyAddress                     Address,
    cardHolderPreferredLanguage        Language
 }
```

companyName a tulajdonos vállalkozás neve.

companyAddress a tulajdonos vállalkozás címe.

cardHolderPreferredLanguage a kártyatulajdonos által előnyben részesített nyelv.

2.50. **ControlCardApplicationIdentification**

Olyan, ellenőrzőkártyán tárolt információ, amely a kártya alkalmazásának azonosítására vonatkozik (1C melléklet, 357. és 363. követelmény).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId meghatározza az alkalmazott kártyatípust.

cardStructureVersion a kártyán alkalmazott struktúra verzióját határozza meg.

noOfControlActivityRecords a kártyán tárolható ellenőrző tevékenységi rekordok száma.

▼B

2.51. **ControlCardControlActivityData**

Olyan, ellenőrzőkártyán tárolt információ, amely a kártyával végrehajtott ellenőrző tevékenységre vonatkozik (1C melléklet, 361. és 367. követelmény).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
      controlType                       ControlType,
      controlTime                       TimeReal,
      controlledCardNumber              FullCardNumber,
      controlledVehicleRegistration     VehicleRegistrationIdentification,
      controlDownloadPeriodBegin        TimeReal,
      controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord az utoljára aktualizált ellenőrző tevékenységi rekord indexe.

Érték-hozzárendelés: Az ellenőrző tevékenységi rekord számlálójának megfelelő szám, amely az ellenőrző tevékenységi rekordnak a szerkezetben való első előfordulásakor „0”-val kezdődik.

controlActivityRecords az összes ellenőrző tevékenységi rekord sorozata.

controlActivityRecord az egy ellenőrzésre vonatkozó információk sorozata.

controlType az ellenőrzés típusa.

controlTime az ellenőrzés dátuma és ideje.

controlledCardNumber az ellenőrzött kártya kártyaszáma és kiállító tagállama.

controlledVehicleRegistration az ellenőrzött jármű rendszáma és a nyilvántartásba vétele szerinti tagállam.

controlDownloadPeriodBegin és **controlDownloadPeriodEnd** az adott esetben letöltött időtartam.

2.52. **ControlCardHolderIdentification**

Olyan, ellenőrzőkártyán tárolt információ, amely a kártyatulajdonos azonosítására vonatkozik (1C melléklet, 360. és 366. követelmény).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                   Name,
   controlBodyAddress                Address,
   cardHolderName                    HolderName,
   cardHolderPreferredLanguage       Language
}
```

controlBodyName a kártyatulajdonos ellenőrző szervének neve.

controlBodyAddress a kártyatulajdonos ellenőrző szervének címe.

cardHolderName az ellenőrzőkártya tulajdonosának neve és utóneve(i).

▼B

cardHolderPreferredLanguage a kártyatulajdonos által előnyben részesített nyelv.

2.53. **ControlType**

Ez a kód egy ellenőrzés alatt végrehajtott tevékenységeket jelzi. Ez az adattípus az 1C melléklet 126., 274., 299., 327. és 350. követelményével függ össze.

```
ControlType ::= OCTET STRING (SIZE(1))
```

1. generáció:

Érték-hozzárendelés – Rendezett oktett: ‘cvpdxxxx’B (8 bit)

‘c’B kártya letöltése:

‘0’B: a kártya ezen ellenőrző tevékenység alatt nem került letöltésre,

‘1’B: a kártya ezen ellenőrző tevékenység alatt letöltésre került

‘v’B járműegység letöltése:

‘0’B: a járműegység ezen ellenőrző tevékenység alatt nem került letöltésre,

‘1’B: a járműegység ezen ellenőrző tevékenység alatt letöltésre került

‘p’B nyomtatás:

‘0’B: ezen ellenőrző tevékenység alatt nem történt nyomtatás,

‘1’B: ezen ellenőrző tevékenység alatt történt nyomtatás

‘d’B kijelzés:

‘0’B: ezen ellenőrző tevékenység alatt a kijelzőt nem használták,

‘1’B: ezen ellenőrző tevékenység alatt a kijelzőt használták

‘xxxx’B Nem használt.

2. generáció:

Érték-hozzárendelés – Rendezett oktett: ‘cvpdexxx’B (8 bit)

‘c’B kártya letöltése:

‘0’B: a kártya ezen ellenőrző tevékenység alatt nem került letöltésre,

‘1’B: a kártya ezen ellenőrző tevékenység alatt letöltésre került

‘v’B járműegység letöltése:

‘0’B: a járműegység ezen ellenőrző tevékenység alatt nem került letöltésre,

‘1’B: a járműegység ezen ellenőrző tevékenység alatt letöltésre került

‘p’B nyomtatás:

‘0’B: ezen ellenőrző tevékenység alatt nem történt nyomtatás,

‘1’B: ezen ellenőrző tevékenység alatt történt nyomtatás

▼B

‘d’B	kijelzés:
	‘0’B: ezen ellenőrző tevékenység alatt a kijelzőt nem használták,
	‘1’B: ezen ellenőrző tevékenység alatt a kijelzőt használták
‘e’B	útmenti kalibrálás-ellenőrzés:
	‘0’B: a kalibrálási paraméterek ezen ellenőrző tevékenység alatt nem kerültek ellenőrzésre,
	‘1’B: a kalibrálási paraméterek ezen ellenőrző tevékenység alatt ellenőrzésre kerültek,
‘xxx’B	RFU.

2.54. **CurrentDateTime**

Az adatrögzítő készülék aktuális dátuma és ideje.

```
CurrentDateTime ::= TimeReal
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.55. **CurrentDateTimeRecordArray**

2. generáció:

Az aktuális dátum és idő plusz a letöltési protokollban használt metaadatok.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType a rekord (CurrentDateTime) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a CurrentDateTime mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records az aktuális dátum- és időrekordok sorozata.

2.56. **DailyPresenceCounter**

Járművezetői vagy műhelykártyán tárolt számláló, amely eggyel nő minden olyan naptári napon, amelyen a kártya a járműegységbe behelyezésre kerül. Ez az adattípus az 1C melléklet 266., 299., 320. és 343. követelményével függ össze.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Érték-hozzárendelés: Folyamatos számozás, amelynek a maximális értéke = 9 999, a számozás 0-val kezdődik újra. A kártya első kiállításának idején a számot 0-ra kell beállítani.

▼B

2.57. **Datef**

Egy könnyen kinyomtatható numerikus formátumban kifejezett dátum.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Érték-hozzárendelés:

yyyy	Év
mm	Hónap
dd	Nap
‘00000000’H	Kifejezetten nem jelöl dátumot.

2.58. **DateOfDayDownloaded**

2. generáció:

A letöltés dátuma és időpontja.

```
DateOfDayDownloaded ::= TimeReal
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.59. **DateOfDayDownloadedRecordArray**

2. generáció:

A letöltés dátuma és időpontja plusz a letöltési protokollban használt metaadatok.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType a rekord (DateOfDayDownloaded) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a CurrentDateTime mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a letöltés aktuális dátumát és idejét tartalmazó rekordok sorozata.

2.60. **Distance**

A megtett távolság (a jármű két kilométerszámláló-értéke közötti különbség kilométerben).

```
Distance ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: Előjel nélküli bináris szám. Az érték km-ben kifejezve a 0-tól 9 999 km-ig terjedő üzemelési tartományban.

2.61. **DriverCardApplicationIdentification**

Olyan, járművezetői kártyán tárolt információ, amely a kártya alkalmazásának azonosítására vonatkozik (1C melléklet, 253. és 278. követelmény).

▼B

1. generáció:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId meghatározza az alkalmazott kártyatípust.

cardStructureVersion a kártyán alkalmazott struktúra verzióját határozza meg.

noOfEventsPerType a kártyán eseménytípusonként tárolható események száma.

noOfFaultsPerType a kártyán hibatípusonként tárolható hibák száma.

activityStructureLength a tevékenységi rekordok eltárolására rendelkezésre álló bájtok számát jelzi.

noOfCardVehicleRecords a kártyán eltárolható járműrekordok száma.

noOfCardPlaceRecords a kártyán eltárolható helyek száma.

2. generáció:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemeket kell alkalmazni:

noOfGNSSCDRecords a kártyán tárolható GNSS megszakítás nélküli járművezetési rekordok száma.

noOfSpecificConditionRecords a kártyán tárolható különlegeskörülmény-rekordok száma.

2.62. **DriverCardHolderIdentification**

Olyan, járművezetői kártyán tárolt információ, amely a kártyatulajdonos azonosítására vonatkozik (1C melléklet, 256. és 281. követelmény).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderName a járművezetői kártya tulajdonosának neve és utóneve(i).

cardHolderBirthDate a járművezetői kártya tulajdonosának születési dátuma.

cardHolderPreferredLanguage a kártyatulajdonos által előnyben részesített nyelv.

2.63. **DSRCSecurityData**

2. generáció:

A menetíró készülékből a távlekérdezőnek (RI) DSRC-n továbbítandó egyszerű szöveges információk és MAC (a részleteket lásd a 11. függelék B részének 13. fejezetében).

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength a DER-TLV kódolás része, értékét ‘81 10’-re kell beállítani (lásd a 11. függelék B részének 13. fejezetét).

currentDateTime a járműegység aktuális dátuma és ideje.

counter az RTM üzeneteket számolja.

vuSerialNumber a járműegység sorozatszáma.

dSRCMKVersionNumber annak a DSRC mesterkulcsnak a verziószáma, amelyből a járműegység specifikus DSRC kulcsait levezették.

tagLengthMac a DER-TLV kódolás részét képező MAC adatobjektum címkéje és hossza. A címkét ‘8E’ értékre kell beállítani, a hossznál pedig a MAC oktettben kifejezett hosszát kell bekódolni (lásd a 11. függelék B részének 13. fejezetét).

mac az RTM-üzenettel összefüggésben kiszámított MAC (lásd a 11. függelék B részének 13. fejezetét).

2.64. **EGFCertificate**

2. generáció:

Külső GNSS-eszköz nyilvános kulcsának tanúsítványa járműegységgel való kölcsönös hitelesítéshez. E tanúsítvány struktúráját a 11. függelék határozza meg.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Az IC-szerelőről szolgáltat információt.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode a modulbeépítő kétbetűs országkódja az ISO 3166 szabványnak megfelelően.

moduleEmbedder a modulbeépítőt azonosítja.

manufacturerInformation a gyártó belső használatára.

2.66. **EntryTypeDailyWorkPeriod**

Ez a kód egy munkanap kezdetének és végének a helyét és a betáplálás körülményeit különbözteti meg.

1. generáció

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Érték-hozzárendelés: az ISO/IEC8824-1 szabványnak megfelelően.

2. generáció

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Érték-hozzárendelés: az ISO/IEC8824-1 szabványnak megfelelően.

2.67. **EquipmentType**

Ez a kód a készülékek különböző típusait különbözteti meg a tachográf-alkalmazás számára.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

1. generáció:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Érték-hozzárendelés: Az ISO/IEC8824-1 szabványnak megfelelően.

A 0 értéket a tagállam vagy Európa jelölésére kell fenntartani a tanúsítványok CHA mezőjében.

2. generáció:

Ugyanazokat az értékeket kell használni, mint az 1. generáció esetében, valamint a következő további értékeket:

```
--GNSS Facility                     (8),
--Remote Communication Module       (9),
--ITS interface module              (10),
--Plaque                            (11), -- may be used in SealRecord
--M1/N1 Adapter                     (12), -- may be used in SealRecord
--European Root CA (ERCA)           (13),
--Member State CA (MSCA)            (14),
--External GNSS connection          (15), -- may be used in SealRecord
--Unused                            (16), -- used in SealDataVu
--RFU                               (17..255)
```

Megjegyzés: A SealRecord tartalmazhatja adott esetben a Plaque (címke), az Adapter (adapter) és az External GNSS connection (külső GNSS-kapcsolat) 2. generációs értékeit, valamint a Vehicle Unit (járműegység) és a Motion Sensor (mozgásérzékelő) 1. generációs értékeit.

2.68. **EuropeanPublicKey**

1. generáció:

Az európai nyilvános kulcs.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Egy esemény vagy hiba rögzítésének okát feltüntető kód.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Érték-hozzárendelés:

'00'H	a 10 legújabb (vagy utolsó) esemény vagy hiba egyike
'01'H	a leghosszabb esemény az előfordulás utolsó 10 napjának egyikén
'02'H	az utolsó 365 nap 5 leghosszabb eseményének egyike
'03'H	a legutolsó esemény az előfordulás utolsó 10 napjának egyikén
'04'H	a legsúlyosabb esemény az előfordulás utolsó 10 napjának egyikén
'05'H	az utolsó 365 nap 5 legsúlyosabb eseményének egyike
'06'H	az utolsó kalibrálás után történt első esemény vagy hiba
'07'H	egy aktív/folyamatban levő esemény vagy hiba
'08'H to '7F'H	RFU
'80'H to 'FF'H	gyártóra jellemző.

▼B

2.70. **EventFaultType**

Eseményt vagy hibát minősítő kód.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Érték-hozzárendelés:

1. generáció:

‘0x’H	Általános események,
‘00’H	Nincsenek további részletek,
‘01’H	Érvénytelen kártya behelyezése,
‘02’H	Kártyaütközés,
‘03’H	Időátfedés,
‘04’H	Járművezetés megfelelő kártya nélkül,
‘05’H	Kártya behelyezése járművezetés közben,
‘06’H	Az utolsó kártyakapcsolat nem megfelelő lezárása,
‘07’H	Gyorshajtás,
‘08’H	Az áramellátás megszakadása,
‘09’H	Mozgásadatok hibája,
‘0A’H	A jármű mozgásával kapcsolatos ellentmondás,
‘0B’ to ‘0F’H	RFU,
‘1x’H	A járműegységgel kapcsolatos, a biztonság rendszer megsértésére tett kísérletek esemé-
‘10’H	nyei,
‘11’H	Nincsenek további részletek,
‘12’H	A mozgásérzékelő hitelesítési hibája,
‘13’H	A tachográfkártya hitelesítési hibája,
‘14’H	A mozgásérzékelő jogosulatlan cseréje,
‘15’H	A kártyaadatok bevitelét érintő integritási hiba,
‘16’H	A tárolt felhasználói adatokat érintő integritási hiba,
‘17’H	Belső adatátviteli hiba,
‘18’H	Jogosulatlan burkolatfelnyitás,
‘19’H to ‘1F’H	Hardverrongálás,
	RFU,
‘2x’H	Az érzékelővel kapcsolatos, a biztonság rendszer megsértésére tett kísérletek esemé-
‘20’H	nyei,
‘21’H	Nincsenek további részletek,
‘22’H	Hitelesítési hiba,
‘23’H	A tárolt adatok integritási hibája,
‘24’H	Belső adatátviteli hiba,
‘25’H	Jogosulatlan burkolatfelnyitás,
‘26’H to ‘2F’H	Hardverrongálás,
	RFU,
‘3x’H	Az adatrögzítő készülék hibái,
‘30’H	Nincsenek további részletek,
‘31’H	A járműegység belső hibája,
‘32’H	Nyomtatóhiba,
‘33’H	Kijelzőhiba,
‘34’H	Letöltési hiba,
‘35’H	Érzékelőhiba,
‘36’H to ‘3F’H	RFU,
‘4x’H	Kártyahibák,
‘40’H	Nincsenek további részletek,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Gyártóspecifikus.

▼B

2. generáció:

Ugyanazokat az értékeket kell használni, mint az 1. generáció esetében, valamint a további értékeket:

‘0B’H	Időütközés (a GNSS és a járműegység belső órája között),
‘0C’ to ‘0F’H	RFU,
‘5x’H	A GNSS-rendszerrel kapcsolatos hibák,
‘50’H	Nincsenek további részletek,
‘51’H	Belső GNSS-vevőhiba,
‘52’H	Külső GNSS-vevőhiba,
‘53’H	Külső GNSS-kommunikációs hiba,
‘54’H	Nincs GNSS-helyzetmeghatározási adat,
‘55’H	A GNSS-rendszer manipulálásészlelése,
‘56’H	A külső GNSS-eszköz tanúsítványának érvényessége lejárt,
‘57’H to ‘5F’H	RFU,
‘6x’H	A távoli kommunikációs modullal kapcsolatos hibák,
‘60’H	Nincsenek további részletek,
‘61’H	A távoli kommunikációs modul hibája,
‘62’H	A távoli kommunikációs modul kommunikációs hibája,
‘63’H to ‘6F’H	RFU,
‘7x’H	Az ITS interfész hibái,
‘70’H	Nincsenek további részletek,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

2. generáció:

A bővített plombaazonosító egyedileg azonosítja a plombát (1C mellék-let, 401. követelmény).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode a plomba gyártójának kódja.

sealIdentifier a gyártó egyedi plombájának azonosítója.

2.72. **ExtendedSerialNumber**

Készülék egyedi azonosítója. Egy készülék nyilvános kulcsának azonosítójaként is használható.

1. generáció:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber a készülék sorozatszáma, amely a gyártó, a készülék típusa, valamint az alábbiakban megadott hónap és év tekintetében egyedi.

monthYear a gyártás évének és hónapjának az azonosítása (vagy a sorozatszám kijelölésének azonosítása).

▼B

Érték-hozzárendelés: A hónap (két számjegy) és az év (az utolsó két számjegy) BCD kódolása.

type a készülék típusának azonosítója.

Érték-hozzárendelés: gyártóspecifikus, az ‘FFh’ érték fenntartva.

manufacturerCode: típusjóváhagyással rendelkező készülék gyártóját azonosító numerikus kód.

2. generáció:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber lásd az 1. generációt

monthYear lásd az 1. generációt

type a készülék típusát jelöli.

manufacturerCode: lásd az 1. generációt.

2.73. **FullCardNumber**

Egy tachográfkártya teljes bizonyossággal történő azonosítására szolgáló kód.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType a tachográfkártya típusa.

cardIssuingMemberState a kártyát kiállító tagállam kódja.

cardNumber a kártyaszám.

2.74. **FullCardNumberAndGeneration**

2. generáció:

Egy tachográfkártya és generációjának teljes bizonyossággal történő azonosítására szolgáló kód.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber a tachográfkártyát azonosítja.

generation az alkalmazott tachográfkártya generációját jelzi.

▼B

2.75. **Generation**

2. generáció:

Az alkalmazott menetíró készülék generációját jelzi.

```
Generation ::= INTEGER(0..255)
```

Érték-hozzárendelés:

‘00’H	RFU
‘01’H	1. generáció
‘02’H	2. generáció
‘03’H … ‘FF’H	RFU

2.76. **GeoCoordinates**

2. generáció:

A földrajzi koordinátákat egész számként kell kódolni. Ezek az egész számok a ± DDMM.M többszörösei a szélesség, és a ± DDDMM.M többszörösei a hosszúság esetében. Itt ± DD, illetve ± DDD a fokokat, MM.M pedig a perceket jelöli.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude kódolása a ± DDMM.M formában lévő adat többszöröseként (10-szereseként) történik.

longitude kódolása a ± DDDMM.M formában lévő adat többszöröseként (10-szereseként) történik.

2.77. **GNSSAccuracy**

2. generáció:

A GNSS helyzetmeghatározási adatok pontossága [eee) definíció]. E pontosság kódolása egész számként történik, amely az X.Y érték többszöröse (10-szerese).

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

2. generáció:

Járművezetői vagy műhelykártyán abban az esetben eltárolt, a jármű GNSS-helyzetére vonatkozó információ, ha a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét (1C melléklet, 306. és 354. követelmény).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord az utoljára aktualizált GNSS megszakítás nélküli járművezetési rekord indexe.

▼B

Érték-hozzárendelés: A GNSS megszakítás nélküli járművezetési rekord számlálójának megfelelő szám, amely a GNSS megszakítás nélküli járművezetési rekordnak a szerkezetben való első előfordulásakor „0”-val kezdődik.

gnssContinuousDrivingRecords azon rekordok sorozata, amelyek annak az időpontnak a dátumát és idejét tartalmazzák, amikor a megszakítás nélküli járművezetési ideje eléri a három óra többszörösét, valamint a jármű helyzetére vonatkozó adatokat.

2.79. **GNSSContinuousDrivingRecord**

2. generáció:

Járművezetői vagy műhelykártyán abban az esetben eltárolt, a jármű GNSS-helyzetére vonatkozó információ, ha a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét (1C melléklet, 305. és 353. követelmény).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp annak az időpontnak a dátuma és ideje, amikor a kártyatulajdonos megszakítás nélküli járművezetési ideje eléri a három óra többszörösét.

gnssPlaceRecord a jármű helyzetére vonatkozó információt tartalmazza.

2.80. **GNSSPlaceRecord**

2. generáció:

A jármű GNSS-helyzetére vonatkozó információ (1C melléklet, 108., 109., 110., 296., 305., 347. és 353. követelmény).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp annak az időpontnak a dátuma és ideje, amikor a jármű GNSS-rendszer szerinti helyzete meghatározásra került.

gnssAccuracy a GNSS-helyzetmeghatározási adatok pontossága.

geoCoordinates a GNSS segítségével rögzített helyzet.

2.81. **HighResOdometer**

A jármű kilométer-számlálójának értéke: A jármű üzemelése alatt megtett távolságok összesített értéke.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Érték-hozzárendelés: Előjel nélküli bináris szám. Az érték 1/200 km-ben kifejezve a 0-tól 21 055 406 km-ig terjedő működési tartományban.

2.82. **HighResTripDistance**

Egy út teljes egésze vagy annak egy része alatt megtett távolság.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Érték-hozzárendelés: Előjel nélküli bináris szám. Az érték 1/200 km-ben kifejezve a 0-tól 21 055 406 km-ig terjedő működési tartományban.

2.83. **HolderName**

A kártyatulajdonos családi neve és utóneve(i).

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname a tulajdonos családi neve. A családi név nem tartalmaz címeket.

Érték-hozzárendelés: Amennyiben nem egy meghatározott személy részére kiállított kártyáról van szó, a holderSurname ugyanazon információkat tartalmazza, mint a companyName, a workshopName vagy a controlBodyName.

holderFirstNames a tulajdonos utóneve(i) és utóneveinek kezdőbetűi.

2.84. **InternalGNSSReceiver**

2. generáció:

Információ arról, hogy a GNSS-vevő a járműegységen belül vagy kívül található. Az igaz azt jelenti, hogy a GNSS-vevő a járműegységen belül található. A hamis azt jelenti, hogy a GNSS-vevő a járműegységen kívül található.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Az adatrögzítő készülék állandója [m) definíció].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: Kilométerenkénti impulzusok a 0-tól 64 255 impulzus/km-ig terjedő működési tartományban.

2.86. **KeyIdentifier**

Egy nyilvános kulcs egyedi azonosítója, amely a kulcsra való hivatkozásra és annak kiválasztására szolgál. Ezen azonosító a kulcs tulajdonosát is azonosítja.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber             ExtendedSerialNumber,
   certificateRequestID             CertificateRequestID,
   certificationAuthorityKID        CertificationAuthorityKID
}
```

▼B

Az első választás alkalmas egy járműegység vagy tachográfkártya nyilvános kulcsára való hivatkozásra.

A második választás alkalmas egy járműegység nyilvános kulcsára való hivatkozásra (amennyiben a járműegység sorozatszáma a tanúsítvány elkészítésének idején nem ismert).

A harmadik választás alkalmas egy tagállam nyilvános kulcsára való hivatkozásra.

2.87. **KMWCKey**

2. generáció:

A járműegység–mozgásérzékelő pár esetében alkalmazott AES kulcs és a hozzá tartozó kulcsverzió. A részleteket lásd a 11. függelékben.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey a járműegység–mozgásérzékelő pár esetében alkalmazott kulccsal összefűzött AES kulcs hossza.

keyVersion az AES kulcs verzióját jelzi.

2.88. **Language**

A nyelvet azonosító kód.

```
Language ::= IA5String(SIZE(2))
```

Érték-hozzárendelés: Két kisbetűből álló kóddal való kódolás az ISO 639 szabványnak megfelelően.

2.89. **LastCardDownload**

Az utolsó (ellenőrzéstől eltérő célból végrehajtott) kártyaletöltés járművezetői kártyán tárolt dátuma és ideje (1C melléklet, 257. és 282. követelmény). Ez a dátum a járműegységgel vagy bármely kártyaolvasóval aktualizálható.

```
LastCardDownload ::= TimeReal
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.90. **LinkCertificate**

2. generáció:

Az európai legfelső szintű hitelesítésszolgáltató kulcspárjai közötti kapcsolat tanúsítványa.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

A gumiabroncsok tényleges kerülete [u) definíció].

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Érték-hozzárendelés: Előjel nélküli bináris szám, értéke 1/8 mm-ben kifejezve a 0-tól 8 031 mm-ig terjedő működési tartományban.

2.92. **MAC**

2. generáció:

A 11. függelékben meghatározott titkosító csomagoknak megfelelő, 8, 12 vagy 16 bájt hosszúságú titkosítási ellenőrző összeg.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kód annak azonosítására, hogy a kártyatulajdonos betáplált-e manuálisan járművezetői tevékenységeket a kártya behelyezésekor vagy sem (1B melléklet, 081. követelmény és 1C melléklet, 102. követelmény).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.94. **ManufacturerCode**

Típusjóváhagyással rendelkező készülék gyártóját azonosító kód.

```
ManufacturerCode ::= INTEGER(0..255)
```

Az interoperabilitási vizsgálatok elvégzéséért felelős laboratórium kezeli és honlapján közzéteszi a gyártók azonosítására szolgáló kódok jegyzékét (1C melléklet, 454. követelmény).

Az interoperabilitási vizsgálatok elvégzéséért felelős laboratóriumhoz benyújtott kérelem alapján a gyártók azonosítására szolgáló kódokat („ManufacturerCodes”) ideiglenesen a tachográfok konstruktőreinek osztják ki.

2.95. **ManufacturerSpecificEventFaultData**

2. generáció:

A gyártóspecifikus hibakódok leegyszerűsítik a járműegységek hibaelemzését és karbantartását.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode a járműegység gyártóját azonosítja.

manufacturerSpecificErrorCode egy gyártóspecifikus hibakód.

▼B

2.96. **MemberStateCertificate**

Egy tagállam nyilvános kulcsának tanúsítványa, amelyet az európai tanúsító hatóság állít ki.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

2. generáció:

A tagállami tanúsítvány plusz a letöltési protokollban használt metaadatok.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType a rekord (MemberStateCertificate) típusát jelöli. **Értékhozzárendelés:** Lásd: RecordType

recordSize a MemberStateCertificate mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma. Az értéket 1-re kell állítani, mivel a tanúsítványok eltérő hosszúságúak lehetnek.

records a tagállami tanúsítványok sorozata.

2.98. **MemberStatePublicKey**

1. generáció:

Egy tagállam nyilvános kulcsa.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Egy név.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage a 4. fejezetben meghatározott karakterkészletet adja meg,

name egy név, amelyet a meghatározott karakterkészlet felhasználásával kódolnak.

2.100. **NationAlpha**

Az országokra való alfabetikus hivatkozásnak összhangban kell lennie a nemzetközi közlekedésben a járműveken alkalmazott megkülönböztető jelekkel (az Egyesült Nemzetek Szervezete 1968. évi Bécsi Közúti Közlekedési Egyezménye).

```
NationAlpha ::= IA5String(SIZE(3))
```

Az országokra való alfabetikus hivatkozást és a numerikus kódokat („Nation Alpha and Numeric codes”) az 1C melléklet 440. követelményében meghatározottak szerint az interoperabilitási vizsgálatok elvégzésére kijelölt laboratórium honlapján vezetett jegyzékben kell feltüntetni.

▼B

2.101. **NationNumeric**

Numerikus hivatkozás egy országra.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Érték-hozzárendelés: lásd a 2.100. adattípust (NationAlpha).

A fenti bekezdésben említett, az országokra való alfabetikus hivatkozást és a numerikus előírásokat („Nation Alpha and Numeric specification”) csak azt követően lehet módosítani vagy aktualizálni, hogy a kijelölt laboratórium megkapta a típusjóváhagyással rendelkező, digitális és intelligens menetíró készülékkel felszerelt járműegységek gyártóinak véleményét.

2.102. **NoOfCalibrationRecords**

Egy műhelykártyán tárolható kalibrálási rekordok száma.

1. generáció:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2. generáció:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.103. **NoOfCalibrationsSinceDownload**

A műhelykártyával annak utolsó letöltése óta elvégzett kalibrálások számát jelző számláló (1C melléklet, 317. és 340. követelmény).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.104. **NoOfCardPlaceRecords**

Egy járművezetői vagy műhelykártyán tárolható helyrekordok száma.

1. generáció:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2. generáció:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

▼B

2.105. **NoOfCardVehicleRecords**

Egy járművezetői vagy műhelykártyán tárolható, a használt járművekre vonatkozó adatokat tartalmazó rekordok száma.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.106. **NoOfCardVehicleUnitRecords**

2. generáció:

Egy járművezetői vagy műhelykártyán tárolható, a használt járműegységekre vonatkozó adatokat tartalmazó rekordok száma.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.107. **NoOfCompanyActivityRecords**

Egy vállalkozáskártyán tárolható vállalkozási tevékenységi rekordok száma.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.108. **NoOfControlActivityRecords**

Egy ellenőrzőkártyán tárolható ellenőrző tevékenységi rekordok száma.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.109. **NoOfEventsPerType**

Egy kártyán eseménytípusonként tárolható események száma.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.110. **NoOfFaultsPerType**

Egy kártyán hibatípusonként tárolható hibák száma.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Érték-hozzárendelés: lásd a 2. függeléket.

▼B

2.111. **NoOfGNSSCDRecords**

2. generáció:

Egy kártyán tárolható GNSS megszakítás nélküli járművezetési rekordok száma.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.112. **NoOfSpecificConditionRecords**

2. generáció:

Egy kártyán tárolható különlegeskörülmény-rekordok száma.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Érték-hozzárendelés: lásd a 2. függeléket.

2.113. **OdometerShort**

A jármű kilométer-számlálójának értéke rövid alakban.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Érték-hozzárendelés: Előjel nélküli bináris szám. Az érték km-ben kifejezve a 0-tól 9 999 999 km-ig terjedő működési tartományban.

2.114. **OdometerValueMidnight**

A jármű kilométer-számlálójának értéke éjfélkor egy adott napon (1B melléklet, 090. követelmény és 1C melléklet, 113. követelmény).

```
OdometerValueMidnight ::= OdometerShort
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

2.115. **OdometerValueMidnightRecordArray**

2. generáció:

Az OdometerValueMidnight plusz a letöltési protokollban használt metaadatok.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType a rekord (OdometerValueMidnight) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a OdometerValueMidnight mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records az OdometerValueMidnight rekordok sorozata.

▼B

2.116. **OverspeedNumber**

A gyorshajtási események száma a gyorshajtás legutóbbi ellenőrzése óta.

```
OverspeedNumber ::= INTEGER(0..255)
```

Érték-hozzárendelés: A 0 azt jelenti, hogy nem történt gyorshajtási esemény a gyorshajtás legutóbbi ellenőrzése óta, az 1 azt jelenti, hogy a gyorshajtás legutóbbi ellenőrzése óta egy gyorshajtási esemény fordult elő, …, a 255 pedig azt jelenti, hogy a gyorshajtás legutóbbi ellenőrzése óta 255 vagy annál több gyorshajtási esemény fordult elő.

2.117. **PlaceRecord**

A munkanap kezdetének vagy végének helyére vonatkozó információ (1C melléklet, 108., 271., 296., 324. és 347. követelmény).

1. generáció:

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort
}
```

entryTime a betáplálásra vonatkozó dátum és idő.

entryTypeDailyWorkPeriod a betáplálás típusa.

dailyWorkPeriodCountry a betáplált ország.

dailyWorkPeriodRegion a betáplált régió.

vehicleOdometerValue a kilométer-számláló értéke a hely betáplálása idején.

2. generáció:

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort,
   entryGNSSPlaceRecord                   GNSSPlaceRecord
}
```

Az 1. generáció értékein túlmenően a következő összetevőket kell alkalmazni:

entryGNSSPlaceRecord a rögzített hely és idő.

▼B

2.118. **PreviousVehicleInfo**

A kártya járműegységbe történő behelyezésekor a járművezető által előzőleg használt járműre vonatkozó információ (1B melléklet, 081. követelmény és 1C melléklet, 102. követelmény).

1. generáció:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification a jármű rendszáma és a nyilvántartásba vétele szerinti tagállam.

cardWithdrawalTime a kártyakivétel dátuma és ideje.

2. generáció:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemet kell alkalmazni:

vuGeneration a járműegység generációját azonosítja.

2.119. **PublicKey**

1. generáció:

Nyilvános RSA kulcs.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus a kulcspár modulusa.

rsaKeyPublicExponent a kulcspár nyilvános kitevője.

2.120. **RecordType**

2. generáció:

hivatkozás rekordtípusra. Ez az adattípus a RecordArrays sorozatban szerepel.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Érték-hozzárendelés:

‘01’H	ActivityChangeInfo,
‘02’H	CardSlotsStatus,
‘03’H	CurrentDateTime,
‘04’H	MemberStateCertificate,
‘05’H	OdometerValueMidnight,
‘06’H	DateOfDayDownloaded,
‘07’H	SensorPaired,
‘08’H	Signature,
‘09’H	SpecificConditionRecord,
‘0A’H	VehicleIdentificationNumber,
‘0B’H	VehicleRegistrationNumber,
‘0C’H	VuCalibrationRecord,
‘0D’H	VuCardIWRecord,
‘0E’H	VuCardRecord,
‘0F’H	VuCertificate,
‘10’H	VuCompanyLocksRecord,
‘11’H	VuControlActivityRecord,
‘12’H	VuDetailedSpeedBlock,
‘13’H	VuDownloadablePeriod,
‘14’H	VuDownloadActivityData,
‘15’H	VuEventRecord,
‘16’H	VuGNSSCDRecord,
‘17’H	VuITSConsentRecord,
‘18’H	VuFaultRecord,
‘19’H	VuIdentification,
‘1A’H	VuOverSpeedingControlData,
‘1B’H	VuOverSpeedingEventRecord,
‘1C’H	VuPlaceDailyWorkPeriodRecord,
‘1D’H	VuTimeAdjustmentGNSSRecord,
‘1E’H	VuTimeAdjustmentRecord,
‘1F’H	VuPowerSupplyInterruptionRecord,
‘20’H	SensorPairedRecord,
‘21’H	SensorExternalGNSSCoupledRecord,
‘22’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Gyártóspecifikus.

2.121. **RegionAlpha**

Alfabetikus hivatkozás egy meghatározott országon belüli régióra.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

1. generáció:

Érték-hozzárendelés:

‘ ’	No information available,
Spain:	
‘AN ’	Andalucía,
‘AR ’	Aragón,
‘AST’	Asturias,
‘C ’	Cantabria,
‘CAT’	Cataluña,
‘CL ’	Castilla-León,
‘CM ’	Castilla-La-Mancha,
‘CV’	Valencia,
‘EXT’	Extremadura,
‘G ’	Galicia,
‘IB ’	Baleares,
‘IC ’	Canarias,
‘LR ’	La Rioja,
‘M ’	Madrid,
‘MU ’	Murcia,
‘NA ’	Navarra,
‘PV ’	País Vasco

▼B

2. generáció:

A RegionAlpha kódokat az interoperabilitási vizsgálatok elvégzésére kijelölt laboratórium honlapján vezetett jegyzékben kell feltüntetni.

2.122. **RegionNumeric**

Numerikus hivatkozás egy meghatározott országon belüli régióra.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

1. generáció:

Érték-hozzárendelés:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

2. generáció:

A RegionNumeric kódokat az interoperabilitási vizsgálatok elvégzésére kijelölt laboratórium honlapján vezetett jegyzékben kell feltüntetni.

2.123. **RemoteCommunicationModuleSerialNumber**

2. generáció:

A távoli kommunikációs modul sorozatszáma.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

1. generáció:

Az RSA kulcspár modulusa.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Érték-hozzárendelés: Nincs meghatározva.

2.125. **RSAKeyPrivateExponent**

1. generáció:

Az RSA kulcspár saját kitevője.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Érték-hozzárendelés: Nincs meghatározva.

▼B

2.126. **RSAKeyPublicExponent**

1. generáció:

Az RSA kulcspár nyilvános kitevője.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Érték-hozzárendelés: Nincs meghatározva.

2.127. **RtmData**

2. generáció:

Ennek az adattípusnak a meghatározását lásd a 14. függelékben.

2.128. **SealDataCard**

2. generáció:

Ezt az adattípust, amely a jármű különböző alkatrészeire erősített plombákra vonatkozó információkat tartalmazza, kártyán kell tárolni. Ez az adattípus az 1C melléklet 337. követelményével függ össze.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords a sealRecords sorozatban található rekordok száma.

sealRecords a plombák rekordjainak sorozata.

2.129. **SealDataVu**

2. generáció:

Ezt az adattípust, amely a jármű különböző alkatrészeire erősített plombákra vonatkozó információkat tartalmazza, járműegységben kell tárolni.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords a plombák rekordjainak sorozata. Amennyiben 5-nél kevesebb plomba van, az EquipmentType értékét valamennyi nem használt sealRecords sorozatban 16-ra, azaz a „nem használt” értékre kell állítani.

2.130. **SealRecord**

2. generáció:

Ez az adattípus az alkatrészekre erősített plombákról tárol információkat. Ez az adattípus az 1C melléklet 337. követelményével függ össze.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType azt a készüléktípust azonosítja, amelyre a plomba rögzítve van.

extendedSealIdentifier a készülékre rögzített plomba azonosítója.

▼B

2.131. **SensorApprovalNumber**

Az érzékelő típus-jóváhagyási száma.

1. generáció:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Érték-hozzárendelés: Nincs meghatározva.

2. generáció:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Érték-hozzárendelés:

A jóváhagyási számot az Európai Bizottság megfelelő honlapján közzétett formában, azaz adott esetben például kötőjelekkel együtt kell megadni. A jóváhagyási számot balra kell igazítani.

2.132. **SensorExternalGNSSApprovalNumber**

2. generáció:

A külső GNSS-eszköz típus-jóváhagyási száma.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Érték-hozzárendelés:

A jóváhagyási számot az Európai Bizottság megfelelő honlapján közzétett formában, azaz adott esetben például kötőjelekkel együtt kell megadni. A jóváhagyási számot balra kell igazítani.

2.133. **SensorExternalGNSSCoupledRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely a járműegységhez csatlakoztatott külső GNSS-eszköz azonosítására vonatkozik (1C melléklet, 100. követelmény).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber a járműegységhez csatlakoztatott külső GNSS-eszköz sorozatszáma.

sensorApprovalNumber e külső GNSS-eszköznek a jóváhagyási száma.

sensorCouplingDate e külső GNSS-eszköz járműegységhez való csatlakoztatásának dátuma.

2.134. **SensorExternalGNSSIdentification**

2. generáció:

A külső GNSS-eszköz azonosítására vonatkozó információ (1C melléklet, 98. követelmény).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber a külső GNSS-eszköz bővített sorozatszáma.

sensorApprovalNumber a külső GNSS-eszköz jóváhagyási száma.

sensorSCIdentifier a külső GNSS-eszköz biztonsági alkatrészének azonosítója.

sensorOSIdentifier a külső GNSS-eszköz operációs rendszerének azonosítója.

2.135. **SensorExternalGNSSInstallation**

2. generáció:

Olyan, külső GNSS-eszközben tárolt információ, amely a külső GNSS-érzékelő beépítésére vonatkozik (1C melléklet, 123. követelmény).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst a külső GNSS-eszköz járműegységhez való első csatlakoztatásának dátuma.

firstVuApprovalNumber a külső GNSS-eszközhöz csatlakoztatott első járműegység jóváhagyási száma.

firstVuSerialNumber a külső GNSS-eszközzel párosított első járműegység sorozatszáma.

sensorCouplingDateCurrent a külső GNSS-eszköz járműegységhez való aktuális csatlakoztatásának dátuma.

currentVuApprovalNumber a külső GNSS-eszközhöz aktuálisan csatlakoztatott járműegység jóváhagyási száma.

currentVUSerialNumber a külső GNSS-eszközhöz aktuálisan csatlakoztatott járműegység sorozatszáma.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

2. generáció:

A külső GNSS-eszköz operációs rendszerének azonosítója.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Érték-hozzárendelés: gyártóspecifikus.

2.137. **SensorExternalGNSSSCIdentifier**

2. generáció:

Ezt a típust például a külső GNSS-eszköz kriptográfiai moduljának azonosítására kell alkalmazni.

A külső GNSS-eszköz biztonsági alkatrészének azonosítója.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Érték-hozzárendelés: alkatrészgyártó-specifikus.

2.138. **SensorGNSSCouplingDate**

2. generáció:

A külső GNSS-eszköz járműegységhez való csatlakoztatásának dátuma.

```
SensorGNSSCouplingDate ::= TimeReal
```

Érték-hozzárendelés: Nincs meghatározva.

2.139. **SensorGNSSSerialNumber**

2. generáció:

Ezt a típust a GNSS-vevő sorozatszámának tárolására kell alkalmazni, akár a járműegység belsejében, akár azon kívül található a GNSS-vevő.

A GNSS-vevő sorozatszáma.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Olyan, mozgásérzékelőben tárolt információ, amely a mozgásérzékelő azonosítására vonatkozik (1B melléklet, 077. követelmény és 1C melléklet, 95. követelmény).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber a mozgásérzékelő kibővített sorozatszáma (tartalmazza az alkatrészszámot és a gyártó kódját).

sensorApprovalNumber a mozgásérzékelő jóváhagyási száma.

sensorSCIdentifier a mozgásérzékelő biztonsági alkatrészének azonosítója.

▼B

sensorOSIdentifier a mozgásérzékelő operációs rendszerének azonosítója.

2.141. **SensorInstallation**

Olyan, mozgásérzékelőben tárolt információ, amely a mozgásérzékelő beépítésére vonatkozik (1B melléklet, 099. követelmény és 1C melléklet, 122. követelmény).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst a mozgásérzékelő járműegységgel való első párosításának dátuma.

firstVuApprovalNumber a mozgásérzékelővel párosított első járműegység jóváhagyási száma.

firstVuSerialNumber a mozgásérzékelővel párosított első járműegység sorozatszáma.

sensorPairingDateCurrent a mozgásérzékelő járműegységgel való aktuális párosításának dátuma.

currentVuApprovalNumber a mozgásérzékelővel aktuálisan párosított járműegység jóváhagyási száma.

currentVUSerialNumber a mozgásérzékelővel aktuálisan párosított járműegység sorozatszáma.

2.142. **SensorInstallationSecData**

Olyan, műhelykártyán tárolt információ, amely a mozgásérzékelők és a járműegységek párosításához szükséges biztonsági adatokra vonatkozik (1C melléklet, 308. és 331. követelmény).

1. generáció:

```
SensorInstallationSecData ::= TdesSessionKey
```

Érték-hozzárendelés: az ISO 16844-3 szabvánnyal összhangban.

2. generáció:

A 11. függelékben leírtak szerint egy műhelykártya legfeljebb három, járműegység–mozgásérzékelő párra vonatkozó kulcsot tárolhat. Ezeknek a kulcsoknak eltérő a kulcsverziója.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

A mozgásérzékelő operációs rendszerének azonosítója.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Érték-hozzárendelés: gyártóspecifikus.

2.144. **SensorPaired**

1. generáció:

Olyan, járműegységben tárolt információ, amely a járműegységgel párosított mozgásérzékelő azonosítására vonatkozik (1B melléklet, 079. követelmény).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber a járműegységgel aktuálisan párosított mozgásérzékelő sorozatszáma.

sensorApprovalNumber a járműegységgel aktuálisan párosított mozgásérzékelő jóváhagyási száma.

sensorPairingDateFirst a járműegységgel aktuálisan párosított mozgásérzékelő járműegységgel való első párosításának dátuma.

2.145. **SensorPairedRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely a járműegységgel párosított mozgásérzékelő azonosítására vonatkozik (1C melléklet, 97. követelmény).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber egy, a járműegységgel aktuálisan párosított mozgásérzékelő sorozatszáma.

sensorApprovalNumber a mozgásérzékelő jóváhagyási száma.

sensorPairingDate e mozgásérzékelő járműegységgel való párosításának dátuma.

2.146. **SensorPairingDate**

A mozgásérzékelő járműegységgel való párosításának dátuma.

```
SensorPairingDate ::= TimeReal
```

Érték-hozzárendelés: Nincs meghatározva.

▼B

2.147. **SensorSCIdentifier**

A mozgásérzékelő biztonsági alkatrészének azonosítója.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Érték-hozzárendelés: alkatrészgyártó-specifikus.

2.148. **SensorSerialNumber**

A mozgásérzékelő sorozatszáma.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Egy digitális aláírás.

1. generáció:

```
Signature ::= OCTET STRING (SIZE(128))
```

Érték-hozzárendelés: a 11. függelékben meghatározott általános biztonsági mechanizmusoknak megfelelően.

2. generáció:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Érték-hozzárendelés: a 11. függelékben meghatározott általános biztonsági mechanizmusoknak megfelelően.

2.150. **SignatureRecordArray**

2. generáció:

Aláírások sorozata plusz a letöltési protokollban használt metaadatok.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType a rekord (Signature) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a Signature mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma. Az értéket 1-re kell állítani, mivel az aláírások eltérő hosszúságúak lehetnek.

records az aláírások sorozata.

2.151. **SimilarEventsNumber**

A hasonló események száma egy adott napon (1B melléklet, 094. követelmény és 1C melléklet, 117. követelmény).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Érték-hozzárendelés: A 0-t nem lehet használni, az 1 azt jelenti, hogy csak egyetlen ilyen típusú esemény történt és lett eltárolva az adott napon, a 2 azt jelenti, hogy 2 ilyen típusú esemény történt az adott napon (csak egy került tárolásra), …, a 255 pedig azt jelenti, hogy 255 vagy annál több ilyen típusú esemény történt az adott napon.

▼B

2.152. **SpecificConditionRecord**

Olyan, járművezetői vagy műhelykártyán vagy járműegységben tárolt információ, amely egy különleges körülményre vonatkozik (1C melléklet, 130., 276., 301., 328. és 355. követelmény).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   specificConditionType              SpecificConditionType
}
```

entryTime a betáplálás dátuma és ideje.

specificConditionType a különleges körülményt azonosító kód.

2.153. **SpecificConditions**

Olyan, járművezetői vagy műhelykártyán vagy járműegységben tárolt információ, amely egy különleges körülményre vonatkozik (1C melléklet, 131., 277., 302., 329. és 356. követelmény).

2. generáció:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord       INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords           SET SIZE(NoOfSpecificConditionRecords) OF
                                      SpecificConditionRecord
}
```

conditionPointerNewestRecord az utoljára aktualizált különlegeskörülmény-rekord indexe.

Érték-hozzárendelés: A különlegeskörülmény-rekord számlálójának megfelelő szám, amely a különlegeskörülmény-rekordnak a szerkezetben való első előfordulásakor „0”-val kezdődik.

specificConditionRecords a rögzített különleges körülményekre vonatkozó információkat tartalmazó rekordok sorozata.

2.154. **SpecificConditionType**

Egy különleges körülményt azonosító kód (1B melléklet, 050b., 105a., 212a. és 230a. követelmény, és 1C melléklet, 62. követelmény).

```
SpecificConditionType ::= INTEGER(0..255)
```

1. generáció:

Érték-hozzárendelés:

‘00’H	RFU
‘01’H	Menetíró készülék nem szükséges – Kezdet
‘02’H	Menetíró készülék nem szükséges – Befejezés
‘03’H	Kompon/vonaton megtett út
‘04’H … ‘FF’H	RFU

2. generáció:

Érték-hozzárendelés:

‘00’H	RFU
‘01’H	Menetíró készülék nem szükséges – Kezdet
‘02’H	Menetíró készülék nem szükséges – Befejezés
‘03’H	Kompon/vonaton megtett út – Kezdet
‘04’H	Kompon/vonaton megtett út – Befejezés
‘05’H … ‘FF’H	RFU

▼B

2.155. **Speed**

A jármű sebessége (km/h).

```
Speed ::= INTEGER(0..255)
```

Érték-hozzárendelés: km/h-ban kifejezett érték a 0-tól 220 km/h-ig terjedő működési tartományban.

2.156. **SpeedAuthorised**

A jármű maximális engedélyezett sebessége [bb) definíció].

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Átlagsebesség egy előzetesen meghatározott időtartam alatt (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Egy előzetesen meghatározott időtartam alatt mért maximális sebesség.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

2. generáció:

Ennek az adattípusnak a meghatározását lásd a 14. függelékben.

2.160. **TachographPayloadEncrypted**

2. generáció:

A tachográf DER-TLV szerint titkosított hasznos adata, azaz az RTM üzenetben titkosítva küldött adatok. A titkosítást lásd a 11. függelék B részének 13. fejezetében.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag a DER-TLV kódolás része, értékét ‘87’-re kell beállítani (lásd a 11. függelék B részének 13. fejezetét).

length a DER-TLV kódolás része, a következő paddingContentIndicatorByte és encryptedData hosszát tartalmazza.

paddingContentIndicatorByte értékét ‘00’-ra kell állítani.

encryptedData a titkosított tachographPayload a 11. függelék B részének 13. fejezetében meghatározott módon. Ezen adat oktettben megadott hosszának mindig a 16 többszörösének kell lennie.

2.161. **TDesSessionKey**

1. generáció:

Egy háromszoros DES munkamenetkulcs.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Érték-hozzárendelés: nincs közelebbi meghatározás.

▼B

2.162. **TimeReal**

Egy kombinált dátum- és adatmezőre vonatkozó kód, ahol a dátum és az idő az 1970. január 1-je 00 ó. 00 p. 00 mp. (UTC) óta eltelt másodpercekben van kifejezve.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Érték-hozzárendelés – Rendezett oktett: Az 1970. január 1-je (UTC) éjfél óta eltelt másodpercek száma.

A legutolsó lehetséges dátum/idő 2106-ban található.

2.163. **TyreSize**

A gumiabroncs méreteinek jelölése.

```
TyreSize ::= IA5String(SIZE(15))
```

Érték-hozzárendelés: a 92/23/EGK irányelvvel (HL L 129., 1992.3.31., 95. o.) összhangban.

2.164. **VehicleIdentificationNumber**

A jármű alvázszáma (VIN), amely a járműre mint egészre vonatkozik, rendszerint az alváz sosorzatszáma vagy az alvázkeret száma.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Érték-hozzárendelés: Az ISO 3779 szabvány fogalommeghatározása szerint.

2.165. **VehicleIdentificationNumberRecordArray**

2. generáció:

A jármű alvázszáma plusz a letöltési protokollban használt metaadatok.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType a rekord (VehicleIdentificationNumber) típusát jelöli.
Érték-hozzárendelés: Lásd: RecordType

recordSize a VehicleIdentificationNumber mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a járművek alvázszámainak sorozata.

2.166. **VehicleRegistrationIdentification**

A jármű Európára vonatkozóan egyedi azonosítása (rendszám és tagállam).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation azon ország, amelyben a jármű nyilvántartásba vétele történt.

▼B

vehicleRegistrationNumber a jármű rendszáma (VRN).

2.167. **VehicleRegistrationNumber**

A jármű rendszáma (VRN). A rendszámot a járművet nyilvántartásba vevő hatóság adja ki.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   vehicleRegNumber                  OCTET STRING (SIZE(13))
}
```

codePage a 4. fejezetben meghatározott karakterkészletet adja meg,

vehicleRegNumber a meghatározott karakterkészlet felhasználásával kódolt rendszám.

Érték-hozzárendelés: országspecifikus.

2.168. **VehicleRegistrationNumberRecordArray**

2. generáció:

A rendszám plusz a letöltési protokollban használt metaadatok.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                        RecordType,
   recordSize                        INTEGER(1..65535),
   noOfRecords                       INTEGER(0..65535),
   records                           SET SIZE(noOfRecords) OF
                                     VehicleRegistrationNumber
}
```

recordType a rekord (VehicleRegistrationNumber) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VehicleRegistrationNumber mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a járművek rendszámainak sorozata.

2.169. **VuAbility**

2. generáció:

A járműegységben arról tárolt információ, hogy a járműegységben használhatók-e az 1. generációba tartozó tachográfkártyák, vagy sem (1C melléklet, 121. követelmény).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Érték-hozzárendelés – Rendezett oktett: ‘xxxxxxxa’B (8 bit)

Az 1. generáció támogatása szempontjából:

‘a’B	A tachográfkártyák 1. generációjának támogatására való képesség
	‘0’ B Az 1. generáció támogatott,
	‘1’ B Az 1. generáció nem támogatott,
‘xxxxxxx’B	RFU

▼B

2.170. **VuActivityDailyData**

1. generáció:

Olyan, járműegységben tárolt információ, amely egy adott naptári napon bekövetkező tevékenységváltásokra és/vagy járművezetésiállapot-váltásokra és/vagy kártyaállapot-váltásokra (1B melléklet, 084. követelmény és 1C melléklet, 105., 106. és 107. követelmény), valamint a kártyaolvasó egységek adott napon 00 óra 00 perckori állapotára vonatkozik.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                    INTEGER SIZE(0..1440),
   activityChangeInfos                    SET SIZE(noOfActivityChanges) OF
                                          ActivityChangeInfo
}
```

noOfActivityChanges az ActivityChangeInfo szavak száma az activityChangeInfos sorozatban.

activityChangeInfos a járműegységben az adott napra tárolt ActivityChangeInfo szavak sorozata. Mindig tartalmaz két ActivityChangeInfo szót, amelyek megadják a két kártyaolvasó egység állapotát az adott napon 00:00-kor.

2.171. **VuActivityDailyRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely egy adott naptári napon bekövetkező tevékenységváltásokra és/vagy járművezetésiállapot-váltásokra és/vagy kártyaállapot-váltásokra (1C melléklet, 105., 106. és 107. követelmény), valamint a kártyaolvasó egységek adott napon 00 óra 00 perckori állapotára vonatkozik.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType a rekord (ActivityChangeInfo) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a ActivityChangeInfo mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a járműegységben az adott napra tárolt ActivityChangeInfo szavak sorozata. Mindig tartalmaz két ActivityChangeInfo szót, amelyek megadják a két kártyaolvasó egység állapotát az adott napon 00:00-kor.

2.172. **VuApprovalNumber**

A járműegység típus-jóváhagyási száma.

1. generáció:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Érték-hozzárendelés: Nincs meghatározva.

2. generáció:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Érték-hozzárendelés:

A jóváhagyási számot az Európai Bizottság megfelelő honlapján közzétett formában, azaz adott esetben például kötőjelekkel együtt kell megadni. A jóváhagyási számot balra kell igazítani.

2.173. **VuCalibrationData**

1. generáció:

Olyan, járműegységben tárolt információ, amely az adatrögzítő készülék kalibrálásaira vonatkozik (1B melléklet, 098. követelmény).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords              INTEGER(0..255),
   vuCalibrationRecords                  SET SIZE(noOfVuCalibrationRecords) OF
                                         VuCalibrationRecord
}
```

noOfVuCalibrationRecords a vuCalibrationRecords sorozatban található rekordok száma.

vuCalibrationRecords a kalibrálási rekordok sorozata.

2.174. **VuCalibrationRecord**

Olyan, járműegységben tárolt információ, amely az adatrögzítő készülék kalibrálására vonatkozik (1B melléklet, 098. követelmény és 1C melléklet, 119. és 120. követelmény).

1. generáció:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose a kalibrálás célja.

workshopName, workshopAddress a műhely neve és címe.

workshopCardNumber a kalibrálás alatt használt műhelykártyát azonosítja.

workshopCardExpiryDate a kártya érvényességi ideje.

vehicleIdentificationNumber a jármű alvázszáma.

▼B

vehicleRegistrationIdentification a rendszámot és a nyilvántartásba vétel szerinti tagállamot tartalmazza.

wVehicleCharacteristicConstant a jármű jellemző együtthatója.

kConstantOfRecordingEquipment a menetíró készülék állandója.

lTyreCircumference a kerék gumiabroncsainak tényleges kerülete.

tyreSize a járműre szerelt gumiabroncsok méreteinek jelölése.

authorisedSpeed a jármű engedélyezett sebessége.

oldOdometerValue, newOdometerValue a kilométer-számláló régi és új értékei.

oldTimeValue, newTimeValue a dátum és az idő régi és új értékei.

nextCalibrationDate a jóváhagyott felülvizsgálati szerv által legközelebb végrehajtandó, a CalibrationPurpose-ban meghatározott típusú kalibrálás dátuma.

2. generáció:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemet kell alkalmazni:

sealDataVu a jármű különböző alkatrészeire erősített plombákról szolgáltat információkat.

2.175. **VuCalibrationRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely az adatrögzítő készülék kalibrálásaira vonatkozik (1C melléklet, 119. és 120. követelmény).

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuCalibrationRecord
}
```

recordType a rekord (VuCalibrationRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuCalibrationRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a kalibrálási rekordok sorozata.

2.176. **VuCardIWData**

1. generáció:

Olyan, járműegységben tárolt információ, amely a járműegységben a járművezetői kártyák vagy műhelykártyák behelyezésének és kivételének ciklusaira vonatkozik (1B melléklet, 081. követelmény és 1C melléklet, 103. követelmény).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                          INTEGER(0..2^16-1),
   vuCardIWRecords                        SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords a vuCardIWRecords sorozatban található rekordok száma.

vuCardIWRecords a kártyabehelyezés- és -kivételciklusokra vonatkozó rekordok sorozata.

2.177. **VuCardIWRecord**

Olyan, járműegységben tárolt információ, amely a járműegységben egy járművezetői kártya vagy műhelykártya behelyezésének és kivételének ciklusára vonatkozik (1B melléklet, 081. követelmény és 1C melléklet, 102. követelmény).

1. generáció:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumber                          FullCardNumber,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo,
   manualInputFlag                         ManualInputFlag
}
```

cardHolderName a járművezetői kártya vagy a műhelykártya tulajdonosának családi neve és utóneve(i) a kártyán tárolt formában.

fullCardNumber a kártya típusa, a kiállító tagállam, és a kártyaszám, a kártyán tárolt formában.

▼B

cardExpiryDate a kártya érvényességi ideje, a kártyán tárolt formában.

cardInsertionTime a behelyezés dátuma és ideje.

vehicleOdometerValueAtInsertion a jármű kilométer-számlálójának értéke a kártya behelyezésekor.

cardSlotNumber azon kártyaolvasó egység, amelybe a kártyát be kell helyezni.

cardWithdrawalTime a kivétel dátuma és ideje.

vehicleOdometerValueAtWithdrawal a jármű kilométer-számlálójának értéke a kártya kivételekor.

previousVehicleInfo a járművezető által használt előző járműről tartalmaz információt, a kártyán tárolt formában.

manualInputFlag egy olyan jelölő, amely a kártyatulajdonos által a kártya behelyezésekor manuálisan betáplált járművezetői tevékenységeket azonosítja.

2. generáció:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                         HolderName,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   cardExpiryDate                         TimeReal,
   cardInsertionTime                      TimeReal,
   vehicleOdometerValueAtInsertion        OdometerShort,
   cardSlotNumber                         CardSlotNumber,
   cardWithdrawalTime                     TimeReal,
   vehicleOdometerValueAtWithdrawal       OdometerShort,
   previousVehicleInfo                    PreviousVehicleInfo,
   manualInputFlag                        ManualInputFlag
}
```

A fullCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

fullCardNumberAndGeneration a kártya típusa, a kiállító tagállam, a kártyaszám és a generáció, a kártyán tárolt formában.

2.178. **VuCardIWRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a járműegységben a járművezetői kártyák vagy műhelykártyák behelyezésének és kivételének ciklusaira vonatkozik (1C melléklet, 103. követelmény).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType a rekord (VuCardIWRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuCardIWRecord mérete bájtokban kifejezve.

▼B

noOfRecords a sorozatban található rekordok száma.

records a kártyabehelyezés- és -kivételciklusokra vonatkozó rekordok sorozata.

2.179. **VuCardRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely egy használatban lévő tachográfkártyára vonatkozik (1C melléklet, 132. követelmény).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber a kártya mesterfájljában található EF_ICC fájlból kiolvasott érték.

cardPersonaliserID a kártya mesterfájljában található EF_ICC fájlból kiolvasott érték.

typeOfTachographCardId a DF_Tachograph_G2 fájlban található EF_Application_Identification fájlból kiolvasott érték.

cardStructureVersion a DF_Tachograph_G2 fájlban található EF_Application_Identification fájlból kiolvasott érték.

cardNumber a DF_Tachograph_G2 fájlban található EF_Identification fájlból kiolvasott érték.

2.180. **VuCardRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a szóban forgó járműegységben használt tachográfkártyákra vonatkozik). Ez az információ a járműegység és a kártya közötti problémák elemzésére szolgál (1C melléklet, 132. követelmény).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType a rekord (VuCardRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuCardRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a járműegységben használt tachográfkártyákra vonatkozó rekordok sorozata.

▼B

2.181. **VuCertificate**

Egy járműegység nyilvános kulcsának tanúsítványa.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

2. generáció:

A járműegység tanúsítványa plusz a letöltési protokollban használt metaadatok.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType a rekord (VuCertificate) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuCertificate mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma. Az értéket 1-re kell állítani, mivel a tanúsítványok eltérő hosszúságúak lehetnek.

records a járműegységek tanúsítványainak sorozata.

2.183. **VuCompanyLocksData**

1. generáció:

Olyan, járműegységben tárolt információ, amely vállalkozás általi lezárásokra vonatkozik (1B melléklet, 104. követelmény).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks a vuCompanyLocksRecords-ban felsorolt lezárások száma.

vuCompanyLocksRecords a vállalkozás általi lezárások rekordjainak sorozata.

2.184. **VuCompanyLocksRecord**

Olyan, járműegységben tárolt információ, amely egy vállalkozás általi lezárásra vonatkozik (1B melléklet, 104. követelmény és 1C melléklet, 128. követelmény).

1. generáció:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime a lezárás és a feloldás dátuma és ideje.

companyName, companyAddress azon vállalkozás neve és címe, amelyre a lezárás vonatkozik.

companyCardNumber a lezáráskor használt kártyát azonosítja.

2. generáció:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

A companyCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

companyCardNumberAnd Generation a lezáráskor használt kártyát és annak generációját azonosítja.

2.185. **VuCompanyLocksRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely vállalkozás általi lezárásokra vonatkozik (1C melléklet, 128. követelmény).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType a rekord (VuCompanyLocksRecord) típusát jelöli. **Értékhozzárendelés:** Lásd: RecordType

recordSize a VuCompanyLocksRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma. Érték: 0..255.

records a vállalkozás általi lezárások rekordjainak sorozata.

2.186. **VuControlActivityData**

1. generáció:

Olyan, járműegységben tárolt információ, amely az e járműegységgel végzett ellenőrzésekre vonatkozik (1B melléklet, 102. követelmény).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls a vuControlActivityRecords-ban felsorolt ellenőrzések száma.

vuControlActivityRecords az ellenőrző tevékenységi rekordok sorozata.

2.187. **VuControlActivityRecord**

Olyan, járműegységben tárolt információ, amely egy e járműegységgel végzett ellenőrzésre vonatkozik (1B melléklet, 102. követelmény és 1C melléklet, 126. követelmény).

1. generáció:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType az ellenőrzés típusa.

controlTime az ellenőrzés dátuma és ideje.

controlCardNumber az ellenőrzéshez használt ellenőrzőkártyát azonosítja.

downloadPeriodBeginTime letöltés esetén a letöltési időtartam kezdési ideje.

downloadPeriodEndTime letöltés esetén a letöltési időtartam bfejezési ideje.

2. generáció:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

A controlCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

controlCardNumberAndGeneration az ellenőrzéshez használt ellenőrzőkártyát és annak generációját azonosítja.

2.188. **VuControlActivityRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely az e járműegységgel végzett ellenőrzésekre vonatkozik (1C melléklet, 126. követelmény).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuControlActivityRecord
}
```

recordType a rekord (VuControlActivityRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuControlActivityRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

record a járműegység ellenőrző tevékenységi rekordjainak sorozata.

2.189. **VuDataBlockCounter**

A kártyán tárolt számláló, amely folyamatosan azonosítja a kártya járműegységekbe való behelyezésének és kivételének ciklusait.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Érték-hozzárendelés: Folyamatos számozás, amelynek a maximális értéke = 9999, a számozás 0-val kezdődik újra.

2.190. **VuDetailedSpeedBlock**

Olyan, járműegységben tárolt információ, amely a jármű mozgás közben egy percen keresztül mért pontos sebességére vonatkozik (1B melléklet, 093. követelmény és 1C melléklet, 116. követelmény).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate az adatblokkon belül az első sebességérték dátuma és ideje.

speedsPerSecond a speedBlockBeginDate-től kezdődő perc minden másodpercében (a speedBlockBeginDate-et is beleértve) mért sebességek időrendi sorrendje.

2.191. **VuDetailedSpeedBlockRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a jármű részletes sebességére vonatkozik.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDetailedSpeedBlock
}
```

recordType a rekord (VuDetailedSpeedBlock) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

▼B

recordSize a VuDetailedSpeedBlock mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a részletes sebességblokkok sorozata.

2.192. **VuDetailedSpeedData**

1. generáció:

Olyan, járműegységben tárolt információ, amely a jármű részletes sebességére vonatkozik.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                         INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks                   SET SIZE(noOfSpeedBlocks) OF
                                           VuDetailedSpeedBlock
}
```

noOfSpeedBlocks a vuDetailedSpeedBlocks sorozatban található sebességblokkok száma.

vuDetailedSpeedBlocks a részletes sebességblokkok sorozata.

2.193. **VuDownloadablePeriod**

Azon legrégebbi és legújabb dátumok, amelyekre vonatkozóan a járműegység a járművezető tevékenységeit érintő adatokat tartalmaz (1B melléklet, 081., 084. vagy 087. követelmény és 1C melléklet, 102., 105. és 108. követelmény).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                     TimeReal
   maxDownloadableTime                     TimeReal
}
```

minDownloadableTime kártyabehelyezésnek, tevékenységváltásnak vagy helybetáplálásnak a járműegységben tárolt legrégebbi dátuma és ideje.

maxDownloadableTime kártyakivételnek, tevékenységváltásnak vagy helybetáplálásnak a járműegységben tárolt legutóbbi dátuma és ideje.

2.194. **VuDownloadablePeriodRecordArray**

2. generáció:

A VUDownloadablePeriod plusz a letöltési protokollban használt metaadatok.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDownloadablePeriod
}
```

recordType a rekord (VuDownloadablePeriod) típusát jelöli. **Értékhozzárendelés:** Lásd: RecordType

▼B

recordSize a VuDownloadablePeriod mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a VuDownloadablePeriod rekordok sorozata.

2.195. **VuDownloadActivityData**

Olyan, járműegységben tárolt információ, amely annak legutolsó letöltésére vonatkozik (1B melléklet, 105. követelmény és 1C melléklet, 129. követelmény).

1. generáció:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime a letöltés dátuma és ideje.

fullCardNumber a letöltés engedélyezésére használt kártyát azonosítja.

companyOrWorkshopName a vállalkozás vagy a műhely neve.

2. generáció:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   companyOrWorkshopName                  Name
}
```

A fullCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

fullCardNumberAndGeneration a letöltés engedélyezésére használt kártyát és annak generációját azonosítja.

2.196. **VuDownloadActivityDataRecordArray**

2. generáció:

A járműegységből történő legutolsó letöltésre vonatkozó információ (1C melléklet, 129. követelmény).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType a rekord (VuDownloadActivityData) típusát jelöli. **Értékhozzárendelés:** Lásd: RecordType

recordSize a VuDownloadActivityData mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

▼B

records a letöltésitevékenység-adatok rekordjainak sorozata.

2.197. **VuEventData**

1. generáció:

Olyan, járműegységben tárolt információ, amely eseményekre vonatkozik (1B melléklet, 094. követelmény, kivéve a gyorshajtási eseményt).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents a vuEventRecords sorozatban felsorolt események száma.

vuEventRecords eseményrekordok sorozata.

2.198. **VuEventRecord**

Olyan, járműegységben tárolt információ, amely egy eseményre vonatkozik (1B melléklet, 094. követelmény és 1C melléklet, 117. követelmény, kivéve a gyorshajtási eseményt).

1. generáció:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType az esemény típusa.

eventRecordPurpose az esemény rögzítésének célja.

eventBeginTime az esemény kezdetének dátuma és ideje.

eventEndTime az esemény befejeződésének dátuma és ideje.

cardNumberDriverSlotBegin az esemény kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberCodriverSlotBegin az esemény kezdetekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberDriverSlotEnd az esemény befejeződésekor a járművezetői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberCodriverSlotEnd az esemény befejeződésekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát azonosítja.

similarEventsNumber az adott napon előforduló hasonló események száma.

E sorozat a gyorshajtás eseményén kívül minden eseményhez felhasználható.

▼B

2. generáció:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemeket kell alkalmazni:

manufacturerSpecificEventFaultData további, gyártóspecifikus információt tartalmaz az eseményről.

A cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd és cardNumberCodriverSlotEnd helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

cardNumberAndGenDriverSlotBegin az esemény kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotBegin az esemény kezdetekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenDriverSlotEnd az esemény befejeződésekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotEnd az esemény befejeződésekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

Ha az esemény időütközést idéz elő, akkor az eventBeginTime és az eventEndTime adatot a következőképpen kell értelmezni:

eventBeginTime az adatrögzítő készülék dátuma és ideje.

eventEndTime a GNSS dátuma és ideje.

2.199. **VuEventRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely eseményekre vonatkozik (1C melléklet, 117. követelmény, kivéve a gyorshajtási eseményt).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType a rekord (VuEventRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

▼B

recordSize a VuEventRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records eseményrekordok sorozata.

2.200. **VuFaultData**

1. generáció:

Olyan, járműegységben tárolt információ, amely hibákra vonatkozik (1B melléklet, 096. követelmény).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults a vuFaultRecords sorozatban felsorolt hibák száma.

vuFaultRecords hibarekordok sorozata.

2.201. **VuFaultRecord**

Olyan, járműegységben tárolt információ, amely hibákra vonatkozik (1B melléklet, 096. követelmény és 1C melléklet, 118. követelmény).

1. generáció:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType az adatrögzítő készülék hibájának típusa.

faultRecordPurpose a hiba rögzítésének célja.

faultBeginTime a hiba kezdetének dátuma és ideje.

faultEndTime a hiba befejeződésének dátuma és ideje.

cardNumberDriverSlotBegin a hiba kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberCodriverSlotBegin a hiba kezdetekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberDriverSlotEnd a hiba befejeződésekor a járművezetői kártyaolvasó egységbe behelyezett kártyát azonosítja.

cardNumberCodriverSlotEnd a hiba befejeződésekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát azonosítja.

▼B

2. generáció:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemet kell alkalmazni:

manufacturerSpecificEventFaultData további, gyártóspecifikus információt tartalmaz a hibáról.

A cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd és cardNumberCodriverSlotEnd helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

cardNumberAndGenDriverSlotBegin a hiba kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotBegin a hiba kezdetekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenDriverSlotEnd a hiba befejeződésekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotEnd a hiba befejeződésekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

2.202. **VuFaultRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely hibákra vonatkozik (1C melléklet, 118. követelmény).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType a rekord (VuFaultRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuFaultRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records hibarekordok sorozata.

▼B

2.203. **VuGNSSCDRecord**

2. generáció:

Járműegységben abban az esetben eltárolt, a jármű GNSS-helyzetére vonatkozó információ, ha a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét (1C melléklet, 108. és 110. követelmény).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   cardNumberAndGenDriverSlot         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot       FullCardNumberAndGeneration,
   gnssPlaceRecord                    GNSSPlaceRecord
}
```

timeStamp annak az időpontnak a dátuma és ideje, amikor a kártyatulajdonos megszakítás nélküli járművezetési ideje eléri a három óra többszörösét.

cardNumberAndGenDriverSlot a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlot a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

gnssPlaceRecord a jármű helyzetére vonatkozó információt tartalmazza.

2.204. **VuGNSSCDRecordArray**

2. generáció:

Járműegységben abban az esetben eltárolt, a jármű GNSS-helyzetére vonatkozó információ, ha a járművezető megszakítás nélküli járművezetési ideje eléri a három óra többszörösét (1C melléklet, 108. és 110. követelmény).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType a rekord (VuGNSSCDRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuGNSSCDRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a GNSS megszakítás nélküli járművezetési rekordok sorozata.

2.205. **VuIdentification**

Olyan, járműegységben tárolt információ, amely a járműegység azonosítására vonatkozik (1B melléklet, 075. követelmény és 1C melléklet, 93. és 121. követelmény).

▼B

1. generáció:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName a járműegység gyártójának neve.

vuManufacturerAddress a járműegység gyártójának címe.

vuPartNumber a járműegység alkatrészszáma.

vuSerialNumber a járműegység sorozatszáma.

vuSoftwareIdentification a járműegységben alkalmazott szoftvert azonosítja.

vuManufacturingDate a járműegység gyártási dátuma.

vuApprovalNumber a járműegység típus-jóváhagyási száma.

2. generáció:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber,
   vuGeneration                          Generation,
   vuAbility                             VuAbility
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemeket kell alkalmazni:

vuGeneration a járműegység generációját azonosítja.

vuAbility arról szolgáltat információt, hogy a járműegység támogatja-e a tachográfkártyák 1. generációját, vagy sem.

2.206. **VuIdentificationRecordArray**

2. generáció:

A VuIdentification plusz a letöltési protokollban használt metaadatok.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType a rekord (VuIdentification) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuIdentification mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records VuIdentification rekordok sorozata.

2.207. **VuITSConsentRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely a járművezető által az intelligens közlekedési rendszerek használatához adott beleegyezésre vonatkozik.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAnd Gen a kártyát és annak generációját azonosítja. Ennek a járművezetői kártyának vagy a műhelykártyának kell lennie.

consent jelző, amely azt jelzi, hogy a járművezető beleegyezését adta-e az intelligens közlekedési rendszerek adott járművön/járműegységben való használatához, vagy sem.

Érték-hozzárendelés:

IGAZ	azt jelzi, hogy a járművezető beleegyezett az intelligens közlekedési rendszerek használatába
HAMIS	azt jelzi, hogy a járművezető megtagadta az intelligens közlekedési rendszerek használatát

2.208. **VuITSConsentRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a járművezető intelligens közlekedési rendszerek használatába való beleegyezésére vonatkozik (1C melléklet, 200. követelmény).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType a rekord (VuITSConsentRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuITSConsentRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records az intelligens közlekedési rendszerek használatára vonatkozó beleegyezésrekordok sorozata.

▼B

2.209. **VuManufacturerAddress**

A járműegység gyártójának címe.

```
VuManufacturerAddress ::= Address
```

Érték-hozzárendelés: Nincs meghatározva.

2.210. **VuManufacturerName**

A járműegység gyártójának neve.

```
VuManufacturerName ::= Name
```

Érték-hozzárendelés: Nincs meghatározva.

2.211. **VuManufacturingDate**

A járműegység gyártási dátuma.

```
VuManufacturingDate ::= TimeReal
```

Érték-hozzárendelés: Nincs meghatározva.

2.212. **VuOverSpeedingControlData**

Olyan, járműegységben tárolt információ, amely az utolsó gyorshajtás-ellenőrzés óta történt gyorshajtási eseményekre vonatkozik (1B melléklet, 095. követelmény és 1C melléklet, 117. követelmény).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime az utolsó gyorshajtás-ellenőrzés dátuma és ideje.

firstOverspeedSince az ezt a gyorshajtás-ellenőrzést követő első gyorshajtás dátuma és ideje.

numberOfOverspeedSince az utolsó gyorshajtás-ellenőrzés óta történt gyorshajtási események száma.

2.213. **VuOverSpeedingControlDataRecordArray**

2. generáció:

A VuOverSpeedingControlData plusz a letöltési protokollban használt metaadatok.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType a rekord (VuOverSpeedingControlData) típusát jelöli.
Érték-hozzárendelés: Lásd: RecordType

recordSize a VuOverSpeedingControlData mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a gyorshajtás-ellenőrzési adatok rekordjainak sorozata.

2.214. **VuOverSpeedingEventData**

1. generáció:

Olyan, járműegységben tárolt információ, amely gyorshajtási eseményekre vonatkozik (1B melléklet, 094. követelmény).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents a vuOverSpeedingEventRecords sorozatban felsorolt események száma.

vuOverSpeedingEventRecords a gyorshajtási események rekordjainak sorozata.

2.215. **VuOverSpeedingEventRecord**

1. generáció:

Olyan, járműegységben tárolt információ, amely gyorshajtási eseményekre vonatkozik (1B melléklet, 094. követelmény és 1C melléklet, 117. követelmény).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType az esemény típusa.

eventRecordPurpose az esemény rögzítésének célja.

eventBeginTime az esemény kezdetének dátuma és ideje.

eventEndTime az esemény befejeződésének dátuma és ideje.

maxSpeedValue az esemény alatt mért maximális sebesség.

averageSpeedValue az esemény alatt mért sebességek számtani átlaga.

▼B

cardNumberDriverSlotBegin az esemény kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát azonosítja.

similarEventsNumber az adott napon előforduló hasonló események száma.

2. generáció:

Olyan, járműegységben tárolt információ, amely gyorshajtási eseményekre vonatkozik (1B melléklet, 094. követelmény és 1C melléklet, 117. követelmény).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   maxSpeedValue                          SpeedMax,
   averageSpeedValue                      SpeedAverage,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber
}
```

A cardNumberDriverSlotBegin helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

cardNumberAndGenDriverSlotBegin az esemény kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

2.216. **VuOverSpeedingEventRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely gyorshajtási eseményekre vonatkozik (1C melléklet, 117. követelmény).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF
                                          VuOverSpeedingEventRecord
}
```

recordType a rekord (VuOverSpeedingEventRecord) típusát jelöli.
Érték-hozzárendelés: Lásd: RecordType

recordSize a VuOverSpeedingEventRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a gyorshajtási események rekordjainak sorozata.

2.217. **VuPartNumber**

A járműegység alkatrészszáma.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Érték-hozzárendelés: A járműegység gyártójára jellemző.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

1. generáció:

Olyan, járműegységben tárolt információ, amely olyan helyekre vonatkozik, ahol a járművezetők a munkanapot megkezdik vagy befejezik (1B melléklet, 087. követelmény és 1C melléklet, 108. és 110. követelmény).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords a vuPlaceDailyWorkPeriodRecords sorozatban felsorolt rekordok száma.

vuPlaceDailyWorkPeriodRecords a helyre vonatkozó rekordok sorozata.

2.219. **VuPlaceDailyWorkPeriodRecord**

1. generáció:

Olyan, járműegységben tárolt információ, amely olyan helyre vonatkozik, ahol egy járművezető a munkanapot megkezdi vagy befejezi (1B melléklet, 087. követelmény és 1C melléklet, 108. és 110. követelmény).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber a járművezető kártyájának típusa, a kártyát kiállító tagállam és a kártyaszám.

placeRecord a betáplált helyre vonatkozó információt tartalmazza.

2. generáció:

Olyan, járműegységben tárolt információ, amely olyan helyre vonatkozik, ahol egy járművezető a munkanapot megkezdi vagy befejezi (1B melléklet, 087. követelmény és 1C melléklet, 108. és 110. követelmény).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

A fullCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

fullCardNumberAndGeneration a kártya típusa, a kiállító tagállam, a kártyaszám és a generáció, a kártyán tárolt formában.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely olyan helyekre vonatkozik, ahol a járművezető a munkanapot megkezdi vagy befejezi (1C melléklet, 108. és 110. követelmény).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType a rekord (VuPlaceDailyWorkPeriodRecord) típusát jelöli.
Érték-hozzárendelés: Lásd: RecordType

recordSize a VuPlaceDailyWorkPeriodRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a helyre vonatkozó rekordok sorozata.

2.221. **VuPrivateKey**

1. generáció:

A járműegység privát kulcs kulcsa.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

1. generáció:

A járműegység nyilvános kulcsa.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

A járműegység sorozatszáma (1B melléklet, 075. követelmény és 1C melléklet, 93. követelmény).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

A járműegység szoftververziójának telepítési dátuma.

```
VuSoftInstallationDate ::= TimeReal
```

Érték-hozzárendelés: Nincs meghatározva.

▼B

2.225. **VuSoftwareIdentification**

Olyan, járműegységben tárolt információ, amely a telepített szoftverre vonatkozik.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion a járműegység szoftververziójának száma.

vuSoftInstallationDate a szoftververzió telepítésének dátuma.

2.226. **VuSoftwareVersion**

A járműegység szoftververziójának száma.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Érték-hozzárendelés: Nincs meghatározva.

2.227. **VuSpecificConditionData**

1. generáció:

Olyan, járműegységben tárolt információ, amely különleges körülményekre vonatkozik.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords a specificConditionRecords sorozatban felsorolt rekordok száma.

specificConditionRecords a különleges körülményekre vonatkozó rekordok sorozata.

2.228. **VuSpecificConditionRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely különleges körülményekre vonatkozik (1C melléklet, 130. követelmény).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType a rekord (SpecificConditionRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a SpecificConditionRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a különleges körülményekre vonatkozó rekordok sorozata.

▼B

2.229. **VuTimeAdjustmentData**

1. generáció:

Olyan, járműegységben tárolt információ, amely a rendes kalibrálás keretein kívül végrehajtott időbeállításokra vonatkozik (1B melléklet, 101. követelmény).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                    INTEGER(0..6),
   vuTimeAdjustmentRecords                 SET SIZE(noOfVuTimeAdjRecords) OF
                                           VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords a vuTimeAdjustmentRecords sorozatban található rekordok száma.

vuTimeAdjustmentRecords az időbeállítási tételek sorozata.

2.230. **VuTimeAdjustmentGNSSRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely a GNSS-rendszer által szolgáltatott időadatokon alapuló időbeállításra vonatkozik (1C melléklet, 124. és 125. követelmény).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal
}
```

oldTimeValue, newTimeValue a dátum és az idő régi és új értékei.

2.231. **VuTimeAdjustmentGNSSRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a GNSS-rendszer által szolgáltatott időadatok alapján végrehajtott időbeállításra vonatkozik (1C melléklet, 124. és 125. követelmény).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuTimeAdjustmentGNSSRecord
}
```

recordType a rekord (VuTimeAdjustmentGNSSRecord) típusát jelöli.
Érték-hozzárendelés: Lásd: RecordType

recordSize a VuTimeAdjustmentGNSSRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a GNSS időbeállítási rekordok sorozata.

▼B

2.232. **VuTimeAdjustmentRecord**

Olyan, járműegységben tárolt információ, amely a rendes kalibrálás keretein kívül végrehajtott időbeállításra vonatkozik (1B melléklet, 101. követelmény és 1C melléklet, 124. és 125. követelmény).

1. generáció:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue a dátum és az idő régi és új értékei.

workshopName, workshopAddress a műhely neve és címe.

workshopCardNumber az időbeállítás végrehajtásához használt műhelykártyát azonosítja.

2. generáció:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

A workshopCardNumber helyett a 2. generáció adatstruktúrája a következő adatelemeket alkalmazza.

workshopCardNumberAndGeneration az időbeállítás végrehajtásához használt műhelykártyát és annak generációját azonosítja.

2.233. **VuTimeAdjustmentRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely a rendes kalibrálás keretein kívül végrehajtott időbeállításokra vonatkozik (1C melléklet, 124. és 125. követelmény).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType a rekord (VuTimeAdjustmentRecord) típusát jelöli. **Értékhozzárendelés:** Lásd: RecordType

recordSize a VuTimeAdjustmentRecord mérete bájtokban kifejezve.

▼B

noOfRecords a sorozatban található rekordok száma.

records az időbeállítási rekordok sorozata.

2.234. **WorkshopCardApplicationIdentification**

Olyan, műhelykártyán tárolt információ, amely a kártya alkalmazásának azonosítására vonatkozik (1C melléklet, 307. és 330. követelmény).

1. generáció:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId meghatározza az alkalmazott kártyatípust.

cardStructureVersion a kártyán alkalmazott struktúra verzióját határozza meg.

noOfEventsPerType a kártyán eseménytípusonként tárolható események száma.

noOfFaultsPerType a kártyán hibatípusonként tárolható hibák száma.

activityStructureLength a tevékenységi rekordok eltárolására rendelkezésre álló bájtok számát jelzi.

noOfCardVehicleRecords a kártyán eltárolható járműrekordok száma.

noOfCardPlaceRecords a kártyán eltárolható helyek száma.

noOfCalibrationRecords a kártyán tárolható kalibrálási rekordok száma.

2. generáció:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemeket kell alkalmazni:

noOfGNSSCDRecords a kártyán tárolható GNSS megszakítás nélküli járművezetési rekordok száma.

▼B

noOfSpecificConditionRecords a kártyán tárolható különlegeskörülmény-rekordok száma.

2.235. **WorkshopCardCalibrationData**

Olyan, műhelykártyán tárolt információ, amely a kártyával végrehajtott műhelytevékenységre vonatkozik (1C melléklet, 314., 316., 337. és 339. követelmény).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber a kártyával végrehajtott kalibrálások száma összesen.

calibrationPointerNewestRecord az utoljára aktualizált kalibrálási rekord indexe.

Érték-hozzárendelés: A kalibrálási rekord számlálójának megfelelő szám, amely a kalibrálási rekordoknak a szerkezetben való első előfordulásakor „0”-val kezdődik.

calibrationRecords a kalibrálásra és/vagy időbeállításra vonatkozó információkat tartalmazó rekordok sorozata.

2.236. **WorkshopCardCalibrationRecord**

Olyan, műhelykártyán tárolt információ, amely a kártyával végrehajtott kalibrálásra vonatkozik (1C melléklet, 314. és 337. követelmény).

1. generáció:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose a kalibrálás célja.

vehicleIdentificationNumber a jármű alvázszáma.

vehicleRegistration a rendszámot és a nyilvántartásba vétele szerinti tagállamot tartalmazza.

wVehicleCharacteristicConstant a jármű jellemző együtthatója.

▼B

kConstantOfRecordingEquipment a menetíró készülék állandója.

lTyreCircumference a kerék gumiabroncsainak tényleges kerülete.

tyreSize a járműre szerelt gumiabroncsok méreteinek jelölése.

authorisedSpeed a jármű maximális engedélyezett sebessége.

oldOdometerValue, newOdometerValue a kilométer-számláló régi és új értékei.

oldTimeValue, newTimeValue a dátum és az idő régi és új értékei.

nextCalibrationDate a jóváhagyott felülvizsgálati szerv által legközelebb végrehajtandó, a CalibrationPurpose-ban meghatározott típusú kalibrálás dátuma.

vuPartNumber, **vuSerialNumber** és **sensorSerialNumber** a készülék azonosítására szolgáló adatelemek.

2. generáció:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Az 1. generáció adatelemein túlmenően a következő adatelemeket kell alkalmazni:

sensorGNSSSerialNumber, amely a külső GNSS-eszközt azonosítja

rcmSerialNumber a távoli kommunikációs modult azonosítja.

sealDataCard a jármű különböző alkatrészeire erősített plombákról szolgáltat információkat.

▼B

2.237. **WorkshopCardHolderIdentification**

Olyan, műhelykártyán tárolt információ, amely a kártyatulajdonos azonosítására vonatkozik (1C melléklet, 311. és 334. követelmény).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName a kártyatulajdonos műhelyének neve.

workshopAddress a kártyatulajdonos műhelyének címe.

cardHolderName a tulajdonos családi neve és utóneve(i) (például a szerelő neve).

cardHolderPreferredLanguage a kártyatulajdonos által előnyben részesített nyelv.

2.238. **WorkshopCardPIN**

A műhelykártya személyazonosító kódja (PIN kód) (1C melléklet, 309. és 332. követelmény).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Érték-hozzárendelés: A kártyatulajdonos számára ismert PIN kód, jobbra maximálisan feltöltve 8 „FF” bájttal.

2.239. **W-VehicleCharacteristicConstant**

A jármű jellemző együtthatója [k) definíció].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Érték-hozzárendelés: Kilométerenkénti impulzusok a 0-tól 64 255 impulzus/km-ig terjedő működési tartományban.

2.240. **VuPowerSupplyInterruptionRecord**

2. generáció:

Olyan, járműegységben tárolt információ, amely áramellátás megszakadása eseményekre vonatkozik (1C melléklet, 117. követelmény).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType az esemény típusa.

eventRecordPurpose az esemény rögzítésének célja.

eventBeginTime az esemény kezdetének dátuma és ideje.

▼B

eventEndTime az esemény befejeződésének dátuma és ideje.

cardNumberAndGenDriverSlotBegin az esemény kezdetekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenDriverSlotEnd az esemény befejeződésekor a járművezetői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotBegin az esemény kezdetekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

cardNumberAndGenCodriverSlotEnd az esemény befejeződésekor a járműkísérői kártyaolvasó egységbe behelyezett kártyát és annak generációját azonosítja.

similarEventsNumber az adott napon előforduló hasonló események száma.

2.241. **VuPowerSupplyInterruptionRecordArray**

2. generáció:

Olyan, járműegységben tárolt információ, amely áramellátás megszakadása eseményekre vonatkozik (1C melléklet, 117. követelmény).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VuPowerSupplyInterruptionRecord
}
```

recordType a rekord (VuPowerSupplyInterruptionRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a VuPowerSupplyInterruptionRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records az áramellátás megszakadására vonatkozó eseményrekordok sorozata.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

2. generáció:

Egy SensorExternalGNSSCoupledRecord rekordsorozat plusz a letöltési protokollban használt metaadatok.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         SensorExternalGNSSCoupledRecord
}
```

recordType a rekord (SensorExternalGNSSCoupledRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

▼B

recordSize a SensorExternalGNSSCoupledRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records a SensorExternalGNSSCoupledRecord rekordok sorozata.

2.243. **VuSensorPairedRecordArray**

2. generáció:

Egy SensorPairedRecord rekordsorozat plusz a letöltési protokollban használt metaadatok.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType a rekord (SensorPairedRecord) típusát jelöli. **Érték-hozzárendelés:** Lásd: RecordType

recordSize a SensorPairedRecord mérete bájtokban kifejezve.

noOfRecords a sorozatban található rekordok száma.

records az érzékelők párosítására vonatkozó rekordok sorozata.

3. ÉRTÉK- ÉS MÉRETTARTOMÁNY-MEGHATÁROZÁSOK

A 2. bekezdésben a definíciókhoz felhasznált változó értékek meghatározása.

```
TimeRealRange ::= 2^32-1
```

4. KARAKTERKÉSZLETEK

Az IA5String karakterláncok az ISO/IEC 8824-1 szabványban definiált ASCII karaktereket használják. Az olvashatóság és a könnyebb hivatkozás érdekében az alábbiakban található az érték-hozzárendelés. A tájékoztatásul feltüntetett adatokkal való ellentmondás esetén mindig az ISO/IEC 8824-1 szabvány az irányadó.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Az egyéb karakterláncok (Address, Name, VehicleRegistrationNumber) emellett a következő 8-bites szabványos karakterkészletek 161–255. decimáliskarakterkód-tartományába tartozó karaktereket is alkalmazzák; a karakterkészletet a kódlap száma határozza meg: Szabványos karakterkészlet	Kódlap (decimális)
ISO/IEC 8859-1 Latin-1 nyugat-európai	1
ISO/IEC 8859-2 Latin-2 közép-európai	2
ISO/IEC 8859-3 Latin-3 dél-európai	3
ISO/IEC 8859-5 Latin / cirill	5
ISO/IEC 8859-7 Latin / görög	7
ISO/IEC 8859-9 Latin-5 török	9

▼B

Az egyéb karakterláncok (Address, Name, VehicleRegistrationNumber) emellett a következő 8-bites szabványos karakterkészletek 161–255. decimáliskarakterkód-tartományába tartozó karaktereket is alkalmazzák; a karakterkészletet a kódlap száma határozza meg: Szabványos karakterkészlet	Kódlap (decimális)
ISO/IEC 8859-13 Latin-7 balti	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 délkelet-európai	16
KOI8-R Latin/cirill	80
KOI8-U Latin/cirill	85

5. KÓDOLÁS

Amennyiben az ASN.1 kódolási szabályok szerint történik a kódolás, az összes definiált adattípust az ISO/IEC 8825-2 szabványnak megfelelően kell kódolni, különbözőképpen elrendezve.

6. OBJEKTUMAZONOSÍTÓK ÉS ALKALMAZÁSAZONOSÍTÓK

6.1. **Objektumazonosítók**

Az e fejezetben felsorolt objektumazonosítók csak a 2. generációra vonatkoznak. Ezeknek az objektumazonosítóknak a meghatározása a TR-03110-3 számú technikai jelentésben található, itt a teljesség kedvéért kerülnek felsorolásra. Ezeket az objektumazonosítókat a bsi-de részfa tartalmazza:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Járműegység-hitelesítési protokollazonosítók

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Példa: Abból a feltevésből kiindulva, hogy a járműegység hitelesítését a SHA-384 algoritmussal kell végezni, az alkalmazandó objektumazonosító (ASN.1 jelöléssel): `bsi-de protocols(2) smartcard(2) 2 2 4`. Ennek az objektumazonosítónak az értéke pontozott jelölést alkalmazva: `0.4.0.127.0.7.2.2.2.2.4`.

	Pontozott jelölés	Bájtjelölés
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

▼B

Chiphitelesítési protokollazonosítók

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Példa: Abból a feltevésből kiindulva, hogy a chiphitelesítést az ECDH algoritmussal kell végezni, az AES munkamenetkulcs 128 bit hosszú. A későbbiekben ezt a munkamenetkulcsot kell alkalmazni a CBC üzemeltetési módban az adatok bizalmas kezelésének, illetve a CMAC algoritmussal az adatok hitelességének biztosítására. Ezért az alkalmazandó objektumazonosító (ASN.1 jelöléssel) `bsi-de protocols(2) smartcard(2) 3 2 2`. Ennek az objektumazonosítónak az értéke pontozott jelölést alkalmazva: `0.4.0.127.0.7.2.2.3.2.2`.

	Pontozott jelölés	Bájtjelölés
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. **Alkalmazásazonosítók**

2. generáció:

A (2. generációs) külső GNSS-eszköz alkalmazásazonosítóját (AID) az ‘FF 44 54 45 47 4D’ adja meg. Ez egy tulajdonosi AID az ISO/IEC 7816-4 szabványnak megfelelően

Megjegyzés: Az utolsó 5 bájt tartalmazza a DTEGM-et az intelligens menetíró készülék külső GNSS-eszközéhez.

A 2. generációs tachográfkártya alkalmazásazonosítóját az ‘FF 53 4D 52 44 54’ adja meg. Ez egy tulajdonosi AID az ISO/IEC 7816-4 szabványnak megfelelően

▼B

2. függelék

A TACHOGRÁFKÁRTYÁKRA VONATKOZÓ ELŐÍRÁSOK

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. Rövidítések

1.2. Hivatkozások

2. ELEKTROMOS ÉS FIZIKAI JELLEMZŐK

2.1. Tápfeszültség és áramfelvétel

2.2. A V_{pp} programozási feszültség

2.3. Órajel-generálás és -frekvencia

2.4. I/O érintkező

2.5. A kártya állapotai

3. HARDVER ÉS KOMMUNIKÁCIÓ

3.1. Bevezetés

3.2. Adatátviteli protokoll

3.2.1 Protokollok

3.2.2 ATR

3.2.3 PTS

3.3. Hozzáférési szabályok

3.4. Parancsok és hibakódok áttekintése

3.5. A parancsok leírása

3.5.1 SELECT

3.5.2 READ BINARY

3.5.3 UPDATE BINARY

3.5.4 GET CHALLENGE

3.5.5 VERIFY

3.5.6 GET RESPONSE

3.5.7 PSO: VERIFY CERTIFICATE

3.5.8 INTERNAL AUTHENTICATE

3.5.9 EXTERNAL AUTHENTICATE

3.5.10 GENERAL AUTHENTICATE

3.5.11 MANAGE SECURITY ENVIRONMENT

3.5.12 PSO: HASH

▼B

3.5.13 PERFORM HASH of FILE

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

3.5.15 PSO: VERIFY DIGITAL SIGNATURE

3.5.16 PROCESS DSRC MESSAGE

4. A TACHOGRÁFKÁRTYÁK STRUKTÚRÁJA

4.1. Törzsállomány (MF)

4.2. Járművezetőikártya-alkalmazások

4.2.1 1. generációs járművezetőikártya-alkalmazás

4.2.2 2. generációs járművezetőikártya-alkalmazás

4.3. Műhelykártya-alkalmazások

4.3.1 1. generációs műhelykártya-alkalmazás

4.3.2 2. generációs műhelykártya-alkalmazás

4.4. Ellenőrzőkártya-alkalmazások

4.4.1 1. generációs ellenőrzőkártya-alkalmazás

4.4.2 2. generációs ellenőrzőkártya-alkalmazás

4.5. Vállalkozáskártya-alkalmazások

4.5.1 1. generációs vállalkozáskártya-alkalmazás

4.5.2 2. generációs vállalkozáskártya-alkalmazás

1. BEVEZETÉS

1.1. **Rövidítések**

E függelék alkalmazásában a következő rövidítések alkalmazandók:

AC	Access conditions – hozzáférési feltételek
AES	Advanced Encryption Standard – továbbfejlesztett adattitkosítási szabvány
AID	Application Identifier – alkalmazásazonosító
ALW	Always – mindig
APDU	Application Protocol Data Unit – alkalmazási protokoll adategysége (a parancs szerkezete)
ATR	Answer To Reset – válasz az alaphelyzetbe állításra
AUT	Authenticated – hitelesített
C6, C7	Contacts N° 6 and 7 – a kártya 6-os és 7-es számú érintkezői az ISO/IEC 7816-2 leírása szerint
cc	clock cycles – órajelciklusok
CHV	Card holder Verification Information – a kártyatulajdonos ellenőrzésére szolgáló információ
CLA	Class byte of an APDU command – egy APDU parancs besorolási bájtja

▼B

DSRC	Dedicated Short Range Communication – speciális célú, rövid hatótávolságú adatátvitel
DF	Dedicated File – speciális célú fájl. Egy DF tartalmazhat egyéb (EF vagy DF) fájlokat is
ECC	Elliptic Curve Cryptography – elliptikus görbe alapú titkosítás
EF	Elementary File – elemi fájl
etu	elemi időegység – elemi időegység
G1	Generation 1 – 1. generáció
G2	Generation 2 – 2. generáció
IC	Integrated Circuit – integrált áramkör
ICC	Integrated Circuit Card – integrált áramkörös kártya
ID	Identifier – azonosító
IFD	Interface Device – interfészkészülék
IFS	Information Field Size – információs mező mérete
IFSC	Information Field Size for the card – a kártya információs mezőjének mérete
IFSD	Information Field Size Device – a terminál információs mezőjének mérete
INS	Instruction byte of an APDU command – egy APDU parancs utasítási bájtja
Lc	Length of the input data for a APDU command – a bemeneti adat hossza egy APDU parancs esetében
Le	Length of the expected data – a várt adat hossza (kimeneti adat egy parancs esetében)
MF	Master File – törzsállomány (gyökér DF)
NAD	Node Address used in T=1 protocol – a T=1 protokollban felhasznált csomópontcím
NEV	Never – egyszer sem
P1-P2	Parameter bytes – paraméterbájtok
PIN	Personal Identification Number – személyazonosító kód
PRO SM	Protected with secure messaging – biztonságos üzenetküldéssel védve
PTS	Protocol Transmission Selection – protokollátvitel kiválasztása
RFU	Reserved for Future Use – későbbi használatra fenntartva
RST	Reset – alaphelyzetbe állítás (a kártyára vonatkozik)
SFID	Short EF Identifier – rövid EF azonosító
SM	Secure Messaging – biztonságos üzenetküldés
SW1-SW2	Status bytes – állapotbájtok
TS	Initial ATR character – kezdeti ATR karakter
VPP	Programming Voltage – programozási feszültség
VU	Vehicle Unit – járműegység
XXh	Value XX in hexadecimal notation – XX érték hexadecimális jelöléssel
‘XXh’	Value XX in hexadecimal notation – XX érték hexadecimális jelöléssel
||	az összefűzés szimbóluma, 03||04=0304

▼B

1.2. **Hivatkozások**

E függelékben a következő hivatkozások jelennek meg:

ISO/IEC 7816-2 Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards – Integrated circuit cards – Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011.

2. ELEKTROMOS ÉS FIZIKAI JELLEMZŐK

TCS_01 Eltérő utasítás hiányában minden elektronikus jelnek összhangban kell lennie az ISO/IEC 7816-3 szabvánnyal.

TCS_02 A kártya érintkezőinek elhelyezése és méretei megfelelnek az ISO/IEC 7816-2 szabványnak.

2.1. **Tápfeszültség és áramfelvétel**

TCS_03 A kártya az ISO/IEC 7816-3 szabványban meghatározott áramfelvételi határértékeken belül üzemel, az előírásoknak megfelelően.

TCS_04 A kártyának a Vcc = 3V (± 0,3V) vagy Vcc = 5V (± 0,5V) feszültségen kell működnie.

A feszültséget az ISO/IEC 7816-3 szabványnak megfelelően kell kiválasztani.

2.2. **A V_{pp} programozási feszültség**

TCS_05 A kártya nem igényel programozási feszültséget a C6-os érintkezőnél. A C6-os érintkező várhatóan nem csatlakozik egy IFD-be. A C6-os érintkező a V_{cc}-re kapcsolható a kártyán, de nem kell földelni. E feszültség semmilyen esetben sem értelmezhető.

2.3. **Órajel-generálás és -frekvencia**

TCS_06 A kártya az 1–5 MHz frekvenciatartományban üzemel és magasabb frekvenciákat is támogathat. Egy kártyakapcsolaton belül az órajel frekvenciája ± 2 %-ot változhat. Az órajel-frekvenciát a járműegység generálja, nem maga a kártya. A működési periódus 40 és 60 % között változhat.

TCS_07 Az EF ICC kártyafájlban rögzített körülmények között a külső óra megállítható. Az EF ICC fájl főrészének első bájtja a Clockstop (óraleállítás) üzemmód feltételeit kódolja:

▼B

Alacsony	Magas		
3-es bit	2-es bit	1-es bit	
0	0	1	Clockstop engedélyezett, nincs előnyben részesített szint
0	1	1	Clockstop engedélyezett, a magas az előnyben részesített szint
1	0	1	Clockstop engedélyezett, az alacsony az előnyben részesített szint
0	0	0	Clockstop nem engedélyezett
0	1	0	Clockstop csak a magas szinten engedélyezett
1	0	0	Clockstop csak az alacsony szinten engedélyezett

A 4–8-as bit nem kerül felhasználásra.

2.4. **I/O érintkező**

TCS_08 A C7-es I/O érintkezőt arra kell használni, hogy adatokat fogadjon az IFD-től, valamint adatokat továbbítson az IFD felé. A művelet végzése alatt vagy csak a kártya, vagy csak az IFD lehet adatátviteli üzemmódban. Amennyiben mindkét egység átviteli üzemmódban van, a kártya ezáltal nem sérülhet meg. Amennyiben a kártya nem bonyolít le átvitelt, fogadás üzemmódba lép.

2.5. **A kártya állapotai**

TCS_09 A kártya két állapotban üzemel, miközben rendelkezésre áll a megkívánt tápfeszültség:

üzemelési állapotban, amikor parancsokat hajt végre, vagy összeköttetésben van a digitális egységgel,

minden egyéb időben tétlen állapotban; ezen állapotban a kártya minden adatot visszatart.

3. HARDVER ÉS KOMMUNIKÁCIÓ

3.1. **Bevezetés**

Ez a szakasz a tachográfkártya és a járműegységek (VU) minimális funkcionális követelményeit ismerteti, amelyek biztosítják a megfelelő üzemelést és az interoperabilitást.

A tachográfkártyák, amennyire lehetséges, megfelelnek a hatályos ISO/IEC szabványoknak (különösen az ISO/IEC 7816 szabványnak). Azonban a parancsokat és a protokollokat részletesen ismertetni kell, hogy adott esetben bizonyos, használatra vonatkozó korlátozások vagy különbségek meghatározásra kerüljenek. Eltérő utasítás hiányában e parancsoknak teljes mértékben meg kell felelniük az említett szabványoknak.

3.2. **Adatátviteli protokoll**

TCS_10 Az adatátviteli protokoll megfelel az ISO/IEC 7816-3 szabványnak T = 0 és T = 1 esetén. A járműegység felismeri különösen a kártya által küldött várakozásiidő-kiterjesztéseket.

3.2.1 *Protokollok*

TCS_11 A kártya mind a **T=0**, mind a **T=1** protokollt támogatja. Ezenkívül a kártya támogathat további érintkezőorientált protokollokat.

TCS_12 A **T=0** az alapértelmezésű protokoll, ezért a protokoll **T=1**-re történő átváltásához szükség van a **PTS** parancsra.

▼B

TCS_13 Az eszközök mindkét protokoll szerint támogatják a **direct convention**-t, amely ily módon kötelező a kártya tekintetében.

TCS_14 A **kártya információsmező-méret** bájtjának jelen kell lennie az ATR-nél a TA3-as karakterben. Ezen érték legalább ‘F0h’ (= 240 bájt).

A protokollokra a következő korlátozások vonatkoznak:

TCS_15 **T=0**

— Az interfészkészülék támogat egy választ az I/O szinten, az RST-n, 400 cc-től a jel felfutó éle után.

— Az interfészkészülék képes elolvasni a 12 etu-val elválasztott karaktereket.

— Az interfészkészülék leolvassa a hibás karaktert és annak ismételt előfordulását, ha azt 13 etu választja el. Amennyiben hibás karaktert észlel, az I/O-n egy hibajel jelenik meg 1 etu és 2 etu között. Az eszköz 1 etu késleltetést támogat.

— Az interfészkészülék elfogad egy 33 bájtos ATR (TS+32)-t.

— Ha a TC1 jelen van az ATR-ben, az Extra Guard Timenak (külön biztonsági időnek) rendelkezésre kell állnia az interfészkészülék által elküldött karakterekre vonatkozóan, bár a kártya által elküldött karakterek még 12 etu-val elválaszthatók. Ez szintén igaz az interfészkészülék által kiadott P3-as karakter után a kártya által elküldött ACK karakterre is.

— Az interfészkészülék figyelembe veszi a kártya által kiadott NUL karaktert is.

— Az interfészkészülék elfogadja a komplementer üzemmódot az ACK-ra.

— A Get Response parancs nem használható a láncolási üzemmódban olyan adat fogadására, amelynek hossza meghaladhatja a 255 bájtot.

TCS_16 **T=1**

— NAD bájt: nincs használatban (a NAD-ot ‘00’-ra kell beállítani).

— S-block ABORT: nincs használatban.

— S-blokk VPP állapot-hiba: nincs használatban.

— Az adatmező teljes láncolási hossza nem haladja meg a 255 bájtot (ezt az IFD biztosítja).

— Az IFSD-t az IFD közvetlenül az ATR után jelzi: az IFD továbbítja az S-Block IFS kérését az ATR után, és a kártya az S-Block IFS-t küldi vissza. Az IFSD-re javasolt érték: 254 bájt.

— A kártya nem kér IFS kiigazítást.

▼B

3.2.2 *ATR*

TCS_17 Az eszköz ellenőrzi az ATR bájtokat, az ISO/IEC 7816-3 szabványnak megfelelően. Nem kell végezni ellenőrzést az ATR előzménykaraktereken.

Példa az ISO/IEC 7816-3 szabványnak megfelelő Basic Biprotocol ATR-re

Karakter	Érték	Megjegyzések
TS	‘3Bh’	Jelzi a direct convention-t.
T0	‘85h’	TD1 jelen van; 5 előzménybájt jelen van
TD1	‘80h’	TD2 jelen van; T=0 használandó
TD2	‘11h’	TA3 jelen van; T=1 használandó
TA3	‘XXh’ (legalább ‘F0h’)	Kártya információsmező-méret (IFSC)
TH1 – TH5	‘XXh’	Előzménykarakterek
TCK	‘XXh’	Ellenőrző karakter (OR nélkül)

TCS_18 Az Answer To Reset (ATR) után a törzsállomány (MF) implicit módon kiválasztásra kerül, és ez lesz az aktuális könyvtár.

3.2.3 *PTS*

TCS_19 Az alapértelmezett protokoll a T=0. A T=1 protokoll beállításához a PTS-t (PPS-ként is ismert) el kell küldeni a kártyához az eszköz segítségével.

TCS_20 Mivel mind a T=0, mind a T=1 protokoll kötelező a kártyára vonatkozóan, ezért a protokollok átkapcsolását engedélyező alap-PTS ugyancsak kötelező.

Az ISO/IEC 7816-3 szabvány szerint a PTS felhasználható egy nagyobb átviteli sebességre való átkapcsolásra, mint adott esetben az ATR-ben a kártya által javasolt alapértelmezett sebesség (TA(1) bájt).

A nagyobb átviteli sebességek opcionálisak a kártya részére.

TCS_21 Ha az alapértelmezett sebességen kívül más átviteli sebesség nem támogatott (vagy ha a kiválasztott átviteli sebesség nem támogatott), a kártya helyesen válaszol a PTS-re, az ISO/IEC 7816-3 szabványnak megfelelően, kihagyva a PPS1 bájtot.

Alap PTS példák protokoll-kiválasztáshoz:

Karakter	Érték	Megjegyzések
PPSS	‘FFh’	A kezdő karakter
PPS0	‘00h’ vagy ‘01h’	PPS1 – PPS3 nincs jelen; ‘00h’ a T0 kiválasztásához, ‘01h’ a T1 kiválasztásához
PK	‘XXh’	Ellenőrző karakter: ‘XXh’ = ‘FFh’, ha PPS0 = ‘00h’, ‘XXh’ = ‘FEh’, ha PPS0 = ‘01h’.

▼B

3.3. **Hozzáférési szabályok**

TCS_22 Egy hozzáférési szabály a hozzáférési mód – azaz parancs – tekintetében meghatározza a megfelelő biztonsági feltételeket. A biztonsági feltételek teljesülése esetén a megfelelő parancs feldolgozásra kerül.

TCS_23 A tachográfkártya esetében a következő biztonsági feltételek alkalmazandók:

Rövidítés	Jelentés
ALW	A művelet mindig lehetséges, és minden korlátozás nélkül végrehajtható. APDU parancs és válasz egyszerű szövegben, vagyis biztonságos üzenetküldés nélkül került megküldésre.
NEV	A művelet soha sem lehetséges.
PLAIN-C	APDU parancs egyszerű szövegben, vagyis biztonságos üzenetküldés nélkül került megküldésre.
PWD	A művelet csak a műhelykártya PIN kódjának sikeres ellenőrzését követően kerülhet végrehajtásra, azaz ha a kártya belső biztonsági állapota: „PIN_Verified”. A parancsot biztonságos üzenetküldés nélkül kell elküldeni.
EXT-AUT-G1	A művelet csak akkor kerülhet végrehajtásra, ha az 1. generációs hitelesítésre vonatkozó External Authenticate parancs (lásd még: 11. függelék A. rész) sikeresen végre lett hajtva.
SM-MAC-G1	Az APDU (parancs és válasz) 1. generációs biztonságos üzenetküldéssel együtt alkalmazandó csak hitelesítésre szolgáló üzemmódban (lásd: 11. függelék A. rész).
SM-C-MAC-G1	Az APDU parancs 1. generációs biztonságos üzenetküldéssel együtt alkalmazandó csak hitelesítésre szolgáló üzemmódban (lásd: 11. függelék A. rész).
SM-R-ENC-G1	Az APDU válasz 1. generációs biztonságos üzenetküldéssel együtt alkalmazandó titkosítás üzemmódban (lásd: 11. függelék A. rész), vagyis nem érkezik vissza üzenethitelesítési kód.
SM-R-ENC-MAC-G1	Az APDU válasz 1. generációs biztonságos üzenetküldéssel együtt alkalmazandó „titkosítás, majd hitelesítés” üzemmódban (lásd: 11. függelék A. rész).
SM-MAC-G2	Az APDU (parancs és válasz) 2. generációs biztonságos üzenetküldéssel együtt alkalmazandó csak hitelesítésre szolgáló üzemmódban (lásd: 11. függelék B. rész).
SM-C-MAC-G2	Az APDU parancs 2. generációs biztonságos üzenetküldéssel együtt alkalmazandó csak hitelesítésre szolgáló üzemmódban (lásd: 11. függelék B. rész).
SM-R-ENC-MAC-G2	Az APDU válasz 2. generációs biztonságos üzenetküldéssel együtt alkalmazandó „titkosítás, majd hitelesítés” üzemmódban (lásd: 11. függelék B. rész).

TCS_24 Ezek a biztonsági feltételek összekapcsolhatók az alábbiak szerint:

ÉS: valamennyi biztonsági feltételnek teljesülnie kell.

VAGY: legalább egy biztonsági feltételnek teljesülnie kell.

A fájlrendszerre vonatkozó hozzáférési szabályokat (tehát a SELECT, READ BINARY és UPDATE BINARY parancsokat) a 4. fejezet határozza meg. A többi paranccsal kapcsolatos hozzáférési szabályokat a következő táblázatok határozzák meg.

▼B

TCS_25 A DF Tachograph G1 alkalmazásban a következő hozzáférési szabályok alkalmazandók:

Parancs	Járművezetői kártya	Műhelykártya	Ellenőrzőkártya	Vállalkozáskártya
External Authenticate				
— Az 1. generáció hitelesítéséhez	ALW	ALW	ALW	ALW
— A 2. generáció hitelesítéséhez	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nem alkalmazható	Nem alkalmazható
PSO: Hash	Nem alkalmazható	Nem alkalmazható	ALW	Nem alkalmazható
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nem alkalmazható	Nem alkalmazható
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nem alkalmazható	Nem alkalmazható	ALW	Nem alkalmazható
Verify	Nem alkalmazható	ALW	Nem alkalmazható	Nem alkalmazható

TCS_26 A DF Tachograph_G2 alkalmazásban a következő hozzáférési szabályok alkalmazandók:

Parancs	Járművezetői kártya	Műhelykártya	Ellenőrzőkártya	Vállalkozáskártya
External Authenticate				
— Az 1. generáció hitelesítéséhez	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
— A 2. generáció hitelesítéséhez	ALW	PWD	ALW	ALW
Internal Authenticate	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható

▼B

Parancs	Járművezetői kártya	Műhelykártya	Ellenőrzőkártya	Vállalkozáskártya
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nem alkalmazható	ALW	ALW	Nem alkalmazható
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nem alkalmazható	Nem alkalmazható
PSO: Hash	Nem alkalmazható	Nem alkalmazható	ALW	Nem alkalmazható
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Nem alkalmazható	Nem alkalmazható
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Nem alkalmazható	Nem alkalmazható	ALW	Nem alkalmazható
Verify	Nem alkalmazható	ALW	Nem alkalmazható	Nem alkalmazható

TCS_27 Az MF-ben a következő hozzáférési szabályok alkalmazandók:

Parancs	Járművezetői kártya	Műhelykártya	Ellenőrzőkártya	Vállalkozáskártya
External Authenticate				
— Az 1. generáció hitelesítéséhez	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
— A 2. generáció hitelesítéséhez	ALW	PWD	ALW	ALW
Internal Authenticate	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható

▼B

Parancs	Járművezetői kártya	Műhelykártya	Ellenőrzőkártya	Vállalkozáskártya
PSO: Compute Digital Signature	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
PSO: Hash	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
PSO: Hash of File	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható	Nem alkalmazható
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Nem alkalmazható	ALW	Nem alkalmazható	Nem alkalmazható

TCS_28 A tachográfkártya elfogadhatja vagy elutasíthatja a biztonsági feltételek által meghatározott parancsnál magasabb biztonsági szintű parancsot. Vagyis ha a biztonsági feltétel ALW (vagy PLAIN-C), a kártya elfogadhat egy biztonságos üzenetküldéssel ellátott parancsot (titkosítási és/vagy hitelesítési üzemmód). Amennyiben a biztonsági feltétel biztonságos üzenetküldést és hitelesítési üzemmódot ír elő, a tachográfkártya elfogadhatja az azonos generációhoz tartozó biztonságos üzenetküldéssel ellátott parancsot titkosítási és hitelesítési üzemmódban.

Megjegyzés: A leírások további részletekkel szolgálnak a parancsok támogatásáról a különböző tachográfkártya-típusok és a különböző DF-ek esetében.

3.4. **Parancsok és hibakódok áttekintése**

A parancsok és a fájlok szervezése az ISO/IEC 7816-4 szabványból következik és megfelel e szabvány rendelkezéseinek.

E szakasz a következő APDU parancs-válasz párokat ismerteti. Az 1. és 2. generációs alkalmazások által támogatott parancsvariánsokat a megfelelő parancsleírások határozzák meg.

Parancs	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Parancs	INS
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 A válaszüzeneteket az SW1 és SW2 állapotszavak kísérik és jelzik a parancs feldolgozási állapotát.

SW1	SW2	Jelentés
90	00	Normál feldolgozás.
61	XX	Normál feldolgozás. XX = a rendelkezésre álló válaszbájtok száma
62	81	Figyelmeztető feldolgozás. A visszaküldött adatok egy része sérült lehet
63	00	Sikertelen hitelesítés (figyelmeztetés)
63	CX	Rossz CHV (PIN). A további kísérletek számlálóját az ‘X’ szolgáltatja.
64	00	Végrehajtási hiba – A nem felejtő memória állapota változatlan. Integritási hiba
65	00	Végrehajtási hiba – A nem felejtő memória állapota megváltozott.
65	81	Végrehajtási hiba – A nem felejtő memória állapota megváltozott – Memóriahiba
66	88	Védelmi hiba: rossz titkosítási ellenőrző összeg (a biztonságos üzenetküldés során) vagy rossz tanúsítvány (a tanúsítvány ellenőrzése során) vagy rossz kriptogram (a külső hitelesítés során) vagy rossz aláírás (az aláírás ellenőrzése során)
67	00	Téves hossz (rossz Lc vagy Le)

▼B

SW1	SW2	Jelentés
68	82	A biztonságos üzenetküldés nem támogatott
68	83	A lánc utolsó parancsa várható
69	00	Tiltott parancs (nem áll rendelkezésre válasz a T=0-ban)
69	82	A biztonsági állapot nem valósul meg
69	83	A hitelesítési módszer blokkolva
69	85	A használati feltételek nem teljesülnek
69	86	A parancs nem engedélyezett (nincs aktuális EF)
69	87	A várt biztonságos üzenetküldés adatobjektumai hiányoznak
69	88	Helytelen biztonságos üzenetküldési adatobjektumok
6A	80	Helytelen paraméterek az adatmezőben
6A	82	A fájl nem található
6A	86	Rossz P1-P2 paraméterek
6A	88	A hivatkozott adat nem található
6 B	00	Rossz paraméterek (eltolás az EF-en kívül)
6C	XX	Téves hossz, az SW2 jelzi a pontos hosszt. Nem érkezett vissza adatmező
6D	00	Az utasításkód nem támogatott vagy érvénytelen
6E	00	A besorolás nem támogatott
6F	00	Egyéb ellenőrzési hibák

TCS_30 Ha egyetlen APDU parancsban egynél több hibafeltétel teljesül, a kártya a megfelelő állapotszavak bármelyikét visszaküldheti.

3.5. **A parancsok leírása**

E fejezetben a tachográfkártyákra vonatkozó kötelező érvényű parancsok leírása szerepel.

További releváns, titkosítási műveletekkel kapcsolatos részletek a 11. függelékben találhatók (Közös biztonsági mechanizmusok az 1.és 2. generációs menetíró készülék tekintetében).

Minden parancsot le kell írni, függetlenül a felhasznált protokolltól (T=0 vagy T=1). A CLA, INS, P1, P2, Lc és Le APDU bájtok mindig megadásra kerülnek. Amennyiben az Lc vagy Le nem szükséges a leírt parancshoz, a hozzárendelt hossz, az érték és a leírás üresen marad.

TCS_31 Amennyiben mindkét hosszbájt (Lc és Le) szükséges, a leírt parancsot két részre kell osztani, ha az IFD a T=0 protokollt használja fel: az IFD elküldi a P3=Lc + adatokkal leírt parancsot, és azután elküld egy GET RESPONSE (lásd: 3.5.6. pont) parancsot a P3=Le-vel.

TCS_32 Ha mindkét hosszbájt szükséges, és Le=0 (biztonságos üzenetküldés), akkor:

▼B

— a T=1 protokoll használatakor a kártya az összes rendelkezésre álló kimeneti adat elküldésével válaszol az Le=0-ra;

— a T=0 protokoll használatakor az IFD elküldi az első parancsot a P3=Lc + adattal, a kártya pedig válaszol (erre az implicit Le=0-ra) a '**61La**' állapotbájttal, ahol La a rendelkezésre álló válaszbájtok száma. Ekkor az IFD előállít egy GET RESPONSE parancsot a P3=La-val az adatok olvasására.

TCS_33 A tachográfkártya opcionális lehetőségként támogathat kiterjesztett hosszúságú adatmezőket az ISO/IEC 7816-4 szabványnak megfelelően. A kiterjesztett hosszúságú adatmezőket támogató tachográfkártya:

— jelzi a kiterjesztett hosszúságú adatmezők támogatását az ATR-ben;

— kiterjesztett hosszúságú információk révén megadja a támogatott pufferméretet az ATR/INFO EF-ben, lásd: TCS_146 szakasz;

— jelzi, hogy támogatja-e a kiterjesztett hosszúságú adatmezőket az Extended Length EF-ben T = 1 és/vagy T = 0 esetében, lásd: TCS_147 szakasz;

— támogatja a kiterjesztett hosszúságú adatmezőket az 1. és 2. generációs tachográf-alkalmazás esetében.

Megjegyzések:

Minden parancs rövid hosszúságú mezőkre lett meghatározva. A kiterjesztett hosszúságú APDU-k használatát az ISO/IEC 7816-4 szabvány egyértelműsíti.

Általánosságban a parancsok egyszerű, vagyis biztonságos üzenetküldés nélküli üzemmódra lettek meghatározva; a biztonságos üzenetküldési réteget a 11. függelék határozza meg. Egy parancs hozzáférési szabályaiból egyértelműen kiderül, hogy a parancs támogatja-e a biztonságos üzenetküldést vagy sem, és ha igen, akkor az 1. vagy 2. generációs biztonságos üzenetküldést támogatja-e, vagy mindkettőt. A biztonságos üzenetküldés használatának szemléltetése érdekében egyes parancsvariánsok biztonságos üzenetküldéssel együtt kerülnek bemutatásra.

TCS_34 A VU végrehajtja a 2. generációs VU és a kártya teljes kölcsönös hitelesítési protokollját az adott művelet tekintetében, ideértve (ha szükséges) a tanúsítvány ellenőrzését is a következőkben: DF Tachograph, DF Tachograph_G2 vagy MF.

3.5.1 *SELECT*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

A SELECT parancs az alábbiakra szolgál:

— egy alkalmazás DF kiválasztása (a név szerinti kiválasztás kötelező),

— a javasolt fájl ID-nek megfelelő elemi fájl kiválasztása.

3.5.1.1 Név szerinti kiválasztás (AID)

Ez a parancs lehetővé teszi a kártyán regisztrált alkalmazás DF kiválasztását.

TCS_35 Ez a parancs a fájlszerkezetben bárhonnan végrehajtható (az ATR után vagy bármikor).

▼B

TCS_36 Egy alkalmazás kiválasztása visszaállítja az aktuális biztonsági környezetet. Az alkalmazás kiválasztásának végrehajtása után már semmilyen aktuális nyilvános kulcs nem választható ki. Az EXT-AUT-G1 hozzáférési feltétel szintén elveszik. Ha a parancs biztonságos üzenetküldés nélkül került végrehajtásra, a korábbi munkamenetkulcs többé nem áll rendelkezésre biztonságos üzenetküldéshez.

TCS_37 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Név szerinti kiválasztás (AID)
P2	1	‘0Ch’	Nincs várt válasz
Lc	1	‘NNh’	A kártyára küldött bájtok száma (az AID hossza): ‘06h’ a tachográf-alkalmazáshoz
#6 – #(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ az 1. generációs tachográf-alkalmazáshoz AID: ‘FF 53 4D 52 44 54’ a 2. generációs tachográf-alkalmazáshoz

A SELECT parancsra nem szükséges a válasz (a Le hiányzik a T=1-ben, vagy nincs válaszkérés a T=0-ban).

TCS_38 **Válaszüzenet (nincs válaszkérés)**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az AID-nek megfelelő alkalmazás nem található, a visszaküldött feldolgozási állapot: ‘**6A82**’.

— Ha a T=1-ben az Le bájt jelen van, a visszaküldött állapot: ‘**6700**’.

— Ha a T=0-ban a SELECT parancs után válaszra van szükség, a visszaküldött állapot: ‘**6900**’.

— Ha a kiválasztott alkalmazás sérültnek minősül (a fájlattribútumon belül integritási hiba észlelhető), a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

3.5.1.2 Egy elemi fájl (EF) kiválasztása a fájlazonosítójának felhasználásával

TCS_39 **Parancsüzenet**

TCS_40 E parancsvariáns esetében a tachográfkártya támogatja a 2. generációs biztonságos üzenetküldést a 11. függelék B. részében meghatározottak szerint.

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Egy EF kiválasztása az aktuális DF alatt

▼B

Bájt	Hossz	Érték	Leírás
P2	1	‘0Ch’	Nincs várt válasz
Lc	1	‘02h’	A kártyára küldött bájtok száma
#6–#7	2	‘XXXXh’	Fájlazonosító

A SELECT parancsra nem szükséges a válasz (a Le hiányzik a T=1-ben, vagy nincs válaszkérés a T=0-ban).

TCS_41 **Válaszüzenet (nincs válaszkérés)**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha a fájlazonosítónak megfelelő alkalmazás nem található, a visszaküldött feldolgozási állapot: ‘**6A82**’.

— Ha a T=1-ben az Le bájt jelen van, a visszaküldött állapot: ‘**6700**’.

— Ha a T=0-ban a SELECT parancs után válaszra van szükség, a visszaküldött állapot: ‘**6900**’.

— Ha a kiválasztott fájl sérültnek minősül (a fájl-attribútumon belül integritási hiba észlelhető), a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

3.5.2 *READ BINARY*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

A READ BINARY parancsot transzparens fájlból való adatkiolvasásra kell használni.

A kártya válasza a kiolvasott adatok visszaküldéséből áll, amelyek opcionálisan beillesztésre kerülhetnek egy biztonságos üzenetküldési struktúrába.

3.5.2.1 Parancs eltolással a P1-P2-ben

Ez a parancs lehetővé teszi, hogy az IFD adatokat olvasson ki az aktuálisan kiválasztott EF-ből biztonságos üzenetküldés nélkül.

Megjegyzés: Biztonságos üzenetküldés nélkül ez a parancs csak arra használható, hogy elolvasson egy olyan fájlt, amely támogatja a hozzáférés olvasásra üzemmóddal kapcsolatos ALW biztonsági feltételt.

TCS_42 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legnagyobb helyértékű bájt

▼B

Bájt	Hossz	Érték	Leírás
P2	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legkisebb helyértékű bájt
Le	1	‘XXh’	A várt adathossz. Az olvasandó bájtok száma.

Megjegyzés: a P1 8-as bitjét 0-ra kell állítani.

TCS_43 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #X	X	‘XX..XXh’	Kiolvasott adat
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha nincs kiválasztott EF, a visszaküldött feldolgozási állapot: ‘**6986**’.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a ‘**6982**’ értékkel.

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: ‘**6B00**’.

— Ha a kiolvasandó adat mérete nem egyeztethető össze az EF méretével (eltolás + Le > EF méret), a visszaküldött feldolgozási állapot: ‘**6700**’ vagy ‘**6Cxx**’, ahol ‘xx’ a pontos hosszt jelzi.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: ‘**6400**’ vagy ‘**6581**’.

— Ha az eltárolt adatokon belül integritási hiba érzékelhető, a kártya visszaküldi a kívánt adatokat, és a visszaküldött feldolgozási állapot: ‘**6281**’.

3.5.2.1.1 Parancs biztonságos üzenetküldéssel (példák)

Ez a parancs lehetővé teszi, hogy az IFD adatokat olvasson le az aktuálisan kiválasztott EF-ből biztonságos üzenetküldéssel annak érdekében, hogy a fogadott adatok integritását ellenőrizze, és védje az adatok titkosságát, amennyiben az SM-R-ENC-MAC-G1 (1. generáció) vagy az SM-R-ENC-MAC-G2 (2. generáció) biztonsági feltétel kerül alkalmazásra.

TCS_44 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘0Ch’	Biztonságos üzenetküldés kérése
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (eltolás bájtokban a fájl elejétől kezdve): a legnagyobb helyértékű bájt
P2	1	‘XXh’	P2 (eltolás bájtokban a fájl elejétől kezdve): a legkisebb helyértékű bájt

▼B

Bájt	Hossz	Érték	Leírás
Lc	1	‘XXh’	A biztonságos üzenetküldés bemeneti adatának hossza
#6	1	‘97h’	T_{LE}: Címke a várt hossz meghatározására
#7	1	‘01h’	L_{LE}: Várt hossz
#8	1	‘NNh’	A várt hossz meghatározása (eredeti Le): Az olvasandó bájtok száma
#9	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#10	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza ‘04h’ az 1. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék A. rész) Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#11 – #(10+L)	L	‘XX..XXh’	Titkosítási ellenőrző összeg
Le	1	‘00h’	Az ISO/IEC 7816-4 szabvány meghatározása szerint

TCS_45 **Válaszüzenet, ha az SM-R-ENC-MAC-G1 (1. generáció) vagy az SM-R-ENC-MAC-G2 (2. generáció) nem követelmény, és ha a biztonságos üzenetküldés bemeneti formája helyes:**

Bájt	Hossz	Érték	Leírás
#1	1	‘99h’	Címke a feldolgozási állapothoz (SW1-SW2) – opcionális az 1. generációs biztonságos üzenetküldés esetén
#2	1	‘02h’	Feldolgozási állapot hossza
#3 – #4	2	‘XX XXh’	A nem védett APDU válasz feldolgozási állapota
#5	1	‘81h’	T_{PV}: Címke a normál értékadatokhoz
#6	L	‘NNh’ vagy ‘81 NNh’	L_{PV}: a visszaküldött adat hossza (= eredeti Le) L 2 bájtos, ha L_{PV}>127 bájt
#(6+L) – #(5+L+NN)	NN	‘XX..XXh’	Normál adatok értéke
#(6+L+NN)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(7+L+NN)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza ‘04h’ az 1. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék A. rész) Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(8+L+NN) – #(7+M+L+NN)	M	‘XX..XXh’	Titkosítási ellenőrző összeg
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

▼B

TCS_46 **Válaszüzenet, ha az SM-R-ENC-MAC-G1 (1. generáció) vagy az SM-R-ENC-MAC-G2 (2. generáció) követelmény, és ha a biztonságos üzenetküldés bemeneti formája helyes:**

Bájt	Hossz	Érték	Leírás
#1	1	‘87h’	$T_{PI\ CG}$: Címke a titkosított adatokhoz (kriptogram)
#2	L	‘MMh’ vagy ‘81 MMh’	$L_{PI\ CG}$: a visszaküldött titkosított adatok hossza (a parancs eredeti Le értékétől eltérő, a feltöltésnek köszönhetően) L 2 bájtos, ha $L_{PI\ CG}$>127 bájt
#(2+L) – #(1+L+MM)	MM	‘01XX..XXh’	Titkosított adatok: Feltöltésjelző és kriptogram
#(2+L+MM)	1	‘99h’	Címke a feldolgozási állapothoz (SW1-SW2) – opcionális az 1. generációs biztonságos üzenetküldés esetén
#(3+L+MM)	1	‘02h’	Feldolgozási állapot hossza
#(4+L+MM) – #(5+L+MM)	2	‘XX XXh’	A nem védett APDU válasz feldolgozási állapota
#(6+L+MM)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(7+L+MM)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza ‘04h’ az 1. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék A. rész) Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(8+L+MM) – #(7+N+L +MM)	N	‘XX..XXh’	Titkosítási ellenőrző összeg
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

A READ BINARY parancs a biztonságos üzenetküldés válaszstruktúrájával visszaküldheti azon szabályos feldolgozási állapotokat, amelyek a ‘99h’ címke alatt a TCS_43-ban fel vannak sorolva és le vannak írva a TCS_59-ben.

Ezenkívül felléphet néhány hiba, különösen a biztonságos üzenetküldésre vonatkozóan. Ekkor a feldolgozási állapot egyszerűen visszaérkezik anélkül, hogy biztonságos üzenetküldési struktúrát tartalmazna:

TCS_47 **Válaszüzenet, ha a biztonságos üzenetküldés bemeneti formátuma nem helyes**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha aktuális munkamenetkulcs nem áll rendelkezésre, a visszaküldött feldolgozási állapot: ‘**6A88**’. Ez akkor fordul elő, ha a munkamenetkulcsot még nem generálták, vagy ha a munkamenetkulcs érvényessége lejárt (ekkor az IFD-nek újra le kell futtatnia egy kölcsönös hitelesítési eljárást az új munkamenetkulcs beállításához).

▼B

— Ha a biztonságos üzenetküldési formátumában néhány várt adatobjektum (a fent meghatározottak szerint) hiányzik, a visszaküldött feldolgozási állapot: '**6987**': ez a hiba akkor fordul elő, ha egy várt címke hiányzik, vagy ha a parancstörzs szerkezete nem megfelelő.

— Ha néhány adatobjektum helytelen, a visszaküldött feldolgozási állapot: '**6988**': ez a hiba akkor fordul elő, ha az összes szükséges címke jelen van, de néhány hossz különbözik a várt hossztól.

— Ha a titkosítási ellenőrző összeg ellenőrzése sikertelen, a visszaküldött feldolgozási állapot: '**6688**'.

3.5.2.2 Parancs rövid EF (elemifájl-) azonosítóval

Ez a parancsvariáns lehetővé teszi, hogy egy rövid EF azonosító segítségével az IFD kiválasszon egy EF-t és adatokat olvasson le erről az EF-ről.

TCS_48 A tachográfkártya támogatja ezt a parancsvariánst minden olyan EF esetében, amely meghatározott rövid EF azonosítóval rendelkezik. Ezeket a rövid EF azonosítókat a 4. fejezet határozza meg.

TCS_49 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	A 8-as bitet 1-re kell állítani. A 7-es és 6-os bitet 00-ra kell állítani. Az 5–1-es bit a megfelelő EF rövid EF azonosítóját kódolja
P2	1	'XXh'	0 és 255 bájt közötti eltolást kódol a P1 által megadott EF-ben
Le	1	'XXh'	A várt adathossz. Az olvasandó bájtok száma.

Megjegyzés: A 2. generációs tachográf-alkalmazás rövid EF azonosítóit a 4. fejezet határozza meg.

Ha P1 rövid EF azonosítót kódol és a parancs sikeres, az azonosított EF lesz az aktuálisan kiválasztott EF (aktuális EF).

TCS_50 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #L	L	'XX..XXh'	Kiolvasott adat
SW	2	'XXXXh'	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: '**9000**'.

— Ha a fájlazonosítónak megfelelő EF azonosító nem található, a visszaküldött feldolgozási állapot: '**6A82**'.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a '**6982**' értékkel.

▼B

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: '**6B00**'.

— Ha a kiolvasandó adat mérete nem egyeztethető össze az EF méretével (eltolás + Le > EF méret), a visszaküldött feldolgozási állapot: '**6700**' vagy '**6Cxx**', ahol 'xx' a pontos hosszt jelzi.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: '**6400**' vagy '**6581**'.

— Ha az eltárolt adatokon belül integritási hiba érzékelhető, a kártya visszaküldi a kívánt adatokat, és a visszaküldött feldolgozási állapot: '**6281**'.

3.5.2.3 Parancs páratlan parancsbájttal

Ez a parancsvariáns lehetővé teszi, hogy az IFD adatokat olvasson ki egy legalább 32 768 bájtos EF-ből.

TCS_51 Az a tachográfkártya, amely támogatja a legalább 32 768 bájtos EF-eket, támogatja ezt a parancsvariánst ezen EF-ek esetében. A tachográfkártya támogathatja vagy elutasíthatja ezt a parancsvariánst más EF-ek esetében, kivéve a Sensor_Installation_Data EF-et, lásd: TCS_156 és TCS_160 szakaszt.

TCS_52 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuális EF
P2	1	'00h'	
Lc	1	'NNh'	Az eltolt adatobjektum Lc hossza
#6 – #(5+NN)	NN	'XX..XXh'	Eltolt adatobjektum: Címke '54h' Hossz '01h' vagy '02h' Érték eltolás
Le	1	'XXh'	Az olvasandó bájtok száma.

Az IFD az eltolt adatobjektum hosszát a lehető legkisebb oktettben kifejezett számmal kódolja, azaz az IDF egy '01h' hosszbájt felhasználásával egy 0 és 255 bájt közötti eltolást, egy '02h' hossz-bájt felhasználásával pedig egy '256' és '65 535' bájt közötti eltolást kódol.

TCS_53 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #L	L	'XX..XXh'	Kiolvasott adatok, amelyek beillesztésre kerülnek egy tetszés szerinti, '53h' címkével ellátott adatobjektumba
SW	2	'XXXXh'	Állapotszavak (SW1, SW2)

▼B

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha nincs kiválasztott EF, a visszaküldött feldolgozási állapot: ‘**6986**’.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a ‘**6982**’ értékkel.

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: ‘**6B00**’.

— Ha a kiolvasandó adat mérete nem egyeztethető össze az EF méretével (eltolás + Le > EF méret), a visszaküldött feldolgozási állapot: ‘**6700**’ vagy ‘**6Cxx**’, ahol ‘xx’ a pontos hosszt jelzi.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: ‘**6400**’ vagy ‘**6581**’.

— Ha az eltárolt adatokon belül integritási hiba érzékelhető, a kártya visszaküldi a kívánt adatokat, és a visszaküldött feldolgozási állapot: ‘**6281**’.

3.5.2.3.1 Parancs biztonságos üzenetküldéssel (példa)

A következő példa a biztonságos üzenetküldés alkalmazását szemlélteti olyan esetben, amikor az SM-MAC-G2 biztonsági feltétel alkalmazandó.

TCS_54 Parancsüzenet

Bájt	Hossz	Érték	Leírás
CLA	1	‘0Ch’	Biztonságos üzenetküldés kérése
INS	1	‘B1h’	Read Binary
P1	1	‘00h’	Aktuális EF
P2	1	‘00h’	
Lc	1	‘XXh’	A biztosított adatmező hossza
#6	1	‘B3h’	Címke a BER-TLV-ben kódolt normálérték-adatokhoz
#7	1	‘NNh’	L_{PV}: a továbbított adat hossza
#(8) – #(7+NN)	NN	‘XX..XXh’	BER-TLV-ben kódolt normál adatok, azaz eltolt adatobjektum ‘54’ címkével
#(8+NN)	1	‘97h’	T_{LE}: Címke a várt hossz meghatározására
#(9+NN)	1	‘01h’	L_{LE}: Várt hossz
#(10+NN)	1	‘XXh’	A várt hossz meghatározása (eredeti Le): Az olvasandó bájtok száma
#(11+NN)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(12+NN)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(13+NN) – #(12+M+NN)	M	‘XX..XXh’	Titkosítási ellenőrző összeg
Le	1	‘00h’	Az ISO/IEC 7816-4 szabvány meghatározása szerint

▼B

TCS_55 Válaszüzenet, ha a parancs sikeres

Bájt	Hossz	Érték	Leírás
#1	1	‘B3h’	BER-TLV-ben kódolt normál adatok
#2	L	‘NNh’ vagy ‘81 NNh’	L_{PV}: a visszaküldött adat hossza (= eredeti Le) L 2 bájtos, ha L_{PV}>127 bájt
#(2+L) – #(1+L+NN)	NN	‘XX..XXh’	BER-TLV-ben kódolt normáladat-érték, azaz olyan kiolvasott adatok, amelyek beillesztésre kerülnek egy tetszés szerinti, ‘53h’ címkével ellátott adatobjektumba
#(2+L+NN)	1	‘99h’	A nem védett APDU válasz feldolgozási állapota
#(3+L+NN)	1	‘02h’	Feldolgozási állapot hossza
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	A nem védett APDU válasz feldolgozási állapota
#(6+L+NN)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(7+L+NN)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(8+L+NN) – #(7+M+L+N-N)	M	‘XX..XXh’	Titkosítási ellenőrző összeg
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

3.5.3 *UPDATE BINARY*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

Az UPDATE BINARY parancsüzenet kezdeményezi a már az EF bináris értékben jelen levő bitek aktualizálását (törlés + írás) az APDU parancsban megadott bitekkel.

3.5.3.1 Parancs eltolással a P1-P2-ben

Ez a parancs lehetővé teszi, hogy az IFD adatokat írjon az aktuálisan kiválasztott EF-be anélkül, hogy a kártya ellenőrizné a fogadott adatok integritását.

Megjegyzés: Biztonságos üzenetküldés nélkül ez a parancs csak arra használható, hogy frissítsen egy olyan fájlt, amely támogatja a hozzáférés frissítése üzemmóddal kapcsolatos ALW biztonsági feltételt.

TCS_56 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legnagyobb helyértékű bájt
P2	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legkisebb helyértékű bájt

▼B

Bájt	Hossz	Érték	Leírás
Lc	1	‘NNh’	A várt adat Lc hossza. A beírandó bájtok száma
#6 – #(5+NN)	NN	‘XX..XXh’	A beírandó adatok

Megjegyzés: a P1 8-as bitjét 0-ra kell állítani.

TCS_57 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha nincs kiválasztott EF, a visszaküldött feldolgozási állapot: ‘**6986**’.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a ‘**6982**’ értékkel.

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: ‘**6B00**’.

— Ha a beírandó adatok mérete nem egyeztethető össze az EF méretével (eltolási érték + Lc > EF mérete), a visszaküldött feldolgozási állapot: ‘**6700**’.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: ‘**6400**’ vagy ‘**6500**’.

— Ha a beírás sikertelen, a visszaküldött feldolgozási állapot: ‘**6581**’.

3.5.3.1.1 Parancs biztonságos üzenetküldéssel (példák)

Ez a parancs lehetővé teszi, hogy az IDF adatokat írjon az aktuálisan kiválasztott EF-be, miközben a kártya ellenőrzi a fogadott adatok teljességét. Mivel a titkosság nem követelmény, az adatokat nem kell titkosítani.

TCS_58 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘0Ch’	Biztonságos üzenetküldés kérése
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legnagyobb helyértékű bájt
P2	1	‘XXh’	Eltolás bájtokban a fájl elejétől kezdve: a legkisebb helyértékű bájt
Lc	1	‘XXh’	A biztosított adatmező hossza
#6	1	‘81h’	T_{PV}: Címke a normál értékadatokhoz
#7	L	‘NNh’ vagy ‘81 NNh’	L_{PV}: a továbbított adatok hossza L 2 bájtos, ha L_{PV} > 127 bájt

▼B

Bájt	Hossz	Érték	Leírás
#(7+L) – #(6+L+NN)	NN	‘XX..XXh’	Normál adatérték (beírandó adatok)
#(7+L+NN)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(8+L+NN)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza ‘04h’ az 1. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék A. rész) Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(9+L+NN) – #(8+M+L+N-N)	M	‘XX..XXh’	Titkosítási ellenőrző összeg
Le	1	‘00h’	Az ISO/IEC 7816-4 szabvány meghatározása szerint

TCS_59 **Válaszüzenet, ha a biztonságos üzenetküldés bemeneti formátuma helyes**

Bájt	Hossz	Érték	Leírás
#1	1	‘99h’	T_{SW}: Címke az állapotszavak részére (CC-vel védendő)
#2	1	‘02h’	L_{SW}: a visszaküldött állapotszavak hossza
#3 – #4	2	‘XXXXh’	A nem védett APDU válasz feldolgozási állapota
#5	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#6	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza ‘04h’ az 1. generációs biztonságos üzenetküldés esetén (lásd:11. függelék A. rész) Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#7 – #(6+L)	L	‘XX..XXh’	Titkosítási ellenőrző összeg
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

A biztonságos üzenetküldés nélküli (lásd: 3.5.3.1. pont) UPDATE BINARY parancshoz leírt „szabályos” feldolgozási állapotok visszaküldhetők a fentiekben leírt válaszüzenet-strukturát felhasználva.

Ezenkívül felléphet néhány hiba, különösen a biztonságos üzenetküldésre vonatkozóan. Ekkor a feldolgozási állapot egyszerűen visszaérkezik anélkül, hogy biztonságos üzenetküldési struktúrát tartalmazna:

TCS_60 **Válaszüzenet, ha a biztonságos üzenetküldésben hiba van**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

▼B

— Ha aktuális munkamenetkulcs nem áll rendelkezésre, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha a biztonságos üzenetküldési formátumában néhány várt adatobjektum (a fent meghatározottak szerint) hiányzik, a visszaküldött feldolgozási állapot: ‘**6987**’: ez a hiba akkor fordul elő, ha egy várt címke hiányzik, vagy ha a parancstörzs szerkezete nem megfelelő.

— Ha néhány adatobjektum helytelen, a visszaküldött feldolgozási állapot: ‘**6988**’: ez a hiba akkor fordul elő, ha az összes szükséges címke jelen van, de néhány hossz különbözik a várt hossztól.

— Ha a titkosítási ellenőrző összeg ellenőrzése sikertelen, a visszaküldött feldolgozási állapot: ‘**6688**’.

3.5.3.2 Parancs rövid EF azonosítóval

Ez a parancsvariáns lehetővé teszi, hogy egy rövid EF azonosító segítségével az IFD kiválasszon egy EF-t és adatokat írjon le erről az EF-ről.

TCS_61 A tachográfkártya támogatja ezt a parancsvariánst minden olyan EF esetében, amely meghatározott rövid EF azonosítóval rendelkezik. Ezeket a rövid EF azonosítókat a 4. fejezet határozza meg.

TCS_62 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	A 8-as bitet 1-re kell állítani. A 7-es és 6-os bitet 00-ra kell állítani. Az 5–1-es bit a megfelelő EF rövid EF azonosítóját kódolja
P2	1	‘XXh’	0 és 255 bájt közötti eltolást kódol a P1 által megadott EF-ben
Lc	1	‘NNh’	A várt adat Lc hossza. A beírandó bájtok száma
#6 – #(5+NN)	NN	‘XX..XXh’	A beírandó adatok

TCS_63 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

Megjegyzés: A 2. generációs tachográf-alkalmazás rövid EF azonosítóit a 4. fejezet határozza meg.

Ha P1 rövid EF azonosítót kódol és a parancs sikeres, az azonosított EF lesz az aktuálisan kiválasztott EF (aktuális EF).

▼B

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha a fájlazonosítónak megfelelő EF azonosító nem található, a visszaküldött feldolgozási állapot: ‘**6A82**’.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a ‘**6982**’ értékkel.

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: ‘**6B00**’.

— Ha a beírandó adatok mérete nem egyeztethető össze az EF méretével (eltolási érték + Lc > EF mérete), a visszaküldött feldolgozási állapot: ‘**6700**’.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: ‘**6400**’ vagy ‘**6581**’.

— Ha a beírás sikertelen, a visszaküldött feldolgozási állapot:‘**6581**’.

3.5.3.3 Parancs páratlan parancsbájttal

Ez a parancsvariáns lehetővé teszi, hogy az IFD adatokat írjon egy legalább 32 768 bájtos EF-re.

TCS_64 Az a tachográfkártya, amely támogatja a legalább 32 768 bájtos EF-eket, támogatja ezt a parancsvariánst ezen EF-ek esetében. A tachográfkártya támogathatja vagy elutasíthatja ezt a parancsvariánst más EF-ek esetében.

TCS_65 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘D7h’	Update Binary
P1	1	‘00h’	Aktuális EF
P2	1	‘00h’	
Lc	1	‘NNh’	A parancsadat-mező adatainak Lc hossza
#6 – #(5+NN)	NN	‘XX..XXh’	Eltolt adatobjektum ‘54h’ || címkével Tetszés szerinti, ‘53h’ címkével ellátott adatobjektum, amelybe beillesztésre kerültek a beírandó adatok

Az IFD az eltolt adatobjektum és a tetszés szerinti adatobjektum hosszát a lehető legkisebb oktettben kifejezett számmal kódolja, azaz az IDF egy ‘01h’ hossz-bájt felhasználásával egy 0 és 255 bájt közötti eltolást/hosszt, egy ‘02h’ hosszbájt felhasználásával pedig egy ‘256’ és ‘65 535’ bájt közötti eltolást/hosszt kódol.

TCS_66 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

▼B

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha nincs kiválasztott EF, a visszaküldött feldolgozási állapot: ‘**6986**’.

— Ha a kiválasztott fájl biztonsági feltételei nem teljesülnek, a parancs megszakad a ‘**6982**’ értékkel.

— Ha az eltolás nem egyeztethető össze az EF méretével (eltolás > EF méret), a visszaküldött feldolgozási állapot: ‘**6B00**’.

— Ha a beírandó adatok mérete nem egyeztethető össze az EF méretével (eltolás érték + Lc > EF mérete), a visszaküldött feldolgozási állapot: ‘**6700**’.

— Ha a fájl attribútumain belül integritási hiba érzékelhető, a kártya a fájlt sérültnek és javíthatatlannak tekinti, a visszaküldött feldolgozási állapot pedig: ‘**6400**’ vagy ‘**6500**’.

— Ha a beírás sikertelen, a visszaküldött feldolgozási állapot: ‘**6581**’.

3.5.3.3.1 Parancs biztonságos üzenetküldéssel (példa)

A következő példa a biztonságos üzenetküldés alkalmazását szemlélteti olyan esetben, amikor az SM-MAC-G2 biztonsági feltétel alkalmazandó.

TCS_67 Parancsüzenet

Bájt	Hossz	Érték	Leírás
CLA	1	‘0Ch’	Biztonságos üzenetküldés kérése
INS	1	‘D7h’	Update Binary
P1	1	‘00h’	Aktuális EF
P2	1	‘00h’	
Lc	1	‘XXh’	A biztosított adatmező hossza
#6	1	‘B3h’	Címke a BER-TLV-ben kódolt normálérték-adatokhoz
#7	L	‘NNh’ vagy ‘81 NNh’	L_{PV}: a továbbított adatok hossza L 2 bájtos, ha L_{PV} > 127 bájt
#(7+L) – #(6+L+NN)	NN	‘XX..XXh’	BER-TLV-ben kódolt normál adatok, azaz eltolt adatobjektum ‘54h’ || címkével Tetszés szerinti, ‘53h’ címkével ellátott adatobjektum, amelybe beillesztésre kerültek a beírandó adatok
#(7+L+NN)	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#(8+L+NN)	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#(9+L+NN) – #(8+M+L+N-N)	M	‘XX..XXh’	Titkosítási ellenőrző összeg
Le	1	‘00h’	Az ISO/IEC 7816-4 szabvány meghatározása szerint

▼B

TCS_68 Válaszüzenet, ha a parancs sikeres

Bájt	Hossz	Érték	Leírás
#1	1	‘99h’	T_{SW}: Címke az állapotszavak részére (CC-vel védendő)
#2	1	‘02h’	L_{SW}: a visszaküldött állapotszavak hossza
#3 – #4	2	‘XXXXh’	A nem védett APDU válasz feldolgozási állapota
#5	1	‘8Eh’	T_{CC}: Címke a titkosítási ellenőrző összeghez
#6	1	‘XXh’	L_{CC}: A következő titkosítási ellenőrző összeg hossza Az AES kulcs hosszától függően ‘08h’, ‘0Ch’ vagy ‘10h’ a 2. generációs biztonságos üzenetküldés esetén (lásd: 11. függelék B. rész)
#7 – #(6+L)	L	‘XX..XXh’	Titkosítási ellenőrző összeg
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

3.5.4 *GET CHALLENGE*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

A GET CHALLENGE parancs a kártyát egy véletlen szám kiadására kéri, amelyet egy olyan, a biztonsággal kapcsolatos eljárásban használ fel, amelyben egy kriptogramnak vagy néhány titkosított adatnak a kártyára küldésére kerül sor.

TCS_69 A kártya által kiadott véletlen szám csak a következő parancsra érvényes, amely egy, a kártyára küldött véletlen számot használ fel.

TCS_70 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (a várt véletlen szám hossza)

TCS_71 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #8	8	‘XX..XXh’	Véletlen szám
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az Le eltér a ‘08h’ értéktől, a feldolgozási állapot: ‘**6700**’.

— Ha a P1-P2 paraméterek helytelenek, a feldolgozási állapot: ‘**6A86**’.

▼B

3.5.5 *VERIFY*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

Ezt a parancsot csak a műhelykártyának kell támogatnia.

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot, de esetükben nem kerül sor referencia-CHV megszemélyesítésére. Ezért ezek a kártyák nem tudják végrehajtani teljes körűen a szóban forgó parancsot. A parancs megküldésekor ez a viselkedés, vagyis hibaüzenet visszaküldése a műhelykártyától eltérő típusú tachográfkártyák esetében ezen előírás hatókörén kívül esik.

A Verify parancs megkezdi a kártyán a parancsból elküldött CHV (PIN) adatoknak a kártyán eltárolt referencia-CHV-val történő összehasonlítását.

TCS_72 A felhasználó által betáplált PIN-t ASCI-ben kell kódolni és jobb oldalon az IFD-nek fel kell tölteni ‘FFh’ bájtokkal, maximum 8 bájt hosszúságban, lásd még a Workshop-CardPIN adattípust az 1. függelékben.

TCS_73 Az 1. és 2. generációs tachográf-alkalmazásoknak ugyanazt a referencia-CHV-t kell használniuk.

TCS_74 A tachográfkártya megvizsgálja, hogy a parancs helyesen lett-e kódolva. Ha a parancs nem lett helyesen kódolva, a kártya nem hasonlítja össze a CHV értékeket, nem csökkenti a maradék CHV kísérletek számlálóját és nem állítja vissza a „PIN_Verified” biztonsági állapotot, hanem megszakítja a parancsot. A parancs kódolása helyes, ha a CLA, INS, P1, P2, Lc bájtok a meghatározott értékekkel rendelkeznek, Le nincs és a parancsadat-mező hossza megfelelő.

TCS_75 Ha a parancs sikeres, a maradék CHV kísérletek számlálója újra inicializálásra kerül. A maradék CHV kísérletek számlálójának kezdeti értéke: 5. Ha a parancs sikeres, a kártya a belső biztonsági állapotot „PIN_Verified”-ra állítja. A kártya visszaállítja ezt a biztonsági állapotot, ha a kártyát alaphelyzetbe állítják vagy ha a parancsban továbbított CHV kód nem illeszkedik a tárolt referencia-CHV-hoz.

Megjegyzés: Az ugyanazon referencia-CHV és az általános biztonsági állapot használata feleslegessé teszi, hogy egy másik tachográf-alkalmazás DF kiválasztását követően a műhely valamely munkatársának újra be kelljen táplálnia a PIN kódot.

TCS_76 A sikertelen összehasonlítást rögzíteni kell a kártyán (azaz a maradék CHV kísérletek számlálóját csökkenteni kell eggyel) annak érdekében, hogy a referencia-CHV használatára tett további kísérletek száma korlátozva legyen.

TCS_77 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘20h’	INS
P1	1	‘00h’	P1

▼B

Bájt	Hossz	Érték	Leírás
P2	1	‘00h’	P2 (az ellenőrzött CHV implicite ismert)
Lc	1	‘08h’	A továbbított CHV-kód hossza
#6 – #13	8	‘XX..XXh’	CHV

TCS_78 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha a referencia-CHV nem található, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha a CHV blokkolt (a maradék CHV kísérletek számlálója nulla), a visszaküldött feldolgozási állapot: ‘**6983**’. Ha ezen állapot bekövetkezik, a CHV nem jelenhet meg többé eredményesen.

— Ha az összehasonlítás sikertelen, a maradék kísérletek számlálójának értéke csökken, és a ‘**63CX**’ állapot érkezik vissza (X>0, és X egyenlő a maradék CHV kísérletek számlálójával).

— Ha a referencia-CHV sérültnek minősül, a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

— Ha az Lc eltér a ‘08h’ értéktől, a feldolgozási állapot: ‘**6700**’.

3.5.6 *GET RESPONSE*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak.

Ez a parancs (csak a T=0 protokoll esetében szükséges és áll rendelkezésre) az előkészített adatoknak a kártyáról az interfészkészülék felé történő továbbítására szolgál (azon eset, amikor a parancs az Lc-t és az Le-t is tartalmazta).

A GET RESPONSE parancsot közvetlenül az adatelőkészítési parancs után kell kiadni, különben az adatok elvesznek. A GET RESPONSE parancs végrehajtása után (kivéve, ha a ‘**61xx**’ vagy ‘**6Cxx**’ hiba fordul elő, lásd alább) az előzőleg előkészített adatok többé nem állnak rendelkezésre.

TCS_79 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	A várt bájtok száma

▼B

TCS_80 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #X	X	‘XX..XXh’	Adatok
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha a kártya nem készített elő adatot, a visszaküldött feldolgozási állapot: ‘**6900**’ vagy ‘**6F00**’.

— Ha Le meghaladja a rendelkezésre álló bájtok számát, vagy ha az Le nulla, úgy a visszaküldött feldolgozási állapot: ‘**6Cxx**’, ahol xx a rendelkezésre álló bájtok pontos számát jelöli. Ebben az esetben az előkészített adatok még rendelkezésre állnak a következő GET RESPONSE parancshoz is.

— Ha Le nem nulla és kevesebb, mint a rendelkezésre álló bájtok száma, normál esetben a kártya elküldi a kívánt adatokat, és a visszaküldött feldolgozási állapot: ‘**61xx**’, ahol xx azon extra bájtok számát jelöli, amelyek még rendelkezésre állnak egy későbbi GET RESPONSE parancs végrehajtásához.

— Ha a parancs nem támogatott (T=1 protokoll), a kártya ezt küldi vissza: ‘**6D00**’.

3.5.7 *PSO: VERIFY CERTIFICATE*

Ez a parancs megfelel az ISO/IEC 7816-8 szabványnak, de a használata korlátozott a szabványban meghatározott parancshoz képest.

A VERIFY CERTIFICATE parancsot arra használja a kártya, hogy kívülről egy nyilvános kulcsot kapjon, és ellenőrizze annak érvényességét.

3.5.7.1 1. generációs parancs – válaszpár

TCS_81 Ezt a parancsvariánst csak 1. generációs tachográf-alkalmazás támogatja.

TCS_82 Amennyiben a VERIFY CERTIFICATE parancs sikeres, a nyilvános kulcs a biztonsági környezetben tárolódik későbbi használat céljából. Ezt a kulcsot kifejezetten a biztonságot érintő parancsok keretében való használatra kell beállítani (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE vagy VERIFY CERTIFICATE) az MSE paranccsal (lásd: 3.5.11. pont) annak kulcsazonosítóját felhasználva.

TCS_83 A VERIFY CERTIFICATE parancs minden esetben az MSE paranccsal előzőleg kiválasztott nyilvános kulcsot használja fel a tanúsítvány megnyitására. A nyilvános kulcsnak egy tagállami vagy európai nyilvános kulcsnak kell lennie.

TCS_84 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘00h’	P1

▼B

Bájt	Hossz	Érték	Leírás
P2	1	‘AEh’	P2: nem BER-TLV-ben kódolt adatok (az adatelemek összefűzése)
Lc	1	‘C2h’	Lc: A tanúsítvány hossza, 194 bájt
#6 – #199	194	‘XX..XXh’	Tanúsítvány: adatelemek összefűzése (a 11. függelékben leírtak szerint)

TCS_85 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha a tanúsítvány ellenőrzése sikertelen, a visszaküldött feldolgozási állapot: ‘**6688**’. G1 és G2 tekintetében a tanúsítvány ellenőrzési és kicsomagolási eljárásának leírása a 11. függelékben található.

— Ha nincs nyilvános kulcs a biztonsági környezetben, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha a kiválasztott (és a tanúsítvány kicsomagolásához felhasznált) nyilvános kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

— Csak az 1. generációra vonatkozik: ha a kiválasztott (és a tanúsítvány kicsomagolásához felhasznált) nyilvános kulcs ‘00’-tól különböző CHA.LSB-vel rendelkezik (`CertificateHolderAuthorisation.equipmentType`) (tehát nem egy tagállami vagy európai nyilvános kulcs), a visszaküldött feldolgozási állapot: ‘**6985**’.

3.5.7.2 2. generációs parancs – válaszpár

A görbe méretétől függően az ECC tanúsítványok olyan hosszúak lehetnek, hogy azok nem továbbíthatók egyetlen APDU-ban. Ilyen esetben ISO/IEC 7816-4 szabvány szerinti parancsláncot kell alkalmazni, és a tanúsítványt két egymást követő PSO: Verify Certificate APDU-ban kell továbbítani.

A tanúsítvány struktúráját és a domain paramétereit a 11. függelék határozza meg.

TCS_86 A parancs végrehajtható a következőkben: MF, DF Tachograph és DF Tachograph_G2, lásd még: TCS_33.

TCS_87 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘X0h’	A parancsláncot jelző CLA-bájt: ‘00h’ a lánc egyetlen vagy utolsó parancsa ‘10h’ a lánc nem utolsó parancsa
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘00h’	
P2	1	‘BEh’	Az önleíró tanúsítvány ellenőrzése

▼B

Bájt	Hossz	Érték	Leírás
Lc	1	‘XXh’	A parancsadat-mező hossza, lásd: TCS_88 és TCS_89 szakasz.
#6 – #5+L	L	‘XX..XXh’	DER-TLV-ben kódolt adatok: ECC Certificate Body adatobjektum mint első adatobjektum összefűzve az ECC Certificate Signature adatobjektummal mint második adatobjektummal, vagy e láncolat egy része. A ‘7F21’ címke és a megfelelő hossz nem továbbítandó. Ezen adatobjektumok sorrendje rögzített.

TCS_88 A rövid hosszúságú APDU-kra a következő előírások vonatkoznak: Az IFD azt a minimális számú APDU-t használja, amelyre a parancsadatok továbbításához szüksége van, és az első APDU parancsban a maximális számú bájtot továbbítja az IFSC értékének megfelelően, lásd: TCS_14 szakasz. Ha az IFD másként viselkedik, a kártya viselkedése e meghatározás hatókörén kívül esik.

TCS_89 A kiterjesztett hosszal rendelkező APDU-kra a következő előírások vonatkoznak: ha a tanúsítvány nem fér el egyetlen APDU-ban, a kártya a parancsláncot támogatja. Az IFD azt a minimális számú APDU-t használja, amelyre a parancsadatok továbbításához szüksége van, és az első APDU parancsban a maximális számú bájtot továbbítja. Ha az IFD másként viselkedik, a kártya viselkedése e meghatározás hatókörén kívül esik.

Megjegyzés: A 11. függeléknek megfelelően a kártya eltárolja a tanúsítványt vagy a tanúsítvány releváns tartalmait, és frissíti annak currentAuthenticatedTime adatát.

A válaszüzenet struktúrája és az állapotszavak a TCS_85 szerint kerülnek meghatározásra.

TCS_90 A TCS_85-ben felsorolt hibakódokon kívül a kártya a következő hibakódokat küldheti vissza:

— Ha a kiválasztott (és a tanúsítvány kicsomagolásához felhasznált) nyilvános kulcs olyan CHA.LSB-vel rendelkezik (CertificateHolderAuthorisation.equipmentType), amely nem alkalmas a tanúsítvány 11. függelék szerinti ellenőrzésére, a visszaküldött feldolgozási állapot: ‘**6985**’.

— Ha a kártya szerinti currentAuthenticatedTime későbbi időpont, mint a tanúsítvány lejárata, a visszaküldött feldolgozási állapot: ‘**6985**’.

— Ha a lánc utolsó parancsa várható, a kártya ezt küldi vissza: ‘**6883**’.

— Ha a parancsadat-mezőben helytelen paraméterek kerültek küldésre, a kártya ezt küldi vissza: ‘**6A80**’ (abban az esetben is, ha az adatobjektumok nem a meghatározott sorrendben kerültek küldésre).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak.

TCS_91 Minden tachográfkártya támogatja ezt a parancsot a DF Tachograph G1 alkalmazásban. A parancs elérhető vagy nem elérhető az MF-ben és/vagy a DF Tachograph G2 alkalmazásban. Ha elérhető, a parancs megfelelő hibakóddal leáll, mivel a kártya privát kulcsa (Card.SK) az 1. generációs hitelesítési protokoll esetében csak a DF Tachograph G1 alkalmazásban érhető el.

Az INTERNAL AUTHENTICATE parancs felhasználásával az IFD hitelesítheti a kártyát. A hitelesítési eljárást a 11. függelék írja le. Az a következő utasításokat tartalmazza:

TCS_92 Az INTERNAL AUTHENTICATE parancs a kártya privát kulcsát (implicite kiválasztva) használja a hitelesítési adatok, köztük a K1 (a munkamenetkulcs megállapodás első eleme) és az RND1 aláírására, valamint az (utolsó MSE parancs segítségével) aktuálisan kiválasztott nyilvános kulcsot használja az aláírás titkosítására és a hitelesítési token létrehozására (további részletek a 11. függelékben találhatók).

TCS_93 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	A kártyára küldött adatok hossza
#6 – #13	8	‘XX..XXh’	A kártya hitelesítéséhez felhasznált véletlen szám
#14 – #21	8	‘XX..XXh’	VU.CHR (lásd: 11. függelék)
Le	1	‘80h’	A kártyáról várt adatok hossza

TCS_94 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1– #128	128	‘XX..XXh’	Kártyahitelesítési token (lásd: 11. függelék)
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha nincs nyilvános kulcs a biztonsági környezetben, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha nincs privát kulcs a biztonsági környezetben, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha a VU.CHR nem illeszkedik az aktuális nyilvános kulcs azonosítójához, a visszaküldött feldolgozási állapot: ‘**6A88**’.

▼B

— Ha a kiválasztott privát kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: '**6400**' vagy '**6581**'.

TCS_95 Ha az INTERNAL AUTHENTICATE parancs sikeres, az aktuális munkamenetkulcs – amennyiben van ilyen – törlődik, és a továbbiakban nem áll rendelkezésre. Annak érdekében, hogy új munkamenetkulcs álljon rendelkezésre, az 1. generációs hitelesítési mechanizmus esetében az EXTERNAL AUTHENTICATE parancsot sikeresen végre kell hajtani.

3.5.9 *EXTERNAL AUTHENTICATE*

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak.

Az EXTERNAL AUTHENTICATE parancsot felhasználva a kártya hitelesítheti az IFD-t. A G1 és G2 menetíró készülékre vonatkozó hitelesítési eljárást a 11. függelék írja le (VU hitelesítés).

TCS_96 Az 1. generációs kölcsönös hitelesítési mechanizmus esetében a parancsvariánst csak az 1. generációs tachográf-alkalmazás támogatja.

TCS_97 A 2. generációs kölcsönös VU-kártyahitelesítés esetében a parancsvariáns a következőkben hajható végre: MF, DF Tachograph és DF Tachograph_G2 (lásd még: TCS_34).

TCS_98 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Kulcsok és algoritmusok implicite ismertek
P2	1	'00h'	
Lc	1	'XXh'	Lc (a kártyára küldött adatok hossza)
#6 – #(5+L)	L	'XX..XXh'	1. generációra vonatkozó hitelesítés: Kriptogram (lásd: 11. függelék A. rész) 2. generációra vonatkozó hitelesítés: Az IFD által generált aláírás (lásd: 11. függelék B. rész)

TCS_99 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	'XXXXh'	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: '**9000**'.

— Ha az aktuálisan beállított nyilvános kulcs CHA-ja nem a menetíró készülék AID alkalmazásnak és a VU berendezéstípusnak a láncolata, a visszaküldött feldolgozási állapot: '**6F00**'.

— Ha a parancsot nem előzi meg közvetlenül GET CHALLENGE parancs, a visszaküldött feldolgozási állapot: '**6985**'.

▼B

Az 1. generációs tachográf-alkalmazás a következő hibakódokat küldheti vissza:

— Ha nincs nyilvános kulcs a biztonsági környezetben, a visszaküldött feldolgozási állapot: '**6A88**'.

— Ha nincs privát kulcs a biztonsági környezetben, a visszaküldött feldolgozási állapot: '**6A88**'.

— Ha a kriptogram ellenőrzése hibás, a visszaküldött feldolgozási állapot: '**6688**'.

— Ha a kiválasztott privát kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: '**6400**' vagy '**6581**'.

A 2. generációs hitelesítés esetében a parancsvariáns a következő kiegészítő hibakódot küldheti vissza:

— Ha az aláírás ellenőrzése sikertelen, a kártya ezt küldi vissza: '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Ez a parancs a 11. függelék B. részében meghatározott, 2. generációs chiphitelesítési protokoll esetében alkalmazandó és megfelel az ISO/IEC 7816-4 szabványnak.

TCS_100 A parancs végrehajtható a következőkben: MF, DF Tachograph és DF Tachograph_G2, lásd még: TCS_34.

TCS_101 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Kulcsok és protokoll implicite ismertek
P2	1	'00h'	
Lc	1	'NNh'	Lc: a következő adatmező hossza
#6 – #(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV-ben kódolt efemer nyilvános kulcs értéke (lásd:11. függelék) A járműegységnek ebben a sorrendben kell küldenie az adatobjektumokat.

TCS_102 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV-ben kódolt Dynamic Authentication adatok: egyszer használatos véletlen szám (nonce) és hitelesítési token (lásd: 11. függelék)
SW	2	'XXXXh'	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: '**9000**'.

— Az adatmező helytelen paramétereinek jelölésére a kártya ezt küldi vissza: '**6A80**'.

▼B

— Ha az External Authenticate parancs nem került sikeresen végrehajtásra, a kártya ezt küldi vissza: ‘**6982**’.

A ‘7Ch’ Dynamic Authentication válasz-adatobjektumnak

— jelen kell lennie, ha a művelet sikeres, például az állapotszavak: ‘**9000**’,

— nem szabad jelen lennie, ha végrehajtási vagy ellenőrzési hiba történt, vagyis ha az állapotszavak a ‘**6400**’ és ‘**6FFF**’ közötti tartományban vannak, valamint

— hiányozhat figyelmeztetés esetén, vagyis ha az állapotszavak a ‘**6200**’ és ‘**63FF**’ közötti tartományban vannak.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Ez a parancs lehetővé teszi egy nyilvános kulcs hitelesítési célra való beállítását.

3.5.11.1 1. generációs parancs – válaszpár

Ez a parancs megfelel az ISO/IEC 7816-4 szabványnak. A parancs használata korlátozott, tekintettel a vonatkozó szabványra.

TCS_103 Ezt a parancsot csak 1. generációs tachográf-alkalmazás támogatja.

TCS_104 Az MSE adatmezőben említett kulcs marad az aktuális nyilvános kulcs a következő helyes MSE parancsig, a DF kiválasztásáig vagy a kártya alaphelyzetbe állításáig.

TCS_105 Ha az említett kulcs (még) nincs a kártyán, a biztonsági környezet változatlan marad.

TCS_106 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: az említett kulcs érvényes az összes titkosítási műveletre
P2	1	‘B6h’	P2 (az említett adatok a digitális aláírásra vonatkoznak)
Lc	1	‘0Ah’	Lc: a következő adatmező hossza
#6	1	‘83h’	Címke egy nyilvános kulcsra való hivatkozáshoz aszimmetrikus esetekben
#7	1	‘08h’	A kulcsreferencia hossza (kulcsazonosító)
#8 – #15	8	‘XX..XXh’	Kulcsazonosító a 11. függelék meghatározása szerint

TCS_107 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

▼B

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az említett kulcs nincs a kártyán, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha a biztonságos üzenetküldési formátumában néhány várt adatobjektum (a fent meghatározottak szerint) hiányzik, a visszaküldött feldolgozási állapot: ‘**6987**’. Ez akkor történhet meg, ha a ‘83h’ címke hiányzik.

— Ha néhány adatobjektum helytelen, a visszaküldött feldolgozási állapot: ‘**6988**’. Ez akkor történhet meg, ha a kulcsazonosító hossza nem ‘08h’.

— Ha a kiválasztott kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

3.5.11.2 2. generációs parancs – válaszpárok

A 2. generációs hitelesítés esetén a tachográfkártya a következő MSE-t támogatja: Az ISO/IEC 7816-4 szabványnak megfelelő parancsverzió beállítva. Az 1. generációs hitelesítések esetén ezek a parancsverziók nem támogatottak.

3.5.11.2.1 MSE:SET AT chip hitelesítése esetén

A paramétereknek a chip hitelesítése érdekében történő kiválasztásához a következő MSE:SET AT parancs alkalmazandó, melyet az azt követő General Authenticate parancs hajt végre.

TCS_108 A parancs végrehajtható a következőkben: MF, DF Tachograph és DF Tachograph_G2, lásd még: TCS_34.

TCS_109 **MSE:SET AT parancsüzenet chip hitelesítése esetén**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘41h’	Belső hitelesítésre beállítva
P2	1	‘A4h’	Hitelesítés
Lc	1	‘NNh’	Lc: a következő adatmező hossza
#6 – #(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Hivatkozás DER-TLV-ben kódolt titkosítási mechanizmusra: a chiphitelesítés objektumazonosítója (csak az érték, a ‘06h’ címkét el kell hagyni). Az objektumazonosító értékével kapcsolatban lásd az 1. függeléket; alkalmazandó a bájtjelölés. Azzal kapcsolatban, hogy hogyan kell kiválasztani egyet az objektumazonosítók közül, lásd a 11. függeléket.

3.5.11.2.2 MSE:SET AT járműegység hitelesítése esetén

A paramétereknek és kulcsoknak a VU hitelesítése érdekében történő kiválasztásához a következő MSE:SET AT parancs alkalmazandó, melyet az azt követő External Authenticate parancs hajt végre.

▼B

TCS_110 A parancs végrehajtható a következőkben: MF, DF Tachograph és DF Tachograph_G2, lásd még: TCS_34.

TCS_111 **MSE:SET AT parancsüzenet járműegység hitelesítése esetén**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Külső hitelesítésre beállítva
P2	1	‘A4h’	Hitelesítés
Lc	1	‘NNh’	Lc: a következő adatmező hossza
#6 – #(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Hivatkozás DER-TLV-ben kódolt titkosítási mechanizmusra: A VU-hitelesítés objektumazonosítója (csak az érték, a ‘06h’ címkét el kell hagyni). Az objektumazonosító értékével kapcsolatban lásd az 1. függeléket; alkalmazandó a bájtjelölés. Azzal kapcsolatban, hogy hogyan kell kiválasztani egyet az objektumazonosítók közül, lásd a 11. függeléket.
		‘83h’ + ‘08h’ + ‘XX..XXh’	DER-TLV-ben kódolt hivatkozás a VU nyilvános kulcsára a szóban forgó tanúsítványban említett CHR által.
		‘91h’ + L_{91} + ‘XX..XXh’	Az efemer nyilvános VU kulcs DER-TLV-ben kódolt sűrített reprezentációja, amely a chiphitelesítés során kerül felhasználásra (lásd: 11. függelék)

3.5.11.2.3 MSE:SET DST

A következő MSE:SET DST parancs alkalmazandó a nyilvános kulcs beállításához vagy

— egy olyan aláírás ellenőrzéséhez, amelyet egy soron következő PSO: Verify Digital Signature parancs biztosít, vagy

— egy olyan tanúsítvány aláírásának ellenőrzéséhez, amelyet egy soron következő PSO: Verify Certificate parancs biztosít.

TCS_112 A parancs végrehajtható a következőkben: MF, DF Tachograph és DF Tachograph_G2, lásd még: TCS_33.

TCS_113 **MSE:SET DST parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Ellenőrzésre beállítva
P2	1	‘B6h’	Digitális aláírás

▼B

Lc	1	‘NNh’	Lc: a következő adatmező hossza
#6 – #(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	DER-TLV-ben kódolt hivatkozás egy nyilvános kulcsra, vagyis a CHR a nyilvános kulcs tanúsítványában (lásd: 11. függelék)

Minden parancsverzió esetében a következők adják meg a válaszüzenet struktúráját és állapotszavait:

TCS_114 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’. A protokoll kiválasztásra és inicializálásra került.

— ‘**6A80**’ hibás paramétereket jelez a parancs-adatmezőben.

— ‘**6A88**’ azt jelzi, hogy a hivatkozott adatok (vagyis egy hivatkozott kulcs) nem elérhetők.

3.5.12 *PSO: HASH*

Ezt a parancsot a bizonyos adatokon elvégzett hasítási számítás eredményének a kártyára történő továbbítására kell felhasználni. Ez a parancs a digitális aláírások ellenőrzésére szolgál. A hasítási érték ideiglenesen tárolódik a következő parancshoz: PSO: Verify Digital Signature

Ez a parancs megfelel az ISO/IEC 7816-8 szabványnak. A parancs használata korlátozott, tekintettel a vonatkozó szabványra.

A DF Tachograph és a DF Tachograph_G2 esetében csak az ellenőrzőkártyának kell támogatnia ezt a parancsot.

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot. A parancs elérhető vagy nem elérhető az MF-ben.

Az 1. generációs ellenőrzőkártya-alkalmazás csak az SHA-1-et támogatja.

TCS_115 Az átmenetileg tárolt hasítási értéket törölni kell, ha a PSO: HASH parancs révén új érték került kiszámításra, ha a DF ki lett választva és ha a tachográfkártyát alaphelyzetbe állították.

TCS_116 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘90h’	A hash kód visszaküldése

▼B

Bájt	Hossz	Érték	Leírás
P2	1	‘A0h’	Címke: a hasításhoz megfelelő DO-t tartalmazó adatmező
Lc	1	‘XXh’	A következő Lc adatmező hossza
#6	1	‘90h’	Címke a hash kódhoz
#7	1	‘XXh’	A hash kód L hossza: ‘14h’ az 1. generációs alkalmazás esetében (lásd: 11. függelék A. rész) ‘20h’, ‘30h’ vagy ‘40h’ a 2. generációs alkalmazás esetében (lásd: 11. függelék B. rész)
#8 – #(7+L)	L	‘XX..XXh’	Hash kód

TCS_117 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha néhány várt adatobjektum (a fenti meghatározás szerint) hiányzik, a visszaküldött feldolgozási állapot: ‘**6987**’. Ez akkor történhet meg, ha egy ‘90h’ címke hiányzik.

— Ha néhány adatobjektum helytelen, a visszaküldött feldolgozási állapot: ‘**6988**’. Ez a hiba akkor történik meg, ha a kívánt címke rendelkezésre áll ugyan, de hosszúsága az SHA-1 esetében nem ‘14h’, az SHA-256 esetében nem ‘20h’, az SHA-384 esetében nem ‘30h’ és az SHA-512 esetében nem ‘40h’ (2. generációs alkalmazás).

3.5.13 *PERFORM HASH of FILE*

Ez a parancs nem felel meg az ISO/IEC 7816-8 szabványnak. Így e parancs CLA bájtja jelzi, hogy a PERFORM SECURITY OPERATION/HASH kizárólagos felhasználásáról van szó.

A DF Tachograph és a DF Tachograph_G2 esetében csak a járművezetői és a műhelykártyának kell támogatnia ezt a parancsot.

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot. Ha a vállalkozási és az ellenőrzőkártya végrehajtja ezt a parancsot, annak az e fejezetben meghatározottak szerint kell történnie.

A parancs elérhető vagy nem elérhető az MF-ben. Ha elérhető, a parancsot az e fejezetben meghatározottak szerint kell végrehajtani, azaz a parancs nem teszi lehetővé hasítási érték kiszámítását, de megfelelő hibakóddal leáll.

TCS_118 A PERFORM HASH of FILE parancs az aktuálisan kiválasztott EF transzparens adatterületének hasítási számítására szolgál.

TCS_119 A tachográfkártya ezt a parancsot csak a 4. fejezetben felsorolt EF-ek esetében támogatja a DF_Tachograph és a DF_Tachograph_G2 keretében a következő kivételekkel. A tachográfkártya nem támogatja a parancsot a DF Tachograph_G2-höz tartozó EF Sensor_Installation_Data esetében.

▼B

TCS_120 A hasítási művelet eredményét átmenetileg a kártyán kell tárolni. Ez felhasználható a fájl digitális aláírásának a megszerzésére a PSO: COMPUTE DIGITAL SIGNATURE parancs felhasználásával.

TCS_121 Az átmenetileg tárolt fájlhasítási értéket törölni kell, ha a PSO: Hash of File parancs révén új érték került kiszámításra, ha a DF ki lett választva és ha a tachográfkártyát alaphelyzetbe állították.

TCS_122 Az 1. generációs tachográf-alkalmazás támogatja az SHA-1-et.

TCS_123 A 2. generációs tachográf-alkalmazás támogatja az SHA-1-et és az SHA-2-t (256, 384 és 512 bit).

TCS_124 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘90h’	Címke: Hash
P2	1	‘XXh’	P2: Az aktuálisan kiválasztott transzparens fájl adatainak hasításához használt algoritmust jelzi: ‘00h’ SHA-1 esetében ‘01h’ SHA-256 esetében ‘02h’ SHA-384 esetében ‘03h’ SHA-512 esetében

TCS_125 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az aktuális EF nem engedélyezi ezt a parancsot (EF Sensor_Installation_Data a DF Tachograph_G2-ben), a visszaküldött feldolgozási állapot: ‘**6985**’.

— Ha a kiválasztott EF sérültnek minősül (fájlattribútum vagy az eltárolt adatok integritási hibái), a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

— Ha a kiválasztott fájl nem transzparens fájl vagy nincs aktuális EF, a visszaküldött feldolgozási állapot: ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Ez a parancs az előzőleg kiszámított hash kód digitális aláírásának számítására szolgál (lásd: 3.5.13. pont, PERFORM HASH of FILE).

A DF Tachograph és a DF Tachograph_G2 esetében csak a járművezetői és a műhelykártyának kell támogatnia ezt a parancsot.

▼B

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot, de nincs szükségük aláírási kulcsra. Ezért ezek a kártyák nem tudják sikeresen végrehajtani a parancsot, hanem a parancs megfelelő hibakóddal leáll.

A parancs elérhető vagy nem elérhető az MF-ben. Ha igen, a parancs megfelelő hibakóddal leáll.

Ez a parancs megfelel az ISO/IEC 7816-8 szabványnak. A parancs használata korlátozott, tekintettel a vonatkozó szabványra.

TCS_126 Ez a parancs nem az előzőleg kiszámított hash kód digitális aláírásának számítását szolgálja a PSO: HASH paranccsal.

TCS_127 A kártya privát kulcsát kell felhasználni a digitális aláírás kiszámítására; a kártya implicite ismeri ezt a kulcsot.

TCS_128 Az 1. generációs tachográf-alkalmazás digitális aláírást hajt végre a PKCS1-nek megfelelő feltöltési módszer alkalmazásával (a részleteket lásd a 11. függelékben).

TCS_129 A 2. generációs tachográf-alkalmazás kiszámít egy elliptikus görbén alapuló digitális aláírást (a részleteket lásd a 11. függelékben).

TCS_130 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘9Eh’	Visszaküldendő digitális aláírás
P2	1	‘9Ah’	Címke: az adatmező tartalmazza a jelölendő adatokat. Mivel adatmezőt nem tartalmaz, feltételezhető, hogy az adatok már a kártyán vannak (a fájl hasítása)
Le	1	‘NNh’	A várt aláírás hossza

TCS_131 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #L	L	‘XX..XXh’	Az előzőleg kiszámított hasítás aláírása
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az implicite kiválasztott privát kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

— Ha egy előző Perform Hash of File paranccsal kiszámított hasítás nem elérhető, a visszaküldött feldolgozási állapot: ‘**6985**’.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Ez a parancsot kell felhasználni az adatbevitelként betáplált digitális aláírás ellenőrzésére, amelynek hasítása a kártya számára ismert. Az aláírás algoritmusát a kártya implicite ismeri.

Ez a parancs megfelel az ISO/IEC 7816-8 szabványnak. A parancs használata korlátozott, tekintettel a vonatkozó szabványra.

A DF Tachograph és a DF Tachograph_G2 esetében csak az ellenőrzőkártyának kell támogatnia ezt a parancsot.

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot. A parancs elérhető vagy nem elérhető az MF-ben.

TCS_132 A VERIFY DIGITAL SIGNATURE parancs mindig az előző Manage Security Environment MSE által kiválasztott nyilvános kulcsot használja: DST parancs és egy PSO: HASH parancs által beléptetett előző hash kód beállítása.

TCS_133 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘00h’	
P2	1	‘A8h’	Címke: az ellenőrzésnek megfelelő DO-kat tartalmazó adatmező
Lc	1	‘83h’	A következő Lc adatmező hossza
6	1	‘9Eh’	Címke a digitális aláíráshoz
#7 – #8	2	‘81 XXh’	A digitális aláírás hossza: az 1. generációs tachográf-alkalmazás esetében 128 bájt, a 11. függelék A. részének megfelelően kódolva A 2. generációs tachográf-alkalmazás esetében a kiválasztott görbétől függ (lásd: 11. függelék A. rész)
#9 – #(8+L)	L	‘XX..XXh’	A digitális aláírás tartalma

TCS_134 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— Ha az aláírás ellenőrzése sikertelen, a visszaküldött feldolgozási állapot: ‘**6688**’. Az ellenőrzési eljárást a 11. függelék ismerteti.

— Ha nincs kiválasztott nyilvános kulcs, a visszaküldött feldolgozási állapot: ‘**6A88**’.

— Ha néhány várt adatobjektum (a fenti meghatározás szerint) hiányzik, a visszaküldött feldolgozási állapot: ‘**6987**’. Ez akkor történhet meg, ha a szükséges címkék egyike hiányzik.

▼B

— Ha nem áll rendelkezésre hash kód a parancs feldolgozásához (egy előző PSO: Hash parancs eredményeként), a visszaküldött feldolgozási állapot: ‘**6985**’.

— Ha néhány adatobjektum helytelen, a visszaküldött feldolgozási állapot: ‘**6988**’. Ez akkor történhet meg, ha a szükséges adatobjektumok egyikének hossza helytelen.

— Ha a kiválasztott nyilvános kulcs sérültnek minősül, a visszaküldött feldolgozási állapot: ‘**6400**’ vagy ‘**6581**’.

3.5.16 *PROCESS DSRC MESSAGE*

Ez a parancs a DSRC üzenet sértetlenségének és hitelességének ellenőrzését, valamint a VU által egy ellenőrző hatóság vagy műhely felé a DSRC kapcsolaton keresztül megküldött adatok megfejtését szolgálja. A kártya levezeti a DSRC üzenet védelmére használt titkosítási kulcsot és MAC kulcsot, a 11. függelék B. része 13. fejezetének megfelelően.

A DF Tachograph_G2 esetében csak az ellenőrző- és a műhelykártyának kell támogatnia ezt a parancsot.

Más típusú tachográfkártyák végrehajthatják vagy elutasíthatják ezt a parancsot, de nincs szükségük DSRC mesterkulcsra. Ezért ezek a kártyák nem tudják sikeresen végrehajtani a parancsot, hanem a parancs megfelelő hibakóddal leáll.

A parancs elérhető vagy nem elérhető az MF-ben és/vagy a DF Tachograph alkalmazásban. Ha igen, a parancs megfelelő hibakóddal leáll.

TCS_135 A DSRC mesterkulcs csak a DF Tachograph_G2 alkalmazásban érhető el, azaz az ellenőrző- és a műhelykártyának a parancs végrehajtását csak a DF Tachograph_G2-ben kell támogatnia.

TCS_136 A parancsnak csak titkosítania kell a DSRC adatokat és ellenőriznie kell a titkosítási ellenőrző összeget, de nem szükséges értelmeznie a beviteli adatokat.

TCS_137 A parancs-adatmezőben lévő adatobjektumok sorrendjét ez az előírás rögzíti.

TCS_138 **Parancsüzenet**

Bájt	Hossz	Érték	Leírás
CLA	1	‘80h’	Kizárólagos CLA
INS	1	‘2Ah’	Biztonsági művelet végrehajtása
P1	1	‘80h’	Válaszadatok: normál érték
P2	1	‘B0h’	Parancsadatok: BER-TLV-ben kódolt és SM DO-kat tartalmazó normálérték
Lc	1	‘NNh’	A következő Lc adatmező hossza

▼B

Bájt	Hossz	Érték	Leírás
#6 – #(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	DER-TLV-ben kódolt feltöltésjelző bájt, melyet titkosított tachográfadatok követnek. A feltöltésjelző bájt esetében a ‘00h’ értéket („nincs további adat” az ISO/IEC 7816-4:2013 szabvány 52. táblázatának megfelelően) kell használni. A titkosítási mechanizmushoz lásd a 11. függelék. B. részének 13. fejezetét. Az L_{87} hossz megengedett értékei a feltöltésjelző bájt esetében az AES blokk hosszának többszörösei plusz 1, azaz 17 bájttól 193 bájtig terjedhet. *Megjegyzés:* A ‘87h’ címkével ellátott SM adatobjektumhoz lásd az ISO/IEC 7816-4:2013 szabvány 49. táblázatát.
		‘81h’ + ‘10h’	DER-TLV-ben kódolt Control Reference Template for Confidentiality, mely a következő adatelemek láncolatát tartalmazza (lásd: DSRCSecurityData az 1. függelékben és a 11. függelék B. részének 13. fejezete): — 4 bájt időbélyegző — 3 bájt számláló — 8 bájt VU sorozatszám — 1 bájt DSRC mesterkulcs verzió *Megjegyzés:* A ‘81h’ címkével ellátott SM adatobjektumhoz lásd az ISO/IEC 7816-4:2013 szabvány 49. táblázatát.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	DER-TLV-ben kódolt MAC a DSRC üzenet fölött. A MAC algoritmushoz lásd a 11. függelék. B. részének 13. fejezetét. *Megjegyzés:* A ‘8Eh’ címkével ellátott SM adatobjektumhoz lásd az ISO/IEC 7816-4:2013 szabvány 49. táblázatát.

TCS_139 **Válaszüzenet**

Bájt	Hossz	Érték	Leírás
#1 – #L	L	‘XX..XXh’	Hiányzó adatok (hiba esetén) vagy megfejtett adatok (feltöltés eltávolítva)
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, a kártya ezt küldi vissza: ‘**9000**’.

— ‘**6A80**’ hibás paramétereket jelez a parancs-adatmezőben (akkor is használandó, ha az adatobjektumok nem a meghatározott sorrendben kerültek küldésre).

— ‘**6A88**’ azt jelzi, hogy a hivatkozott adatok nem elérhetők, vagyis a hivatkozott DSRC mesterkulcs nem elérhető.

— ‘**6900**’ azt jelzi, hogy a titkosítási ellenőrző összeg ellenőrzése vagy az adatok titkosítása sikertelen.

4. A TACHOGRÁFKÁRTYÁK STRUKTÚRÁJA

Ez a pont a tachográfkártyák fájlszerkezetét határozza meg a hozzáférhető adatok tárolása szempontjából.

▼B

Nem határozza meg a kártya gyártójától függő olyan belső struktúrákat, mint például a fájl fejrésze, továbbá a csak belső használathoz szükséges adatelemek tárolását és kezelését sem, mint pl. `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` vagy `WorkshopCardPin`.

TCS_140 Egy 2. generációs tachográfkártya elfogadja az MF-et és az azonos típusú 1. és 2. generációs alkalmazást (járművezetőikártya-alkalmazásokat).

TCS_141 A tachográfkártya támogatja a megfelelő alkalmazások tekintetében meghatározott legalább minimális rekordszámot, de nem többet, mint a megfelelő alkalmazások tekintetében meghatározott maximális rekordszámot.

A minimális és maximális rekordszámot a különböző alkalmazások esetében ez a fejezet határozza meg.

Az e fejezet szerinti hozzáférési szabályokban alkalmazott biztonsági feltételekhez lásd a 3.3. fejezetet. Általánosságban a „read” hozzáférési mód a READ BINARY parancsot jelöli páros és – ha támogatott – páratlan INS bájttal, kivéve a műhelykártyán lévő Sensor_Installation_Data EF-et, lásd: TCS_156 és TCS_160 szakasz. Az „update” hozzáférési mód az UPDATE BINARY parancsot jelöli páros és – ha támogatott – páratlan INS bájttal, míg a „select” hozzáférési mód a SELECT parancsot jelöli.

4.1. **Törzsállomány (MF)**

TCS_142 Megszemélyesítés után az MF a következő permanens fájlszerkezettel és fájlhozzáférési szabályokkal rendelkezik:

Megjegyzés: Az SFID rövid EF azonosító tizedes törtként kerül megadásra, így a 30-as érték megfelelője a kettes számrendszerben: 11110.

			Hozzáférési szabályok	
Fájl	**Fájlazonosító**	**SFID**	**Olvasás / Kiválasztás**	**Frissítés**
MF	‘3F00h’			
├─ EF ICC	‘0002h’		ALW	NEV
├─ EF IC	‘0005h’		ALW	NEV
├─ EF DIR	‘2F00h’	30	ALW	NEV
├─ EF ATR/INFO (conditional)	‘2F01h’	29	ALW	NEV
├─ EF Extended_Length (conditional)	‘0006h’	28	ALW	NEV
├─ DF Tachograph	‘0500h’		SC1	
└─ DF Tachograph_G2			SC1	

Ebben a táblázatban a biztonsági feltétellel kapcsolatos következő rövidítés kerül alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

TCS_143 Az összes EF szerkezet transzparens.

TCS_144 Az MF a következő adatszerkezettel rendelkezik:

▼B

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
MF		*63*	*184*	
└─EF ICC		*25*	*25*	
└─CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
└─EF IC		*8*	*8*	
└─CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
└─EF DIR		*20*	*20*	
└─See TCS_145		*20*	*20*	{00..00}
└─EF ATR/INFO		*7*	*128*	
└─See TCS_146		*7*	*128*	{00..00}
└─EF EXTENDED_LENGTH		*3*	*3*	
└─See TCS_147		*3*	*3*	{00..00}
└─DF Tachograph				
└─DF Tachograph_G2				

TCS_145 A DIR EF-nek a következő alkalmazásvonatkozású adatobjektumokat kell tartalmaznia: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’.

TCS_146 Az ATR/INFO EF-nek jelen kell lennie, ha a tachográfkártya jelzi ATR-jében, hogy támogatja a kiterjesztett hosszúságú adatmezőket. Ez esetben az ATR/INFO EF-nek tartalmaznia kell az ISO/IEC 7816-4:2013 szabvány 12.7.1. szakaszában meghatározott, kiterjesztett hosszúságú adatobjektumot (DO‘7F66’).

TCS_147 Az Extended_Length EF-nek jelen kell lennie, ha a tachográfkártya jelzi ATR-jében, hogy támogatja a kiterjesztett hosszúságú adatmezőket. Ez esetben az EF-nek tartalmaznia kell az következő adatobjektumot: ‘02 01 xx’, ahol ‘xx’ érték megmutatja, hogy támogatva vannak-e a kiterjesztett hosszúságú adatmezők a T = 1 és/vagy a T = 0 protokoll esetében.

A ‘01’ a kiterjesztett hosszúságú adatmezők támogatását jelöli a T = 1 protokoll esetében.

A ‘10’ a kiterjesztett hosszúságú adatmezők támogatását jelöli a T = 0 protokoll esetében.

A ‘11’ a kiterjesztett hosszúságú adatmezők támogatását jelöli a T = 1 és a T = 0 protokoll esetében.

4.2. **Járművezetőikártya-alkalmazások**

4.2.1 *1. generációs járművezetőikártya-alkalmazás*

TCS_148 Megszemélyesítés után az 1. generációs járművezetőikártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési feltételekkel rendelkezik:

Fájl	Fájlazonosító	Hozzáférési szabályok Olvasás	Kiválasztás	Frissítés
└─DF Tachograph	‘0500h’		SC1	
├─EF Application_Identification	‘0501h’	SC2	SC1	NEV
├─EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├─EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├─EF Identification	‘0520h’	SC2	SC1	NEV
├─EF Card_Download	‘050Eh’	SC2	SC1	SC1
├─EF Driving_Licence_Info	‘0521h’	SC2	SC1	NEV
├─EF Events_Data	‘0502h’	SC2	SC1	SC3
├─EF Faults_Data	‘0503h’	SC2	SC1	SC3
├─EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├─EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├─EF Places	‘0506h’	SC2	SC1	SC3
├─EF Current_Usage	‘0507h’	SC2	SC1	SC3
├─EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└─EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

▼B

Ebben a táblázatban a biztonsági feltételekkel kapcsolatos következő rövidítések kerülnek alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

SC2 ALW VAGY SM-MAC-G1 VAGY SM-MAC-G2

SC3 SM-MAC-G1 VAGY SM-MAC-G2

TCS_149 Az összes EF szerkezet transzparens.

TCS_150 Az 1. generációs járművezetőikártya-alkalmazás a következő adatszerkezettel rendelkezik:

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
DF Tachograph		*11378*	*2492*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

▼B

vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

▼B

TCS_151 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket az 1. generációs járművezetői kártya-alkalmazás adatstruktúrájának alkalmazni kell:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bájt (28 nap * 93 tevékenységváltás)	13 776 bájt (28 nap * 240 tevékenységváltás)

4.2.2 *2. generációs járművezetőikártya-alkalmazás*

TCS_152 Megszemélyesítés után a 2. generációs járművezetőikártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési szabályokkal rendelkezik:

Megjegyzés: Az SFID rövid EF azonosító tizedes törtként kerül megadásra, így a 30-as érték megfelelője a kettes számrendszerben: 11110.

			Hozzáférési szabályok	
Fájl	**Fájlazonosító**	**SFID**	**Olvasás / Kiválasztás**	**Frissítés**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	‘0501h’	1	SC1	NEV
├─EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─EF CardSignCertificate	‘C101h’	3	SC1	NEV
├─EF CA_Certificate	‘C108h’	4	SC1	NEV
├─EF Link_Certificate	‘C109h’	5	SC1	NEV
├─EF Identification	‘0520h’	6	SC1	NEV
├─EF Card_Download	‘050Eh’	7	SC1	SC1
├─EF Driving_Licence_Info	‘0521h’	10	SC1	NEV
├─EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
├─EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
├─EF Places	‘0506h’	16	SC1	SM-MAC-G2
├─EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	‘0522h’	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	‘0523h’	20	SC1	SM-MAC-G2
└─EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

Ebben a táblázatban a biztonsági feltétellel kapcsolatos következő rövidítés kerül alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

TCS_153 Az összes EF szerkezet transzparens.

TCS_154 A 2. generációs járművezetőikártya-alkalmazás a következő adatszerkezettel rendelkezik:

▼B

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
DF Tachograph_G2		*19510*	*3930*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

▼B

├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*4032*	*9600*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├─placePointerNewestRecord		2	2	{00 00}
└─placeRecords		*1764*	*2352*	
└─PlaceRecord	n_4	*21*	*21*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
├─vehicleOdometerValue		3	3	{00..00}
└─entryGNSSPlaceRecord		11	11	
├─timeStamp		4	4	{00..00}
├─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

▼B

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket a 2. generációs járművezetői kártya-alkalmazás adatszerkezetének alkalmazni kell:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bájt (28 nap * 93 tevékenységváltás)	13 776 bájt (28 nap * 240 tevékenységváltás)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Műhelykártya-alkalmazások**

4.3.1 *1. generációs műhelykártya-alkalmazás*

TCS_156 Megszemélyesítés után az 1. generációs műhelykártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési feltételekkel rendelkezik:

▼B

		Hozzáférési szabályok		
Fájl	**Fájlazonosító**	**Olvasás**	**Kiválasztás**	**Frissítés**
└─DF Tachograph	‘0500h’		SC1	
├─EF Application_Identification	‘0501h’	SC2	SC1	NEV
├─EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├─EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├─EF Identification	‘0520h’	SC2	SC1	NEV
├─EF Card_Download	‘0509h’	SC2	SC1	**SC1**
├─EF Calibration	‘050Ah’	SC2	SC1	SC3
├─EF Sensor_Installation_Data	‘050Bh’	**SC4**	SC1	NEV
├─EF Events_Data	‘0502h’	SC2	SC1	SC3
├─EF Faults_Data	‘0503h’	SC2	SC1	SC3
├─EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├─EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├─EF Places	‘0506h’	SC2	SC1	SC3
├─EF Current_Usage	‘0507h’	SC2	SC1	SC3
├─EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└─EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

Ebben a táblázatban a biztonsági feltételekkel kapcsolatos következő rövidítések kerülnek alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

SC2 ALW VAGY SM-MAC-G1 VAGY SM-MAC-G2

SC3 SM-MAC-G1 VAGY SM-MAC-G2

SC4 A páros INS bájtot tartalmazó READ BINARY parancs esetében:

(PLAIN-C ÉS SM-R-ENC-G1) VAGY (SM-C-MAC-G1 ÉS SM-R-ENC-MAC-G1) VAGY

(SM-C-MAC-G2 ÉS SM-R-ENC-MAC-G2)

A páratlan INS bájtot tartalmazó READ BINARY parancs esetében (ha támogatott): NEV

TCS_157 Az összes EF szerkezet transzparens.

TCS_158 Az 1. generációs műhelykártya-alkalmazás a következő adatszerkezettel rendelkezik:

▼B

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

▼B

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

▼B

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket a műhelykártya adatszerkezetében egy 1. generációs alkalmazáshoz alkalmazni kell:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bájt (1 nap * 93 tevékenységváltás)	492 bájt (1 nap * 240 tevékenységváltás)

4.3.2 *2. generációs műhelykártya-alkalmazás*

TCS_160 Megszemélyesítés után a 2. generációs műhelykártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési feltételekkel rendelkezik:

Megjegyzés: Az SFID rövid EF azonosító tizedes törtként kerül megadásra, így a 30-as érték megfelelője a kettes számrendszerben: 11110.

			Hozzáférési szabályok		
Fájl	**Fájlazonosító**	**SFID**	**Olvasás**	**Kiválasztás**	**Frissítés**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	‘0501h’	1	SC1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	SC1	NEV
EF CardSignCertificate	‘C101h’	3	SC1	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	SC1	NEV
EF Identification	‘0520h’	6	SC1	SC1	NEV
EF Card_Download	‘0509h’	7	SC1	SC1	SC1
EF Calibration	‘050Ah’	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	‘050Bh’	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	‘0502h’	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	‘0503h’	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	‘0504h’	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	‘0505h’	15	SC1	SC1	SM-MAC-G2
EF Places	‘0506h’	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	‘0507h’	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	‘0508h’	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	‘0522h’	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	‘0523h’	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	‘0524h’	21	SC1	SC1	SM-MAC-G2

▼B

Ebben a táblázatban a biztonsági feltételekkel kapcsolatos következő rövidítések kerülnek alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

SC5 A páros INS bájtot tartalmazó READ BINARY parancs esetében: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

A páratlan INS bájtot tartalmazó READ BINARY parancs esetében (ha támogatott): NEV

TCS_161 Az összes EF szerkezet transzparens.

TCS_162 A 2. generációs műhelykártya-alkalmazás a következő adatszerkezettel rendelkezik:

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
DF Tachograph_G2		*17837*	*4716*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*4284*	
WorkshopCardCalibrationData		*14788*	*4284*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*4284*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

▼B

oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

▼B

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

▼B

TCS_163 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket a műhelykártya adatszerkezetében egy 2. generációs alkalmazáshoz alkalmazni kell:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bájt (1 nap * 93 tevékenységváltás)	492 bájt (1 nap * 240 tevékenységváltás)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Ellenőrzőkártya-alkalmazások

4.4.1 *1. generációs ellenőrzőkártya-alkalmazás*

TCS_164 Megszemélyesítés után az 1. generációs ellenőrzőkártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési feltételekkel rendelkezik:

		Hozzáférési szabályok		
Fájl	**Fájlazonosító**	**Olvasás**	**Kiválasztás**	**Frissítés**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Ebben a táblázatban a biztonsági feltételekkel kapcsolatos következő rövidítések kerülnek alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

SC2 ALW VAGY SM-MAC-G1 VAGY SM-MAC-G2

SC3 SM-MAC-G1 VAGY SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Az összes EF szerkezet transzparens.

TCS_166 Az 1. generációs ellenőrzőkártya-alkalmazás a következő adatszerkezettel rendelkezik:

▼B

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket az ellenőrzőkártya adatszerkezetében egy 1. generációs alkalmazáshoz alkalmazni kell:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *2. generációs ellenőrzőkártya-alkalmazás*

TCS_168 Megszemélyesítés után a 2. generációs ellenőrzőkártya-alkalmazás a következő permanens fájlszerkezettel és fájl-hozzáférési feltételekkel rendelkezik:

Megjegyzés: Az SFID rövid EF azonosító tizedes törtként kerül megadásra, így a 30-as érték megfelelője a kettes számrendszerben: 11110.

▼B

Fájl	Fájlazonosító	SFID	Hozzáférési szabályok	
			Olvasás / Kiválasztás	Frissítés
└DF Tachograph_G2			SC1	
├EF Application_Identification	‘0501h’	1	SC1	NEV
├EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├EF CA_Certificate	‘C108h’	4	SC1	NEV
├EF Link_Certificate	‘C109h’	5	SC1	NEV
├EF Identification	‘0520h’	6	SC1	NEV
└EF Controller_Activity_Data	‘050Ch’	14	SC1	SM-MAC-G2

Ebben a táblázatban a biztonsági feltétellel kapcsolatos következő rövidítés kerül alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

TCS_169 Az összes EF szerkezet transzparens.

TCS_170 A 2. generációs ellenőrzőkártya-alkalmazás a következő adatszerkezettel rendelkezik:

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	
└DF Tachograph_G2		*11410*	*25161*	
├EF Application_Identification		*5*	*5*	
└ControlCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfControlActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
└LinkCertificate		204	341	{00..00}
├EF Identification		*211*	*211*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└ControlCardHolderIdentification		*146*	*146*	
├controlBodyName		36	36	{00, 20..20}
├controlBodyAddress		36	36	{00, 20..20}
├cardHolderName				
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
└EF Controller_Activity_Data		*10582*	*23922*	
└ControlCardControlActivityData		*10582*	*23922*	
├controlPointerNewestRecord		2	2	{00 00}
└controlActivityRecords		*10580*	*23920*	
└controlActivityRecord	n_7	*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlledCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlledVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket az ellenőrzőkártya adatszerkezetében egy 2. generációs alkalmazáshoz alkalmazni kell:

▼B

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. **Vállalkozáskártya-alkalmazások**

4.5.1 *1. generációs vállalkozáskártya-alkalmazás*

TCS_172 Megszemélyesítés után az 1. generációs vállalkozáskártya-alkalmazás a következő permanens fájlszerkezettel és fájl-hozzáférési feltételekkel rendelkezik:

		Hozzáférési szabályok		
Fájl	**Fájlazon-osító**	**Olvasás**	**Kiválasztás**	**Frissítés**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Ebben a táblázatban a biztonsági feltételekkel kapcsolatos következő rövidítések kerülnek alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

SC2 ALW VAGY SM-MAC-G1 VAGY SM-MAC-G2

SC3 SM-MAC-G1 VAGY SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Az összes EF szerkezet transzparens.

TCS_174 Az 1. generációs vállalkozáskártya-alkalmazás a következő adatszerkezettel rendelkezik:

Fájl/adatelem	Rekordok száma	Méret (bájt) Min	Max	Alapértelmezett értékek
└DF Tachograph		*11114*	*2445*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*2392*	
└CompanyActivityData		*10582*	*2392*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*2392*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_175 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket az 1. generációs vállalkozáskártya-alkalmazás adatszerkezetének alkalmazni kell:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *2. generációs vállalkozáskártya-alkalmazás*

TCS_176 Megszemélyesítés után a 2. generációs vállalkozáskártya-alkalmazás a következő permanens fájlszerkezettel és fájlhozzáférési feltételekkel rendelkezik.

Megjegyzés: Az SFID rövid EF azonosító tizedes törtként kerül megadásra, így a 30-as érték megfelelője a kettes számrendszerben: 11110.

			Hozzáférési szabályok	
Fájl	**Fájlazonosító**	**SFID**	**Olvasás / Kiválasztás**	**Frissítés**
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	NEV
├EF Identification	'0520h'	6	SC1	NEV
└EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Ebben a táblázatban a biztonsági feltétellel kapcsolatos következő rövidítés kerül alkalmazásra:

SC1 ALW VAGY SM-MAC-G2

TCS_177 Az összes EF szerkezet transzparens.

TCS_178 A 2. generációs vállalkozáskártya-alkalmazás a következő adatszerkezettel rendelkezik:

Fájl/adatelem	**Rekordok száma**	**Méret (bájt) Min**	**Max**	**Alapértelmezett értékek**
└DF Tachograph_G2		*11338*	*2508*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
└LinkCertificate		204	341	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*2392*	
└CompanyActivityData		*10582*	*2392*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*2392*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_179 A fenti táblázatban a méretek megadására használt következő értékek azok a minimális és maximális rekordszám-értékek, amelyeket a vállalkozáskártya adatszerkezetében egy 2. generációs alkalmazáshoz alkalmazni kell:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

▼B

3. függelék

PIKTOGRAMOK

PIC_001 A menetíró készülék fakultatív módon alkalmazhatja a következő piktogramokat és piktogram-kombinációkat (vagy a hozzájuk nagy mértékben hasonló, egyértelműen azonosítható piktogramokat és piktogram-kombinációkat):

1. EGYSZERŰ PIKTOGRAMOK

	Személyek	**Műveletek**	**Üzemmódok**
	Vállalkozás		Vállalkozási üzemmód
	Ellenőr	Ellenőrzés	Ellenőrzési üzemmód
	Járművezető	Vezetés	Működési üzemmód
	Műhely/vizsgálóállomás	Vizsgálat/kalibrálás	Kalibrálási üzemmód
	Gyártó		

	Tevékenységek	**Időtartam**
	Készenlét	Aktuális készenléti időszak
	Vezetés	Megszakítás nélküli járművezetési idő
	Pihenés	Aktuális pihenési időszak
	Egyéb munka	Aktuális munkaidőszak
	Szünet	Halmozott szünetidő
	Nem ismert	

	Eszközök	**Funkciók**
1	Járművezetői kártyaolvasó egység	
2	Járműkísérői kártyaolvasó egység	
	Kártya	
	Óra	
	Kijelző	Kijelzés
	Külső tároló	Letöltés
	Áramellátás	
	Nyomtató/kinyomat	Nyomtatás
	Érzékelő	
	Abroncsméret	
	Jármű/járműegység	
	GNSS-eszköz	
	Távérzékelő eszköz	
	ITS-interfész	

▼B

Különleges feltételek

OUT	Menetíró készülék nem szükséges
	Kompon/vonaton megtett út

Vegyes

!	Események		Hibák
	Munkanap kezdete		Munkanap vége
	Hely		
M	Járművezetői tevékenységek manuális betáplálása		
	Biztonság		
	Sebesség		
	Idő		
Σ	Összesen/összesítés		

Határozók

24 h	Naponta
I	Hetente
II	Két hét
+	…-tól/től, illetve …-ig

2. PIKTOGRAM-KOMBINÁCIÓK

Vegyes

	Ellenőrzés helye		
	Munkanap kezdetének helye		Munkanap végének helye
+	Kezdés ideje	+	Befejezés ideje
+	Járműből		
OUT +	Menetíró készülék nem szükséges üzemmód kezdete	+ OUT	Menetíró készülék nem szükséges üzemmód vége

Kártyák

	Járművezetői kártya
	Vállalkozáskártya
	Ellenőrzőkártya
	Műhelykártya
– – –	Nincs kártya

Vezetés

	Vezetés személyzettel
I	Egyheti járművezetési idő
II	Kétheti járművezetési idő

▼B

	Kinyomatok
24h	Járművezetői tevékenységek napi kinyomata kártyáról
24h	Járművezetői tevékenységek napi kinyomata VU-ról
	Események és hibák kinyomata kártyáról
	Események és hibák kinyomata járműegységből
	Műszaki adatok kinyomata
	Gyorshajtások kinyomata
	Események
	Érvénytelen kártya behelyezése
	Kártyaütközés
	Időátfedés
	Járművezetés megfelelő kártya nélkül
	Kártya behelyezése járművezetés közben
	Nem megfelelően lezárt utolsó kártyakapcsolat
	Gyorshajtás
	Áramellátás megszakadása
	Mozgásadathiba
	Járműmozgással kapcsolatos ellentmondás
	Biztonsági rendszer megsértése
	Időbeállítás (műhely által)
	Gyorshajtás ellenőrzése
	Hibák
1	Kártyahiba (járművezetői kártyaolvasó egység)
2	Kártyahiba (járműkísérői kártyaolvasó egység)
	Kijelzőhiba
	Letöltési hiba
	Nyomtatóhiba
	Érzékelőhiba
	VU belső hiba
	GNSS hiba
	Távészlelési hiba
	Manuális adatbevitel
?	Még ugyanaz a munkanap?
?	Az előző munkaidő vége?
?	Munkaidő vége helyének megerősítése vagy bevitele
?	Kezdési idő bevitele
?	Munkaidő kezdete helyének bevitele

Megjegyzés: A kinyomatblokkokhoz vagy rekordazonosítókhoz kapcsolódó további piktogram-kombinációkat a 4. függelék határozza meg.

▼B

4. függelék

KINYOMATOK

TARTALOMJEGYZÉK

1. ÁLTALÁNOS ISMERTETÉS

2. AZ ADATBLOKKOK JELLEMZŐI

3. KINYOMATOK JELLEMZŐI

3.1. Járművezetői tevékenységek kártyáról származó napi kinyomata

3.2. Járművezetői tevékenységek VU-ból való napi kinyomata

3.3. Események és hibák kártyáról származó kinyomata

3.4. Események és hibák járműegységből származó kinyomata

3.5. A műszaki adatok kinyomata

3.6. Gyorshajtásra vonatkozó kinyomat

3.7. A behelyezett kártyák története

1. ÁLTALÁNOS ISMERTETÉS

Minden kinyomat különféle adatblokkok láncolatából épül fel, amelyek blokkazonosítóval láthatók el.

Egy adatblokk egy vagy több rekordot tartalmaz, amelyek rekordazonosítóval láthatók el.

PRT_001 Ha a blokkazonosító közvetlenül a rekordazonosító előtt áll, a rekordazonosító nem kerül kinyomtatásra.

PRT_002 Ha egy adattétel nem ismert vagy adatvédelmi jogi okok miatt nem nyomtatható ki, helyettük szóközöket kell kinyomtatni.

PRT_003 Ha egy teljes sor tartalma ismeretlen, vagy azt nem szükséges kinyomtatni, a teljes sort el kell hagyni.

PRT_004 A numerikus adatmezőket jobbra igazítva kell kinyomtatni, az ezresek és a milliók százasainak helyértékét szóköz választja el, és nincsenek kezdő nullák.

PRT_005 A karakterláncokból álló adatmezőket balra igazítva kell kinyomtatni, és azokat szükség szerint az adatelem hosszáig szóközökkel kell feltölteni, vagy adott esetben az adatelem hosszának megfelelően kell levágni (nevek és címek).

PRT_006 A szöveg hosszúságából adódó sortörés esetén az új sor első karaktereként egy speciális karaktert (egy középmagasan elhelyezett pontot: „•”) kell kinyomtatni.

2. AZ ADATBLOKKOK JELLEMZŐI

Ebben a fejezetben a következő hagyományos formátumjelölések kerültek alkalmazásra:

— a **félkövéren** nyomtatott karakterek nyomtatandó egyszerű szöveget jelentenek (a nyomtatás rendes karakterekkel történik),

▼B

— a rendes karakterek olyan változókat jelölnek (piktogramok vagy adatok), amelyek helyett nyomtatásnál az értékeik jelennek meg,

— a változók neveit aláhúzás kíséri, amely a kérdéses változó rendelkezésére álló adatelem hosszát jelzi,

— a dátumok „nn/hh/éééé” (nap, hónap, év) formátumúak, de a „nn.hh.éééé” formátum is használható,

— a „kártya azonosítása” a következő elemekből áll: a kártyatípus jelölése a megfelelő piktogram-kombinációval, a kártyát kiállító tagállam kódja, ferde törtvonal, amelyet a kártyaszám követ, majd egy szóközzel elválasztott csereindex és megújítási index következik:

P	▪	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Piktogram-kombináció		Kiállító tagállam kódja				A kártyaszám első 14 jegye (adott esetben konszekutív indexet foglal magában)														Csereindex		Megújítási index

▼B

PRT_007 A kinyomatok a következő adatblokkokból és/vagy adattételekből állnak, összhangban a következő jelentésekkel és formátumokkal:

Blokk vagy rekordszám Jelentés	Adatformátum
1 ***A dokumentum nyomtatásának dátuma és időpontja***	▼ nn/hh/éééé óó:pp **(UTC)**
2 ***Kinyomat típusa*** Blokkazonosító Kinyomat piktogram-kombinációja (ld. 3. függelék), sebességkorlátozó készülék beállítása (csak gyorshajtásra vonatkozó kinyomat esetén)	----------▼---------- Piktogram xxx **km/h**
3 ***Kártyatulajdonos azonosítása*** Blokkazonosító P = személyi piktogram Kártyatulajdonos családi neve Kártyatulajdonos utóneve(i) (adott esetben) A kártya azonosítása A kártya lejárati dátuma (ha van) és a kártyageneráció száma (GEN 1 vagy GEN 2) (*)	----------P---------- P Családi_Név_____ Utónév_____ Kártya_azonosítása_____ nn/hh/éééé - GEN 2

Ha nem személyhez kötött kártyáról van szó, és az nem tartalmazza a tulajdonos családi nevét, akkor helyette a vállalkozás vagy a műhely vagy az érintett ellenőrző szerv nevét kell kinyomtatni.

(*) A kártyageneráció száma csak intelligens menetíró készülékkel nyomtatható ki.

4 ***A jármű azonosítása*** Blokkazonosító VIN Nyilvántartásba vétel szerinti tagállam és rendszám	----------🚙---------- 🚙 VIN_____ Ország/Rendszám_____
5 ***A VU azonosítása*** Blokkazonosító A VU gyártójának neve A VU alkatrészszáma Járműegység-generáció száma (*)	----------⊟---------- ⊟ Járműegység_gyártója_____ VU_Part_Number GEN 2

(*) A kártyageneráció száma csak intelligens menetíró készülékkel nyomtatható ki.

6 ***A menetíró készülék legutóbbi kalibrálása*** Blokkazonosító A műhely neve A műhelykártya azonosítása A kalibrálás dátuma	----------🔧---------- 🔧 Műhely_neve_____ Kártya_azonosítása_____ 🔧 nn/hh/éééé

▼B

7 ***Legutóbbi ellenőrzés (ellenőr által)***

Blokkazonosító

Ellenőrkártya azonosítása

Az ellenőrzés dátuma, ideje és típusa

```
----------▫----------
Kártya_azonosítása_____
▫ nn/hh/éééé óó:pp ppppp
```

Az ellenőrzés típusa: maximum öt piktogram. Az ellenőrzés típusai a következők (vagy ezek kombinációi) lehetnek:
▪: Kártyaletöltés, ↧: Járműegység-letöltés, ▼: Nyomtatás, □: Kijelzés, ↑: Közúti kalibrálás-ellenőrzés

8 ***A kártyán az előfordulásuk időrendjében tárolt járművezetői tevékenységek***

Blokkazonosító

Leolvasás dátuma (az a naptári nap, amelyre a kinyomat vonatkozik) + napi kártyajelenlét-számláló

```
----------◙----------
    nn/hh/éééé  xxx
```

8a. *E nap kezdetén menetíró készülék nem szükséges* (ha nincs bekapcsolva ez az üzemmód, üresen kell hagyni)

```
----------OUT----------
```

8.1 *Az az időszak, amelyben a kártya nem volt behelyezve*

8.1a. Rekordazonosító (időszak kezdete)

8.1b. *Ismeretlen időszak* Kezdet, időtartam

8.1c. Manuálisan bevitt tevékenység.

Tevékenység piktogram, kezdet, időtartam

```
  --------------------
?       óó:pp óóhpp***
A       óó:pp óóhpp
```

8.2 *Kártyabehelyezés az S kártyaolvasó egységbe*

Rekordazonosító; S = kártyaolvasó egység piktogram

A járművet nyilvántartásba vevő tagállam és a jármű rendszáma

Jármű kilométer-számlálójának állása a kártya behelyezésekor

```
  ---------S---------
▲ Ország/rendszám_____
  x xxx xxx km
```

8.3 *Tevékenység (behelyezett kártyánál)*

Tevékenység piktogram, kezdet, időtartam, személyzeti státusz (személyzet-piktogram, ha SZEMÉLYZET, üres hely, ha EGYEDÜL).

```
A       óó:pp óóhpp ◙◙
```

8.3a. *Különleges körülmény*. Bevitel ideje, különleges körülmény piktogram (vagy piktogram-kombináció).

```
        óó:pp ---pppp---
```

8.4 *Kártyakivétel*

A kilométer-számláló állásának változása és a jármű által megtett távolság azon utolsó kártyába helyezés óta, amelyre vonatkozóan ismert a kilométer-számláló állása

```
  x xxx xxx km; x xxx km
```

9 ***Kártyaolvasó egységenként a VU-ban tárolt járművezetői tevékenységek időrendben***

Blokkazonosító

Leolvasás dátuma (az a naptári nap, amelyre a kinyomat vonatkozik)

Jármű kilométer-számlálójának állása 00:00 és 24:00 órakor

```
----------◙----------
       nn/hh/éééé
x xxx xxx - x xxx xxx km
```

10 ***Az S kártyaolvasó egységben végzett tevékenységek***

Blokkazonosító

```
----------S----------
```

10a *E nap kezdetén menetíró készülék nem szükséges* (ha nincs bekapcsolva ez az üzemmód, üresen kell hagyni)

```
----------OUT----------
```

10.1 *Az az időszak, amelyben az S kártyaolvasó egységbe nincs behelyezve kártya*

Rekordazonosító.

Nincs behelyezve kártya

Jármű kilométer-számlálójának állása az időszak kezdetén

```
  --------------------
◙▪---
  x xxx xxx km
```

10.2 *Kártyabehelyezés*

Kártyabehelyezés rekordazonosító

A járművezető neve

```
  --------------------
◙ Családi_név_____________
```

▼B

	A járművezető utóneve A járművezetői kártya azonosítása A kártya lejárati dátuma (ha van) és a kártyageneráció száma (GEN 1 vagy GEN 2) (*) Az előző járművet bejegyező tagállam és a jármű rendszáma Az előző járműből történő kártyakivétel dátuma és időpontja Üres sor A jármű kilométer-számlálójának állása a kártya behelyezésekor, a járművezetői tevékenységek jelzésének manuális bevitele (M, ha igen, üres, ha nem). Amennyiben a járművezetői kártya behelyezésére nem került sor azon a napon, amelyre vonatkozóan kinyomtatás történt, akkor a 10.2. blokk esetében a kilométer-számlálónak az előző napi legutolsó hozzáférhető kártyabehelyezésből származó állását kell felhas	Utónév_____ Kártya_azonosítása_____ nn/hh/éééé - GEN 2 Ország/Rendszám_____ nn/hh/éééé óó:pp x xxx xxx **km** M
10.3	*Tevékenység* Tevékenység piktogram, kezdet, időtartam, személyzeti státusz (személyzet-piktogram, ha SZEMÉLYZET, üres hely, ha EGYEDÜL).	A óó:pp óó**h**pp
10.3a	*Különleges körülmény*. Bevitel ideje, különleges körülmény piktogram (vagy piktogram-kombináció).	óó:pp ---pppp---
10.4	*Kártyakivétel vagy „kártyamentes" időszak vége* A jármű kilométer-számlálójának állása a kártya kivételekor vagy a „kártyamentes" időszak végén, valamint a behelyezéstől vagy a „kártyamentes" időszak kezdetétől megtett távolság.	x xxx xxx **km**; x xxx **km**

(*) A kártyageneráció száma csak intelligens menetíró készülékkel nyomtatható ki.

11	***Napi összegzés*** Blokkazonosító	----------Σ----------
11.1	***A járművezetői kártyaolvasó egység kártya nélküli időszakainak VU összegzése*** Blokkazonosító	1----
11.2	***A járműkísérői kártyaolvasó egység kártya nélküli időszakainak VU összegzése*** Blokkazonosító	2----
11.3	***VU napi összegzése járművezetőnként*** Rekordazonosító A járművezető családi neve A járművezető utóneve(i) A járművezetői kártya azonosítása	---------- Családi_név_____ Utónév_____ Kártya_azonosítása_____
11.4	*Azon hely bevitele, ahol a munkanap kezdődik és/vagy végződik* pi = hely kezdet/befejezés piktogram, idő, ország, régió, Kilométer-számláló	pióó:pp Ország Régió x xxx xxx **km**
11.5	*Azon hely bevitele, ahol a munkanap kezdődik és/vagy végződik* valamint 3 óra megszakítás nélküli járművezetési időt követően Kilométer-számláló	óó:pp x xxx xxx **km**
11.6	*Tevékenységek összértéke (kártyáról)* Teljes járművezetési időtartam, megtett távolság Teljes munkaidő és készenléti idő Teljes pihenési és ismeretlen idő Személyzeti tevékenységek teljes időtartama	óó**h**pp x xxx **km** óó**h**pp óó**h**pp óó**h**pp ? óó**h**pp óó**h**pp
11.7	*Tevékenységek összértéke (járművezetői kártyaolvasó egység nélküli időszakok)* Teljes járművezetési időtartam, megtett távolság Teljes munkaidő és készenléti idő Teljes pihenési idő	óó**h**pp x xxx **km** óó**h**pp óó**h**pp óó**h**pp

▼B

11.8	*Tevékenységek összértéke (járműkísérői kártyaolvasó egység nélküli időszakok)*	
	Teljes munkaidő és készenléti idő	* óóhpp ⧈ óóhpp
	Teljes pihenési idő	⊢ óóhpp
11.9	*Tevékenységek összértéke (járművezetőnként, mindkét kártyaolvasó egységet beleértve)*	
	Teljes járművezetési időtartam, megtett távolság	⊙ óóhpp x xxx km
	Teljes munkaidő és készenléti idő	* óóhpp ⧈ óóhpp
	Teljes pihenési idő	⊢ óóhpp
	Személyzeti tevékenységek teljes időtartama	⊙⊙ óóhpp

Ha az adott napra nézve napi kinyomat szükséges, a kinyomtatás időpontjában rendelkezésre álló adatokból kell kiszámítani a napi összegzés adatait.

12	***A kártyán tárolt események és/vagy hibák***	
12.1	Az utolsó 5 „esemény és hiba” blokkazonosítója a kártyáról	----------!×▪----------
12.2	Minden rögzített „esemény” blokkazonosítója a kártyán	----------!▪----------
12.3	Minden rögzített „hiba” blokkazonosítója a kártyán	----------×▪----------
12.4	*Esemény- és/vagy hibarekord*	
	Rekordazonosító Esemény/hiba piktogram, a rekord célja, a kezdés dátuma/időpontja, További esemény/hibakód (ha szükséges), időtartam Az esemény vagy hiba által érintett járművet nyilvántartásba vevő tagállam és a jármű rendszáma	---------- Piktogram (p) nn/hh/éééé óó:pp !xx óóhpp ▟ Ország/Rendszám_____

13	***A VU-ban tárolt vagy folyamatban lévő események és/vagy hibák***	
13.1	Az utolsó 5 „esemény és hiba” blokkazonosítója a VU-ról	----------!×▟----------
13,2	Minden rögzített vagy folyamatban lévő „esemény” blokkazonosítója a VU-ban	----------!▟----------
13.3	Minden rögzített vagy folyamatban lévő „hiba” blokkazonosítója a VU-ban	----------×▟----------
13.4	*Esemény- és/vagy hibarekord*	
	Rekordazonosító Esemény/hiba piktogram, a rekord célja, a kezdés dátuma/időpontja, További esemény/hibakód (ha szükséges), az adott napon történt hasonló események száma, időtartam Az esemény vagy hiba kezdetén vagy végén behelyezett kártyák azonosítása (maximum 4 sor az azonos kártyaszámok ismétlése nélkül) Olyan eset, amikor nem helyeztek be kártyát Gyártóra jellemző adatok	---------- Piktogram (p) nn/hh/éééé óó:pp !xx (xxx) óóhpp Kártya_azonosítása_____ Kártya_azonosítása_____ Kártya_azonosítása_____ Kártya_azonosítása_____ ▪--- < Literal><ErrorCode>

A rekord célja (p) olyan numerikus kód megadása, amely megmagyarázza, hogy miért került az esemény vagy hiba rögzítésre, a kódolás az `EventFaultRecordPurpose` adatelemmel összhangban történik.

A `Literal` a menetírókészülék-gyártóra jellemző, maximum 12 karakter hosszúságú betűkód.

Az `ErrorCode` a menetírókészülék-gyártóra jellemző, maximum 12 karakter hosszúságú hibakód.

▼B

14	***A VU azonosítása***	
	Blokkazonosító	`----------B----------`
	A VU gyártójának neve	`B Név_____`
	A VU gyártójának címe	`Cím_____`
	A VU alkatrészszáma	`Alkatrészszám_____`
	A VU jóváhagyási száma	`Jóváhagyás_____`
	A VU sorozatszáma	`S/N_____`
	A VU gyártási éve	`éééé`
	A VU szoftververziója és az installálás dátuma	`V xxxx nn/hh/éééé`
15	***Az érzékelő azonosítása***	
	Blokkazonosító	`----------Л----------`
15.1	*Párosítási rekord*	
	Az érzékelő sorozatszáma	`Л S/N_____`
	Az érzékelő jóváhagyási száma	`Jóváhagyás_____`
	Az érzékelőpárosítás dátuma	`nn/hh/éééé óó:pp`
16	***A GNSS azonosítása***	
	Blokkazonosító	`----------▚----------`
16.1	*Összekapcsolási rekord*	
	A külső GNSS-eszköz sorozatszáma	`▚ S/N_____`
	A külső GNSS-eszköz jóváhagyási száma	`Jóváhagyás_____`
	A külső GNSS-eszköz összekapcsolási dátuma	`nn/hh/éééé óó:pp`
17	***A kalibrálás adatai***	
	Blokkazonosító	`----------T----------`
17.1	*Kalibrálási rekord*	
	Rekordazonosító	`----------`
	A kalibrálást végző műhely	`T Műhely_neve_____`
	A műhely címe	`Műhely_címe_____`
	A műhelykártya azonosítása	`Kártya_azonosítása_____`
	A műhelykártya lejárati dátuma	`nn/hh/éééé`
	Üres sor	
	Kalibrálás dátuma + kalibrálás célja	`T nn/hh/éééé (p)`
	VIN	`A VIN_____`
	Nyilvántartásba vétel szerinti tagállam és rendszám	`Ország/Rendszám_____`
	A jármű jellemző együtthatója	`w xx xxx Imp/km`
	Az adatrögzítő készülék állandója	`k xx xxx Imp/km`
	Effective circumference of wheel tyres	`l xx xxx mm`
	A felszerelt abroncsok mérete	`● Abroncsméret_____`
	A sebességkorlátozó készülék beállítása	`› xxx km/h`
	Régi és új kilométer-számláló értékek	`x xxx xxx – x xxx xxx km`

A kalibrálás célja (p) olyan numerikus kód megadása, amely megmagyarázza, hogy miért e kalibrálási paraméterek kerültek rögzítésre; a kódolás a `CalibrationPurpose` adatelemmel összhangban történik.

▼B

18	***Időbeállítás***	
	Blokkazonosító	`----------◷----------`
18.1	*Időbeállítási rekord*	
	Rekordazonosító	`--------------------`
	Régi dátum és idő	`!◷ nn/hh/éééé óó:pp`
	Új dátum és idő	`◷ nn/hh/éééé óó:pp`
	Az időbeállítást végző műhely	`⍑ Műhely_neve_____`
	A műhely címe	`Műhely_címe_____`
	A műhelykártya azonosítása	`Kártya_azonosítása_____`
	A műhelykártya lejárati dátuma	`nn/hh/éééé`
19	***A VU-ban rögzített legutóbbi esemény és hiba***	
	Blokkazonosító	`----------!×д----------`
	Legutóbbi esemény dátuma és időpontja	`! nn/hh/éééé óó:pp`
	Legutóbbi hiba dátuma és időpontja	`× nn/hh/éééé óó:pp`
20	***Gyorshajtás ellenőrzésére vonatkozó információ***	
	Blokkazonosító	`----------››----------`
	A legutolsó GYORSHAJTÁS-ELLENŐRZÉS dátuma és időpontja	`›▫nn/hh/éééé óó:pp`
	Az első gyorshajtás dátuma és időpontja, és az azóta bekövetkezett gyorshajtások száma	`››nn/hh/éééé óó:pp (nnn)`
21	***Gyorshajtási rekord***	
21.1	Blokkazonosító „Első gyorshajtás az utolsó kalibrálás után”	`--------››⍑---------`
21.2	Blokkazonosító „Az 5 legsúlyosabb gyorshajtás a legutóbbi 365 napban”	`-------››(365)------`
21.3	Blokkazonosító „A legsúlyosabb gyorshajtás külön-külön az előfordulás utolsó 10 napján”	`-------››(10)-------`
21.4	Rekordazonosító	`--------------------`
	Dátum, időpont és időtartam	`››nn/hh/éééé óó:pp óóhpp`
	Maximális és átlagos sebesség, e napon történt hasonló események száma	`xxx km/h xxx km/h(xxx)`
	A járművezető családi neve	`◙ Családi_név_____`
	A járművezető utóneve(i)	`Utónév_____`
	A járművezetői kártya azonosítása	`Kártya_azonosítása_____`
21.5	Ha a blokkban nem szerepel gyorshajtási rekord	`››---`
22	***Kézzel bevitt adatok***	
	Blokkazonosító	`------------------------`
22.1	Ellenőrzés helye	`▫• ..................`
22.2	Az ellenőr aláírása	`▫ ..................`
22.3	Kezdet	`◷+ ..................`
22.4	Befejezés	`+◷ ..................`
22.5	Járművezető aláírása	`◙ ..................`

„Kézzel bevitt adatok” Elegendő számú üres sort kell beszúrni a kézzel írott tételek fölé ahhoz, hogy elegendő hely legyen a szükséges adatok vagy egy aláírás számára.

▼B

23 ***A VU-ba legutóbb behelyezett kártyák***
Blokkazonosító
23.1 Behelyezett kártya
Rekordazonosító
A kártya típusa, generációja, verziója, gyártója (*)
A kártya azonosítása
A kártya sorozatszáma
A kártya behelyezésének dátuma és időpontja

```
-------- ⊟◪◔ --------

----
⍑ <gen> <version> <MC>
A kártya azonosítása
A kártya sorozatszáma
nn/hh/éééé óó:pp
```

(*) (mindent egy sorba)
a következőképpen:
kártya típusa: piktogram, 1 karakter + szóköz
gen: GEN1 vagy GEN2, 4 karakter + szóköz
version: legfeljebb 10 karakter
MC: a gyártó kódja, 3 karakter

3. KINYOMATOK JELLEMZŐI

E fejezetben a következő jelölési konvenciók használatosak:

N	Nyomtatási blokk vagy rekord N száma
N	Nyomtatási blokk vagy rekord N száma annyiszor megismételve, ahányszor szükséges
X/Y	X és/vagy Y nyomtatási blokkok vagy tételek szükség szerint, és annyiszor megismételve, ahányszor szükséges

3.1. **Járművezetői tevékenységek kártyáról származó napi kinyomata**

PRT_008 A járművezetői tevékenységek kártyáról származó napi kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Az ellenőr azonosítása (ha az ellenőrző kártya a VU-ba van helyezve)
3	A járművezető azonosítása (arról a kártyáról, amelyre a kinyomat vonatkozik + GEN)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
5	VU azonosítása (VU, amelyből a kinyomat vétele történik + GEN)
6	A szóban forgó VU utolsó kalibrálása
7	Az ellenőrzött járművezető utolsó ellenőrzése
8	A járművezetői tevékenység határolójele
8a	E nap kezdetén menetíró készülék nem szükséges
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	A járművezető tevékenységei az előfordulásuk sorrendjében
11	Napi összegzés határolójele

▼B

11.4	Betáplált helyek időrendben
11.5	GNSS adatok
11.6	Tevékenységek összértéke
12.1	A kártyáról kivont események vagy hibák határolójele
12.4	Esemény/hiba rekordok (a kártyán tárolt utolsó 5 esemény vagy hiba)
13.1	A VU-ról kivont események vagy hibák határolójele
13.4	Esemény/hiba rekordok (a VU-n tárolt vagy folyamatban lévő utolsó 5 esemény vagy hiba)
22.1	Ellenőrzés helye
22.2	Az ellenőr aláírása
22.5	A járművezető aláírása

3.2. **Járművezetői tevékenységek VU-ból való napi kinyomata**

PRT_009 A járművezetői tevékenységek VU-ból származó napi kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Kártyatulajdonos azonosítása (a VU-ba helyezett minden kártya esetében + GEN)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
5	VU azonosítása (VU, amelyből a kinyomat vétele történik + GEN)
6	A szóban forgó VU utolsó kalibrálása
7	Az e menetíró készüléken végzett utolsó elenőrzés
9	A járművezetői tevékenység határolójele
10	Járművezetői kártyaolvasó egység határolójele (1 kártyaolvasó egység)
10a	E nap kezdetén menetíró készülék nem szükséges
10.1 / 10.2 / 10.3 /10.3a / 10.4	Tevékenységek időrendben (járművezetői kártyaolvasó egység)
10	Járműkísérői kártyaolvasó egység határolójele (2 kártyaolvasó egység)
10a	E nap kezdetén menetíró készülék nem szükséges
10.1 / 10.2 / 10.3 /10.3a / 10.4	Tevékenységek időrendben (járműkísérői kártyaolvasó egység)
11	Napi összegzés határolójele
11.1	A járművezetői kártyaolvasó egység kártya nélküli időszakainak összegzése
11.4	Betáplált helyek időrendben
11.5	GNSS adatok

▼B

11.6	Tevékenységek összértéke
11.2	A járműkísérői kártyaolvasó egység kártya nélküli időszakainak összegzése
11.4	Betáplált helyek időrendben
11.5	GNSS adatok
11.7	Tevékenységek összértéke
11.3	Tevékenységek összegzése egy járművezetőre nézve, mindkét kártyaolvasó egységet beleértve
11.4	Az adott járművezető által időrendben betáplált helyek
11.5	GNSS adatok
11.8	Tevékenységek összértéke az adott járművezetőre nézve
13.1	Esemény/hiba határolójele
12.4	Esemény/hiba rekordok (a VU-n tárolt vagy folyamatban lévő utolsó 5 esemény vagy hiba)
13.1	Ellenőrzés helye
22.2	Az ellenőr aláírása
22.3	Kezdet (hely, ahol a járművezető kártya nélkül megadhatja a számára releváns időtartamokat)
22.4	Befejezés
22.5	A járművezető aláírása

3.3. **Események és hibák kártyáról származó kinyomata**

PRT_010 Az események és hibák kártyáról származó kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Az ellenőr azonosítása (ha az ellenőrző kártya a VU-ba van helyezve + GEN)
3	A járművezető azonosítása (arról a kártyáról, amelyre a kinyomat vonatkozik)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
12.2	Esemény határolójele
12.4	Eseményrekordok (a kártyán tárolt minden esemény)
12.3	Hiba határolójele
12.4	Hibarekordok (a kártyán tárolt minden hiba)
22.1	Ellenőrzés helye
22.2	Az ellenőr aláírása
22.5	A járművezető aláírása

▼B

3.4. **Események és hibák járműegységből származó kinyomata**

PRT_011 Az események és hibák járműegységből származó kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Kártyatulajdonos azonosítása (a VU-ba helyezett minden kártya esetében + GEN)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
13.2	Esemény határolójele
13.4	Eseményrekordok (a VU-ban tárolt vagy folyamatban lévő összes esemény)
13.3	Hiba határolójele
13.4	Hibarekordok (a VU-ban tárolt vagy folyamatban lévő összes hiba)
22.1	Ellenőrzés helye
22.2	Az ellenőr aláírása
22.5	A járművezető aláírása

3.5. **A műszaki adatok kinyomata**

PRT_012 A műszaki adatok kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Kártyatulajdonos azonosítása (a VU-ba helyezett minden kártya esetében + GEN)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
14	A VU azonosítása
15	Az érzékelő azonosítása
15.1	Érzékelőpárosításra vonatkozó adatok (valamennyi elérhető adat időrendben)
16	A GNSS azonosítása
16.1	A külső GNSS-eszköz párosítására vonatkozó adatok (valamennyi elérhető adat időrendben)
17	Kalibrálási adatok határolójele
17.1	Kalibrálási rekordok (az összes rendelkezésre álló rekord időrendben)
18	Időbeállítás határolójele
18.1	Időbeállítási rekordok (az időbeállítási és a kalibrálási adatrekordokból rendelkezésre álló összes rekord)
19	A VU-ban rögzített legutóbbi esemény és hiba

▼B

3.6. **Gyorshajtásra vonatkozó kinyomat**

PRT_013 A gyorshajtásra vonatkozó kinyomatnak összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	Kártyatulajdonos azonosítása (a VU-ba helyezett minden kártya esetében + GEN)
4	A jármű azonosítása (az a jármű, amelyből a kinyomat származik)
20	Gyorshajtás ellenőrzésére vonatkozó információ
21.1	Gyorshajtási adatok azonosítója
21.4 / 21.5	Első gyorshajtás az utolsó kalibrálás után
21.2	Gyorshajtási adatok azonosítója
21.4 / 21.5	Az 5 legsúlyosabb gyorshajtási esemény a legutóbbi 365 napban
21.3	Gyorshajtási adatok azonosítója
21.4 / 21.5	A legsúlyosabb gyorshajtás külön-külön az előfordulás utolsó 10 napján
22.1	Ellenőrzés helye
22.2	Az ellenőr aláírása
22.5	A járművezető aláírása

3.7. **A behelyezett kártyák története**

PRT_014 A műszaki adatok kinyomatának összhangban kell lennie a következő formátummal:

1	A dokumentum nyomtatásának dátuma és időpontja
2	A kinyomat típusa
3	A kártyatulajdonos azonosítása (a VU-ba helyezett minden kártya esetében)
23	A VU-ba legutóbb behelyezett kártya
23.1	Behelyezett kártyák (legfeljebb 88 rekord)
12.3	Hiba határolójele

▼B

5. függelék

KIJELZÉS

E függelékben a következő hagyományos jelölések kerültek alkalmazásra:

— a **félkövéren** szedett karakterek a megjelenítendő egyszerű szöveget jelölik (a kijelző normál karaktereket mutat),

— a normál karakterek olyan változókat jelölnek (piktogramok vagy adatok), amelyek helyett kijelzéskor az értékeik jelennek meg:

  — nn hh éééé: nap, hónap, év,

  — óó: óra,

  — pp: perc,

  — D: időtartam-piktogram,

  — EF: eseményt vagy hibát jelölő piktogram-kombináció,

  — O: üzemmódot jelölő piktogram.

DIS_001 A menetíró készülék az adatokat a következő formátumban jeleníti meg:

Adatok	Formátum
Alapértelmezett adatok kijelzése	
Helyi idő	óó:pp
Üzemmód	O
Járművezetőre vonatkozó információ	1Dóóhpp IIóóhpp
Járműkísérőre vonatkozó információ	2Dóóhpp
„Menetíró készülék nem szükséges” üzemmód bekapcsolva	OUT
Figyelmeztető kijelzés	
Megszakítás nélküli járművezetési idő túllépése	1⊙óóhpp IIóóhpp
Esemény vagy hiba	EF
Egyéb kijelzések	
UTC dátum idő	UTC⊙nn/hh/éééé vagy UTC⊙nn.hh.éééé óó:pp
Járművezető megszakítás nélküli járművezetési ideje és halmozott pihenőideje	1⊙óóhpp IIóóhpp
Járműkísérő megszakítás nélküli járművezetési ideje és halmozott pihenőideje	2⊙óóhpp IIóóhpp
Járművezető halmozott járművezetési ideje az előző és a folyó héten	1⊙II óóóhpp
Járműkísérő halmozott járművezetési ideje az előző és a folyó héten	2⊙II óóóhpp

▼B

6. függelék

ELŐLAPI KALIBRÁLÁSI ÉS LETÖLTŐ CSATLAKOZÓ

TARTALOMJEGYZÉK

1. HARDVER

1.1. Csatlakozó

1.2. Érintkezőkiosztás

1.3. Blokkdiagram

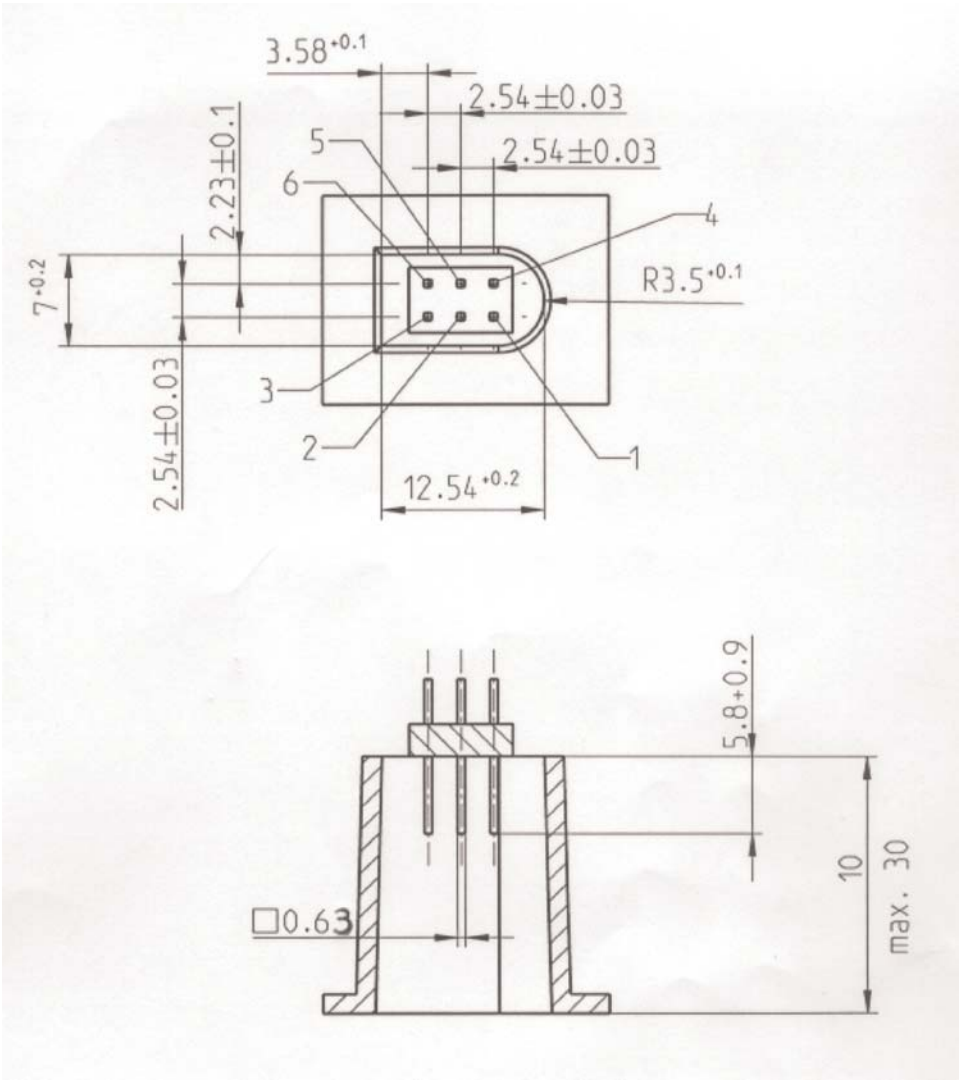
2. LETÖLTŐ INTERFACE

3. KALIBRÁLÁSI INTERFACE

1. HARDVER

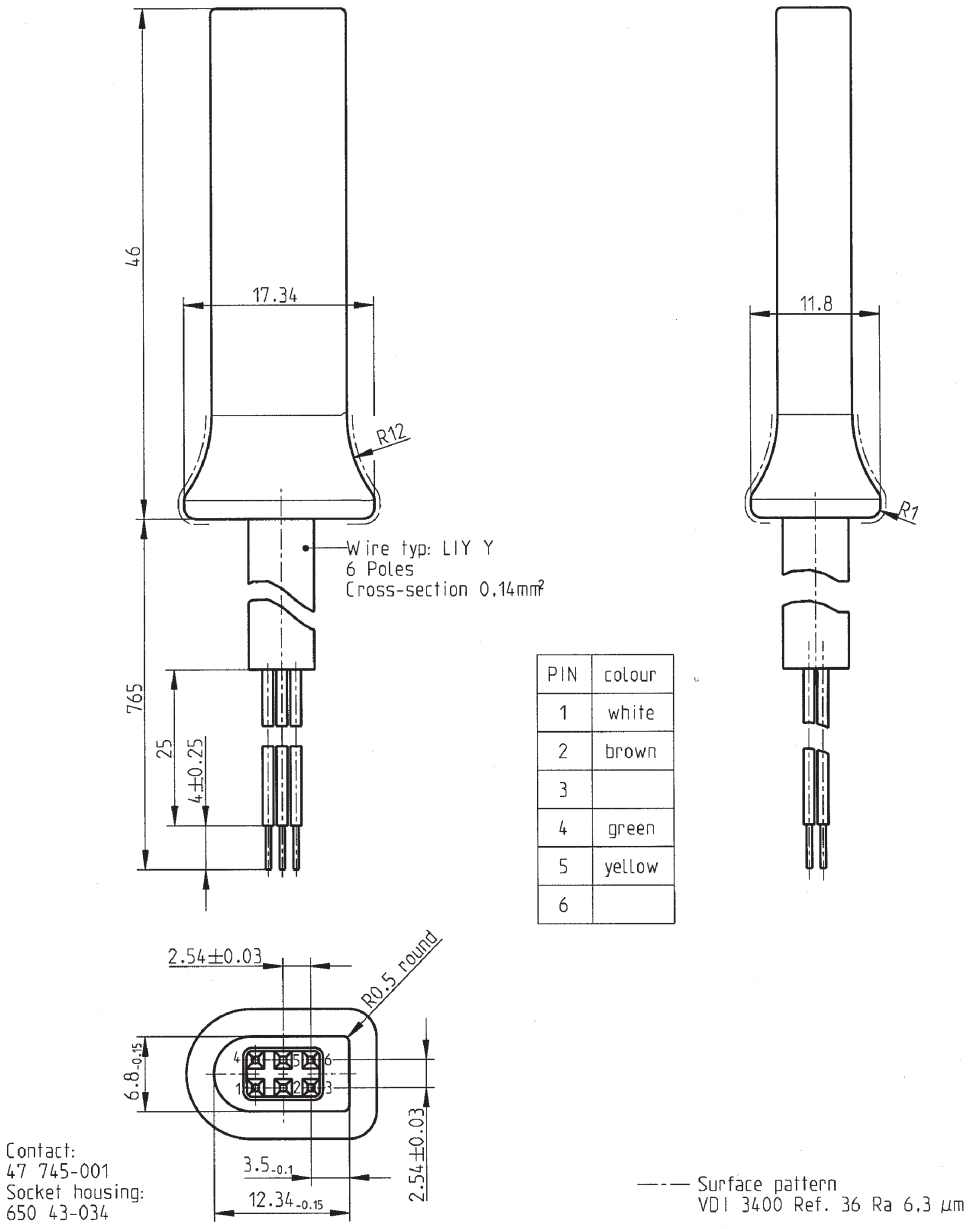
1.1. **Csatlakozó**

INT_001 A letöltő/kalibrálási csatlakozó egy 6-pólusú csatlakozó, amely az előlap felől hozzáférhető anélkül, hogy a menetíró készülék valamely elemét szét kellene kapcsolni, és annak meg kell felelnie a következő vázlatnak (minden méret milliméterben értendő):



▼B

A következő ábra egy tipikus 6-pólusú csatlakozót ábrázol:



1.2. **Érintkezőkiosztás**

INT_002 Az érintkezők a következő táblázattal összhangban kerülnek kiosztásra:

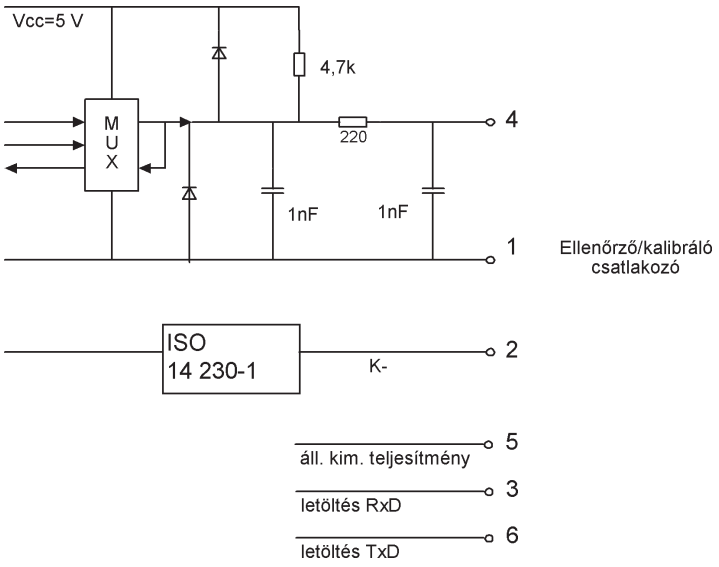
Érintkező	Leírás	Megjegyzés
1	Az akkumulátor negatív pólusa	A jármű akkumulátorának negatív pólusához kapcsolva
2	Adatkommunikáció	K-vonal (ISO 14230-1)
3	RxD – letöltés	Adatbevitel a menetíró készülékbe
4	Bemenő/kimenő jel	Kalibrálás

▼B

Érintkező	Leírás	Megjegyzés
5	Állandó kimeneti teljesítmény	A feszültségtartományt úgy kell meghatározni, hogy 3 V-tal kevesebb legyen a járműben lévő áramra jellemző feszültségtartománynál, ami lehetővé teszi a védelmi áramkör feszültségesését Kimenő áramerősség: 40 mA
6	RxD – letöltés	Adatkivétel a menetíró készülékből

1.3. **Blokkdiagram**

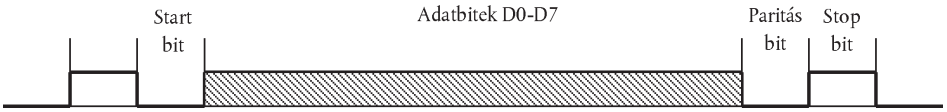
INT_003 A blokkdiagram megfelel az alábbi ábrának:



2. LETÖLTŐ INTERFÉSZ

INT_004 A letöltő interfész megfelel az RS232 előírásoknak.

INT_005 A letöltő interfész egy start bitet, 8 adatbitet (ahol az első helyen a legalacsonyabb értékű bit áll), egy páros paritás bitet és 1 stop bitet használ.



Adatbájt felépítése

Start bit: egy bit az 0 logikai szinten

Adatbitek: a legalacsonyabb értékű bit átvitele első helyen

Paritás bit: páros paritás

Stop bit: egy bit az 1. logikai szinten

Ha egynél több bájtot tartalmazó numerikus adatok kerülnek átvitelre, a rendszer a legmagasabb helyi értékű bájtot viszi át először és a legkisebb helyi értékű bájtot utoljára.

INT_006 Az átviteli sebesség 9 600 bps-től 115 200 bps-ig állítható. Az átvitel a lehető legnagyobb átviteli sebességgel történik, a kezdeti átviteli bitsebesség a kommunikáció kezdetétől számítva 9 600 bps.

▼B

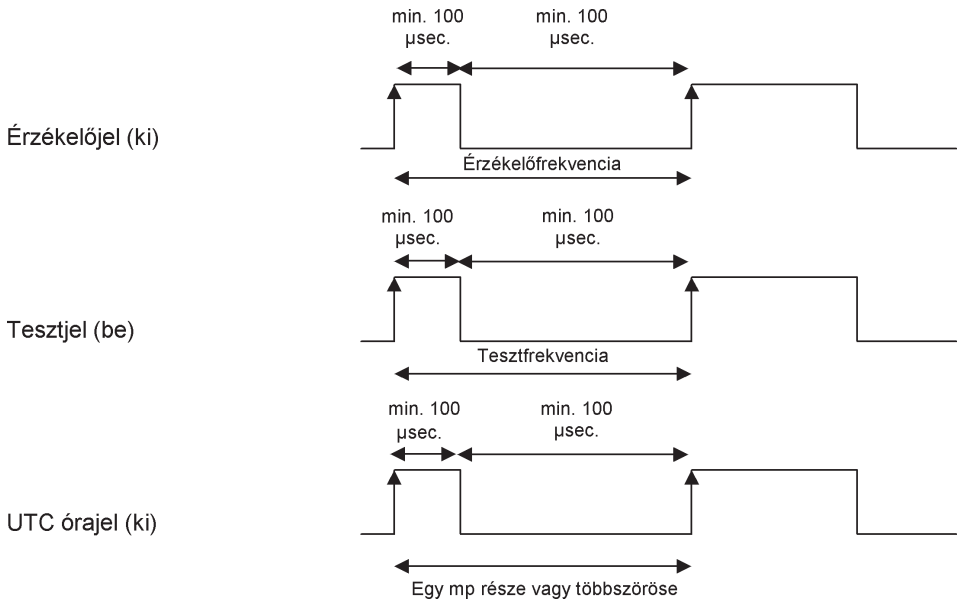
3. KALIBRÁLÁSI INTERFÉSZ

INT_007 Az adatkommunikáció megfelel a következő szabványnak: ISO 14230-1 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer, First edition: 1999.

INT_008 A bemenő/kimenő jel megfelel a következő elektromos jellemzőknek:

Paraméter	Minimum	Tipikus	Maximum	Megjegyzés
$U_{alacsony}$ (be)			1,0 V	I = 750 μA
U_{magas} (be)	4 V			I = 200 μA
Frekvencia			4 kHz	
$U_{alacsony}$ (ki)			1,0 V	I = 1 mA
U_{magas} (ki)	4 V			I = 1 mA

INT_009 A bemenő/kimenő jel megfelel a következő szinkronozási diagramoknak:



▼B

7. függelék

ADATLETÖLTÉSI PROTOKOLLOK

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. Alkalmazási kör

1.2. Betűszavak, jelmagyarázat

2. ADATOK LETÖLTÉSE A JÁRMŰEGYSÉGRŐL

2.1. Letöltési eljárás

2.2. Adatletöltési protokoll

2.2.1 Az üzenetek struktúrája

2.2.2 Az üzenetek típusai

2.2.2.1 Start Communication Request (SID 81)

2.2.2.2 Positive Response Start Communication (SID C1)

2.2.2.3 Start Diagnostic Session Request (SID 10)

2.2.2.4 Positive Response Start Diagnostic (SID 50)

2.2.2.5 Link Control Service (SID 87)

2.2.2.6 Link Control Positive Response (SID C7)

2.2.2.7 Request Upload (SID 35)

2.2.2.8 Positive Response Request Upload (SID 75)

2.2.2.9 Transfer Data Request (SID 36)

2.2.2.10 Positive Response Transfer Data (SID 76)

2.2.2.11 Request Transfer Exit (SID 37)

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

2.2.2.13 Stop Communication Request (SID 82)

2.2.2.14 Positive Response Stop Communication (SID C2)

2.2.2.15 Acknowledge Sub Message (SID 83)

2.2.2.16 Negative Response (SID 7F)

2.2.3 Üzenetáramlás

2.2.4 Szinkronozás

▼B

2.2.5 A hibák kezelése

2.2.5.1 Kommunikációs szakasz megkezdése

2.2.5.2 Kommunikációs szakasz

2.2.6 A válaszüzenet tartalma

2.2.6.1 Positive Response Transfer Data Overview

2.2.6.2 Positive Response Transfer Data Activities

2.2.6.3 Positive Response Transfer Data Events and Faults

2.2.6.4 Positive Response Transfer Data Detailed Speed

2.2.6.5 Positive Response Transfer Data Technical Data

2.3. ESM fájlok tárolása

3. A TACHOGRÁFKÁRTYÁK LETÖLTÉSÉNEK PROTOKOLLJA

3.1. Alkalmazási kör

3.2. Fogalommeghatározások

3.3. Kártyaletöltés

3.3.1 Inicializálási szekvencia

3.3.2 Az alá nem írt adatfájlok szekvenciája

3.3.3 Az aláírt adatfájlok szekvenciája

3.3.4 A kalibrálási számláló alaphelyzetbe történő visszaállításának szekvenciája

3.4. Az adatok tárolási formátuma

3.4.1 Bevezetés

3.4.2 A fájlok formátuma

4. A TACHOGRÁFKÁRTYA LETÖLTÉSE A JÁRMŰEGYSÉGEN KERESZTÜL

1. BEVEZETÉS

Ez a függelék azokat az eljárásokat tartalmazza, amelyeket a külső tárolóeszközökre történő különféle típusú adatletöltések érdekében követni kell, valamint meghatározza azon protokollokat, amelyeket fel kell használni a megfelelő adatátvitel, valamint a letöltött adatok formátuma teljes kompatibilitásának biztosítása érdekében azért, hogy bármely ellenőrző személy megvizsgálhassa ezen adatokat, és elemzésük előtt meggyőződhessen hitelességükről és sértetlenségükről.

1.1. **Alkalmazási kör**

Adatok letölthetők külső tárolóeszközre (ESM):

— egy járműegységről (VU) egy, a járműegységgel összekapcsolt intelligens kijelölt berendezés (IDE) útján,

— egy tachográfkártyáról egy IDE útján, amely fel van szerelve egy kártyainterfész-készülékkel (IFD),

▼B

— egy tachográfkártyáról egy járműegységen keresztül egy, a járműegységgel összekapcsolt IDE felhasználásával.

Annak érdekében, hogy a külső tárolóeszközön tárolt, letöltött adatok hitelességét és sértetlenségét ellenőrizni lehessen, az adatokat a 11. függelékkel (Közös biztonsági mechanizmusok) összhangban mellékelt aláírással együtt kell letölteni. Ezenkívül le kell tölteni a forrásberendezés (VU vagy kártya) azonosítóját és biztonsági tanúsítványait (tagállami és felszerelési). Az adatokat ellenőrző személynek megbízható európai nyilvános kulccsal kell rendelkeznie.

DDP_001 Az egy adott letöltési munkamenet során letöltött adatokat a külső tárolóeszközön egyetlen fájlban kell tárolni.

1.2. **Betűszavak, jelmagyarázat**

E függelék a következő betűszavakat használja:

AID Application Identifier – alkalmazásazonosító

ATR Answer To Reset – válasz az alaphelyzetbe állításra

CS Checksum byte – ellenőrzőösszeg bájt

DF Dedicated File – célra rendelt fájl

DS_ Diagnostic Session – diagnosztikai munkamenet

EF Elementary File – elemi fájl

ESM External Storage Medium – külső tárolóeszköz

FID File Identifier (File ID) – fájlazonosító

FMT formátumbájt (az üzenet fejrészének első bájtja)

ICC Integrated Circuit Card – integrált áramkörös kártya

IDE Intelligent Dedicated Equipment – intelligens kijelölt berendezés: olyan berendezés, amellyel a külső tárolóeszközre (például személyi számítógépre) adatletöltés végezhető

IFD interfészkészülék

KWP Keyword Protocol 2000 – kulcsszóprotokoll 2000

LEN hosszbájt (az üzenet fejrészének utolsó bájtja)

PPS Protocol Parameter Selection – a protokollparaméter kiválasztása

PSO Perform Security Operation – biztonsági művelet végrehajtása

SID Service Identifier – szolgáltatásazonosító

SRC Source byte – forrásbájt

TGT Target Byte – célbájt

TLV Tag Length Value – a címke hosszának értéke

TREP Transfer Response Parameter – átviteli válasz paramétere

TRTP Transfer Request Parameter – átviteli kérés paramétere

VU Vehicle Unit – járműegység

▼B

2. ADATOK LETÖLTÉSE A JÁRMŰEGYSÉGRŐL

2.1. **Letöltési eljárás**

Az adatok járműegységről történő letöltésének végrehajtásához az operátornak el kell végeznie a következő műveleteket:

— tachográfkártyája behelyezése a VU kártyaolvasó egységbe (*);

— az IDE összekapcsolása a VU letöltési csatlakozójával;

— kapcsolatot létrehozása az IDE és a VU között;

— az IDE-n letöltendő adatok kiválasztása és a kérés elküldése a járműegységre;

— a letöltési munkamenet befejezése.

2.2. **Adatletöltési protokoll**

A protokoll mester-szolga alapon strukturált, ahol az IDE tölti be a mester szerepét, a járműegység pedig a szolga szerepét.

Az üzenetek struktúrája, típusai és áramlása alapvetően a „kulcsszó protokoll 2000”-re (KWP) épül (ISO 14230-2 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part2: Data link layer).

Az alkalmazási réteg alapvetően az ISO 14229-1 aktuális tervezetére épül (Road vehicles – Diagnostic systems – Part 1: Diagnostic services, 2001. február 22-i 6. verzió).

2.2.1 *Az üzenetek struktúrája*

DDP_002 Az IDE és a járműegység között kicserélt összes üzenetek egy három részből álló struktúra szerint kerülnek formázásra:

— fejrész, amely egy formátumbájtból (FMT), egy célbájtból (TGT), egy forrásbájtból (SRC) és lehetőleg egy hosszbájtból áll (LEN),

— adatmező, amely egy szolgáltatásazonosító bájtból (SID) és változó számú adatbájtból áll, amelyek között szerepelhet egy választható diagnosztikaimunkamenet-bájt (DS_), vagy egy választható transzferparaméter bájt (TRTP vagy TREP).

— ellenőrző összeg, amely egy ellenőrző bájtból áll (CS).

Fejrész				Adatmező					Ellenőrző összeg
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bájt				Maximum 255 bájt					1 bájt

A célbájt (TGT) és a forrásbájt (SRC) az üzenet fogadójának és feladójának fizikai címét jeleníti meg. Az IDE értéke F0 Hex, a VU értéke pedig EE Hex.

A hosszbájt (LEN) az adatmező hosszát jelenti.

Az ellenőrző bájt 8 biten tartalmazza az üzenet összes bájtja összegének – az ellenőrzőbájt kivételével – 256-tal történő osztási maradékát.

Az FMT, SID, DS_, TRTP és TREP bájtok meghatározása e dokumentum más részében történik.

(*) A behelyezett kártya elindítja a megfelelő hozzáférési jogosultságot a letöltési funkcióhoz és az adatokhoz. A járműegység egyik kártyaolvasó egységébe helyezett járművezetői kártyából is lehet azonban adatokat letölteni, amennyiben a másik kártyaolvasó egységbe nem helyeztek be kártyát.

▼B

DDP_003 Amennyiben azon adatok, amelyeket az üzenetnek hordoznia kell, hosszabbak, mint az adatmezőben rendelkezésre álló hely, az üzenet tényleges elküldése több alüzenet formájában történik. Minden egyes alüzenet egy fejrészből, ugyanolyan SID-ből, TREP-ből és egy két bájtból álló olyan alüzenetszámlálóból áll, amely feltünteti az alüzenet számát a teljes üzeneten belül. A hibaellenőrzés és a megszakítás lehetővé tétele érdekében az IDE minden egyes alüzenetet visszaigazol. Az IDE képes fogadni az alüzeneteket, kérni azok újbóli továbbítását, és képes arra, hogy felszólítsa a járműegységet a továbbítás újraindítására vagy megszakítására.

DDP_004 Amennyiben a legutolsó alüzenet pontosan 255 bájtot tartalmaz az adat-mezőben, csatolni kell egy utolsó alüzenetet üres adatmezővel (az SID TREP és az alüzenet számláló kivételével) az üzenet végének jelölése céljából.

Példa:

Fejrész	SID	TREP	Message	CS
4 bájt	255 bájtnál hosszabb			

Ezt a következőképpen kell továbbítani:

Fejrész	SID	TREP	00	01	1. alüzenet	CS
4 bájt	255 bájt					

Fejrész	SID	TREP	00	02	2. alüzenet	CS
4 bájt	255 bájt					

…

Fejrész	SID	TREP	xx	yy	n. alüzenet	CS
4 bájt	255 bájtnál kevesebb					

vagy:

Fejrész	SID	TREP	00	01	1. alüzenet	CS
4 bájt	255 bájt					

Fejrész	SID	TREP	00	02	2. alüzenet	CS
4 bájt	255 bájt					

…

Fejrész	SID	TREP	xx	yy	n. alüzenet	CS
4 bájt	255 bájt					

Fejrész	SID	TREP	xx	yy + 1	CS
4 bájt	4 bájt				

▼B

2.2.2 *Az üzenetek típusai*

A VU és az IDE közötti adatletöltéshez szükséges kommunikációs protokoll nyolc különféle típusú üzenet cseréjét követeli meg.

A következő táblázat összefoglalja ezen üzeneteket.

Az üzenet struktúrája	Maximum 4 bájt Fejrész				Maximum 255 bájt Adatok			1 bájt Ellenőrző összeg
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (1. fokozat)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (2. fokozat)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF,FF, FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6

▼B

Az üzenet struktúrája	Maximum 4 bájt Fejrész				Maximum 255 bájt Adatok			1 bájt Ellen-őrző összeg
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct vagy Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Megjegyzések:

— Sid Req = A vonatkozó kérés szolgáltatásazonosítója.

— TREP = A vonatkozó kérés TRTP-je.

— A sötét cellák azt jelzik, hogy nem történik adatátvitel.

— Az „upload” (feltöltés) kifejezést kell használni (mint az IDE-nél) az ISO 14229-cel történő kompatibilitás érdekében. Ugyanazt jelenti, mint a „download” (letöltés) kifejezés (mint a járműegységnél).

— E táblázatban nem szerepelnek kétbájtos potenciális alüzenetszámlálók.

— A „slot” a kártyaolvasó egységek számát jelöli, amely vagy 1 (kártya a járművezetői kártyaolvasó egységben) vagy 2 (kártya a járműkísérői kártyaolvasó egységben).

— Ha a „slot” nincs meghatározva, a járműegységnek az 1-es kártyaolvasó egységet kell választania, ha a kártyát ebbe helyezték be, és a 2-es kártyaolvasó egységet kell választania, ha a felhasználó kifejezetten ezt választotta.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Ezt az üzenetet az IDE küldi azért, hogy létrehozza a kommunikációs kapcsolatot a járműegységgel. A kezdeti kommunikációk mindig 9 600 Baud szinten zajlanak (amíg az átviteli sebesség a megfelelő kapcsolatellenőrző szolgáltatás segítségével meg nem változik).

▼B

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Ezt az üzenetet a járműegység küldi el egy „Start Communication Request” kérésre adott pozitív válaszként. Két kulcsbájtot tartalmaz (‘EA’ és ‘8F’), amelyek jelzik, hogy az egység támogatja a protokollt a fejrésszel, beleértve a célra, a forrásra és a hosszra vonatkozó információkat is.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 A „Start Diagnostic Session Request” kérésre vonatkozó üzenetet az IDE küldi azért, hogy egy új diagnosztikai munkamenetet indítson el a járműegységgel. Az „alapértelmezett munkamenet” alfunkció (81 Hex) a megnyitandó szabványos diagnosztikai munkamenetre utal.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 A „Positive Response Start Diagnostic” üzenetet a járműegység küldi azért, hogy pozitív választ adjon a „Diagnostic Session Request” üzenetre.

2.2.2.5 Link Control Service (SID 87)

DDP_052 A „Link Control Service” üzenetet az IDE használja az átviteli sebesség megváltoztatásának kezdeményezésére. Erre két lépésben kerül sor. Az első lépésben az IDE javaslatot tesz az átviteli sebesség megváltoztatására az új érték feltüntetésével. Miután megkapta a pozitív üzenetet a járműegységtől, az IDE elküldi az átviteli sebesség megváltoztatásának megerősítését a járműegységnek (második lépés). Ezután az IDE átáll az új átviteli sebességre. A megerősítés vétele után a járműegység átáll az új átviteli sebességre.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 A „Link Control Positive Response” üzenetet a járműegység küldi azért, hogy pozitív választ adjon a „Link Control Service Request” kérésre (első lépés). Fontos, hogy a megerősítés kérése (második lépés) nem kerül megválaszolásra.

2.2.2.7 Request Upload (SID 35)

DDP_009 A „Request Upload” üzenetet az IDE küldi azért, hogy a járműegység számára jelezze, hogy feltöltési művelet végrehajtását kéri. Az ISO 14229 követelményeinek kielégítése érdekében az adatok tartalmazzák a kért adatok címére, méretére és formátumára vonatkozó részleteket. Mivel az IDE nem ismeri e részleteket a letöltést megelőzően, a memóriacím értékét 0-ra, a formátumot titkosítás és tömörítés nélkülire, a memória méretét pedig maximálisra kell beállítani.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 A „Positive Response Request Upload” üzenetet a járműegység küldi azért, hogy jelezze az IDE-nek, hogy készen áll az adatok letöltésére. Az ISO 14229 követelményeinek kielégítése érdekében az ebben a pozitív válaszüzenetben szereplő adatok azt jelzik az IDE-nek, hogy a további „Positive Response Transfer Data” üzenetek 00FF hex bájtot fognak tartalmazni maximálisan.

▼B

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 A „Transfer Data Request” üzenetet az IDE küldi azért, hogy a járműegység számára meghatározza a letöltendő adatok típusát. Egy egybájtos „Transfer Request Parameter” (TRTP) jelzi az átvitel típusát.

Az adatátvitelnek hat típusa van:

— Overview (TRTP 01),

— Activities of a specified date (TRTP 02),

— Events and faults (TRTP 03),

— Detailed speed (TRTP 04),

— Technical data (TRTP 05),

— Card download (TRTP 06).

DDP_054 Az IDE-nek kötelezően kérnie kell az áttekintési adatok átvitelét (TRTP 01) a letöltési munkamenet során, mivel csak ez biztosítja azt, hogy a járműegység tanúsítványai feljegyzésre kerüljenek a letöltött fájlban (és teszi lehetővé a digitális aláírás hitelesítését).

A második esetben (TRTP 02) a „Transfer Data Request” üzenet tartalmazza a letöltendő naptári nap adatait (`TimeReal` formátum).

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 A „Positive Response Transfer Data” üzenetet a járműegység küldi el a „Transfer Data Request” kérésre adott válaszként. Az üzenet tartalmazza a kért adatokat és azt a „Transfer Response Parameter”-t (TREP), amely megfelel a kérés TRTP-jének.

DDP_055 Az első esetben (TREP 01) a járműegység elküldi az adatokat azért, hogy segítséget nyújtson az IDE operátorának azon adatok kiválasztásához, amelyek letöltését folytatni kívánja. Ezen üzenet a következő információkat tartalmazza:

— biztonsági tanúsítványok,

— a jármű azonosítása,

— a VU aktuális dátuma és ideje,

— min. és max. letölthető dátum (VU adatai),

— a járműegységbe helyezett kártyák adatai,

— korábbi letöltések egy vállalkozás számára,

— vállalkozás általi lezárások,

— korábbi ellenőrzések.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 A „Request Transfer Exit” üzenetet az IDE küldi azért, hogy tájékoztassa a járműegységet a letöltési munkamenet befejezéséről.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 A „Positive Response Request Transfer Exit” üzenetet a járműegység küldi azért, hogy visszaigazolja a „Request Transfer Exit” kérést.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 A „Stop Communication Request” üzenetet az IDE küldi azért, hogy megszakítsa a kommunikációs kapcsolatot a járműegységgel.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 A „Positive Response Stop Communication” üzenetet a járműegység küldi azért, hogy visszaigazolja a „Stop Communication Request” kérést.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Az „Acknowledge Sub Message” üzenetet az IDE küldi azért, hogy megerősítse azon üzenet egyes részeinek vételét, amely több alüzenet formájában került átvitelre. Az adatmező tartalmazza a járműegységtől kapott SID-et és egy kétbájtos kódot, a következők szerint:

— MsgC + 1: visszaigazolja az MsgC számú alüzenet vételét.

Az IDE kéri a járműegységtől a következő alüzenet küldését.

— MsgC: azt jelzi, hogy probléma van az MsgC számú alüzenet vételével.

Az IDE újra kéri a járműegységtől az alüzenet küldését.

— FFFF kéri az üzenet megszakítását.

Ezt az IDE használhatja arra, hogy bármilyen okból megszakítsa a járműegység üzenetének továbbítását.

Az üzenet utolsó alüzenetét (LEN bájt < 255) vissza lehet igazolni bármely fenti kód alkalmazásával, vagy adott esetben nincs visszaigazolás.

A több alüzenetből álló VU-válaszok:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 A „Negative Response” üzenetet a járműegység küldi el, válaszul a fentiekben leírt kérési üzenetekre, ha nem tud eleget tenni a kérésnek. Az üzenet adatmezői tartalmazzák a válasz szolgáltatásazonosítóját (SID) (7F), a kérés szolgáltatásazonosítóját, valamint egy kódot, amely megadja a negatív válasz okát. A következő kódok állnak rendelkezésre:

— 10: általános elutasítás

A műveletet nem lehet végrehajtani, a következőkben nem részletezett okok miatt.

— 11: a szolgáltatás nem támogatott

A kérés szolgáltatásazonosítója nem érthető.

— 12: az alfunkció nem támogatott

A kérés DS_ vagy TRTP nem érthető, vagy nincs több továbbítandó alüzenet.

— 13: az üzenet hossza helytelen

A kapott üzenet hossza rossz.

— 22: a feltételek nem megfelelőek vagy hiba van a kérési szekvenciában

A kért szolgáltatás nem aktív, vagy a kérésüzenet szekvenciája nem megfelelő.

— 31: tartományon kívüli kérés

A kérés paraméterrekordja (adatmező) érvénytelen.

— 50: a feltöltés elutasítva

A kérést nem lehet teljesíteni (a VU nem megfelelő üzemmódban van, vagy benne belső hiba keletkezett).

— 78: a válasz függőben

A kért műveletet nem lehet időben teljesíteni, és a VU nem áll készen további kérések fogadására.

— FA: az adatok nem állnak rendelkezésre

Az adatátviteli kérés adatobjektuma nem áll rendelkezésre a járműegységben (például nincs behelyezve kártya stb.).

2.2.3 *Üzenetáramlás*

A jellemző üzenetáramlás egy normál adatletöltési eljárás során a következő:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

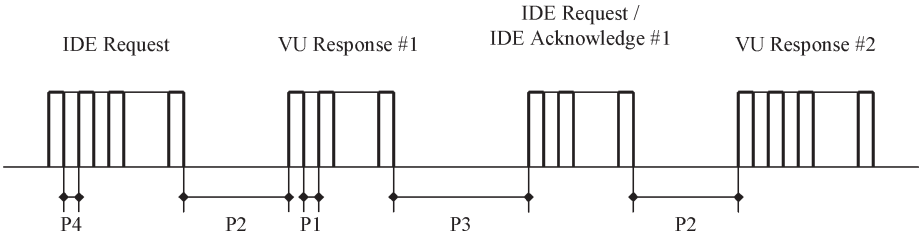
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Szinkronozás*

DDP_019 Normál működés során a következő ábrán bemutatott szinkronozási paraméterek érvényesek:

1. ábra

Üzenetáramlás, szinkronozás



ahol:

P1 = A bájtok áramlása között eltelt idő a járműegység válaszára várva.

P2 = Az IDE kérésének vége és a járműegység válaszának megkezdése között eltelt idő vagy az IDE visszaigazolásának vége és a járműegység következő válaszának megkezdése között eltelt idő.

P3 = A járműegység válaszának vége és az IDE új kérésének megkezdése között eltelt idő vagy a járműegység válaszának vége és az IDE visszaigazolásának megkezdése között eltelt idő, vagy az IDE kérésének vége és az IDE új kérésének megkezdése között eltelt idő, amennyiben a járműegység nem válaszol.

P4 = A bájtok áramlása között eltelt idő az IDE-kérésnél.

P5 = A P3 kiterjesztett értéke a kártya letöltéséhez.

▼B

A szinkronozási paraméterek megengedett értékeit az alábbi táblázat adja meg (a KWP azon kiterjesztett szinkronozási paraméterei vannak beállítva, amelyeket fizikai címzés esetén használnak a gyorsabb kommunikáció érdekében).

Szinkronozási paraméter	Az alsó határ értéke (ms)	A felső határ értéke (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 perc

(*) Amennyiben a járműegység „Negative Response” választ ad, amely válasz tartalmazza „megfelelően fogadott kérés, a válasz függőben” jelentésű kódot, akkor ezen érték kiterjed a P3 felső határával azonos értékre.

2.2.5 *A hibák kezelése*

Amennyiben hiba történik az üzenetek cseréje során, az üzenetáramlási rendszer módosul attól függően, hogy melyik berendezés észlelte a hibát, valamint a hibát generáló üzenettől függően.

A 2. és a 3. ábra bemutatja a VU, valamint az IDE hibakezelési eljárásait.

2.2.5.1 Kommunikációs szakasz megkezdése

DDP_020 Ha az IDE hibát fedez fel a „Kommunikációs szakasz megkezdése” során vagy a szinkronozással, vagy a bitek áramlásával kapcsolatosan, kivár egy P3min periódust a kérés megismétlése előtt.

DDP_021 Ha a JE hibát fedez fel az IDE-től érkező szekvenciában, nem válaszol, és egy P3max perióduson keresztül várja az újabb „Start Communication Request” üzenetet.

2.2.5.2 Kommunikációs szakasz

Két különböző hibakezelési terület határozható meg:

1. **A VU hibát észlel az IDE átvitelében.**

DDP_022 A VU minden egyes kapott üzenet esetében észleli a szinkronozási hibákat, a bájtok formátumában tapasztalható hibákat (például a kezdő és befejező bitek sérülései), valamint a kerethibákat (a kapott bájtok helytelen száma, helytelen ellenőrző bájt).

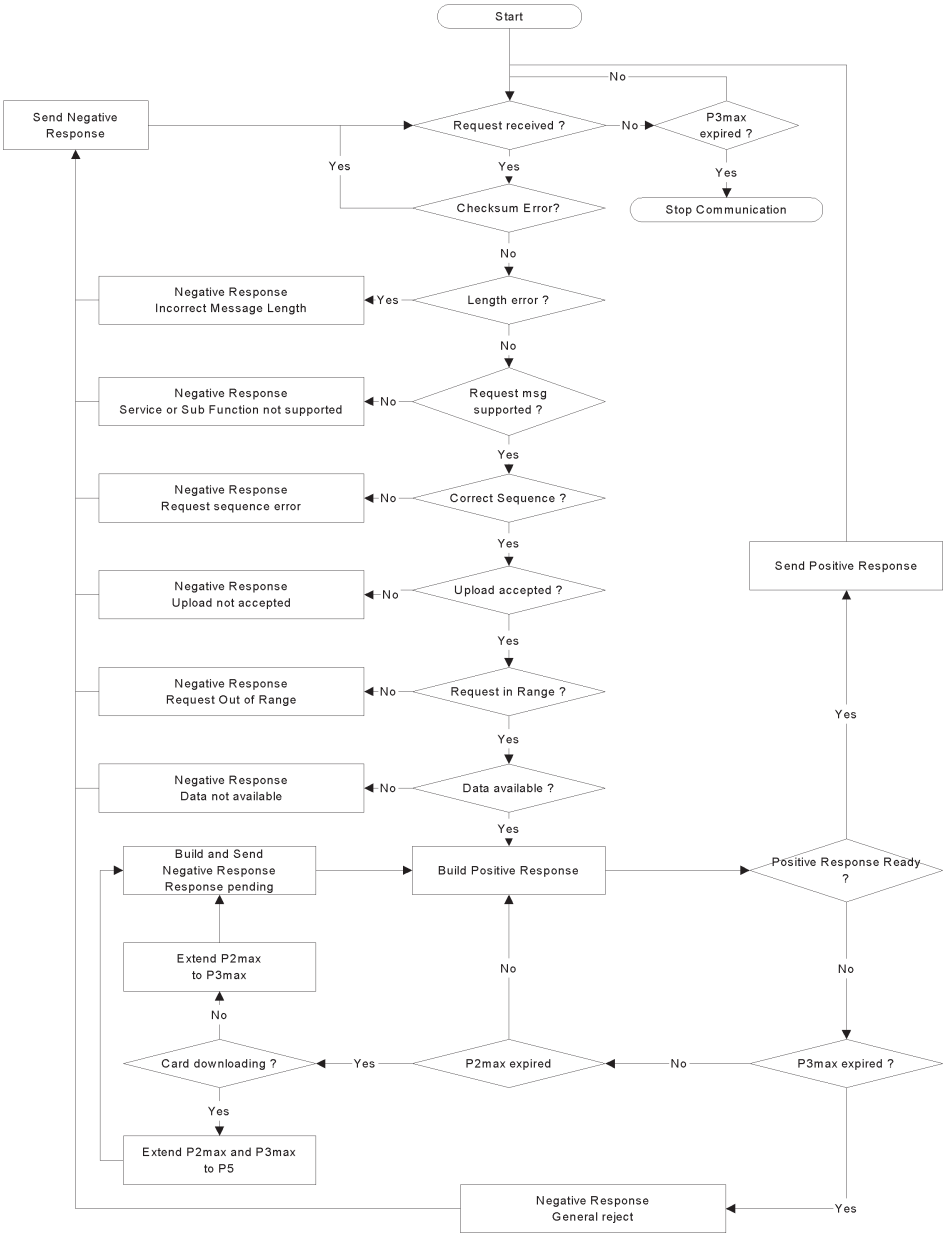
DDP_023 Ha a járműegység észleli valamelyik fenti hibát, nem válaszol és figyelmen kívül hagyja a kapott üzenetet.

DDP_024 A járműegység más hibákat is észlelhet a kapott üzenet formátumában vagy tartalmában (például az üzenet nem támogatott), még akkor is, ha az üzenet megfelel a hosszal és az ellenőrző összeggel kapcsolatos követelményeknek; ilyenkor a járműegység „Negative Response” üzenettel válaszol az IDE-nek, amelyben meghatározza a hiba természetét.

▼B

2. ábra

VU hibakezelés



2. **Az IDE hibát észlel a VU átvitelében.**

DDP_025 Az IDE minden egyes kapott üzenet esetében észleli a szinkronozási hibákat, a bájtok formátumában tapasztalható hibákat (például a kezdő és befejező bitek sérülései), valamint a kerethibákat (a kapott bájtok helytelen száma, helytelen ellenőrző bájt).

DDP_026 Az IDE észleli a szekvenciák hibáit, például az alüzenetek számlálóinak nem megfelelő növekedését az egymás után megkapott üzenetekben.

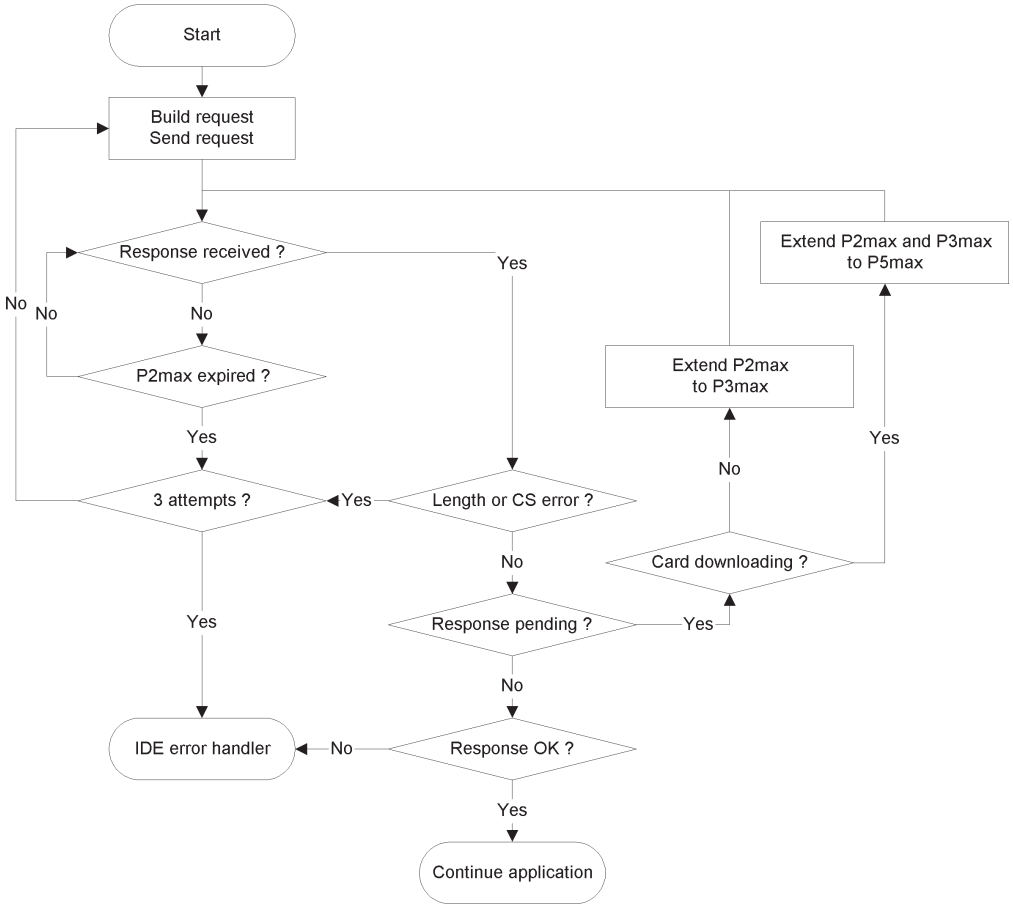
DDP_027 Amennyiben az IDE hibát észlel, vagy nem kap választ a járműegységtől egy P2max perióduson belül, megismétli a kérésüzenet elküldését, összesen legfeljebb háromszor. A hiba észlelése tekintetében az alüzenetek visszaigazolását a járműegységnek elküldött kérésnek kell tekinteni.

▼B

DDP_028 Az IDE legalább P3min periódust vár az egyes átvitelek megkezdése előtt; a várakozási periódust a hiba észlelése után egy befejező bit utolsó számított előfordulásától kezdve kell mérni.

3. ábra

IDE hibakezelés



2.2.6 *A válaszüzenet tartalma*

Ez a pont a különféle pozitív válaszüzenetek adatmezőinek tartalmát határozza meg.

Az adatelemeket az 1. függelék adatszótára határozza meg.

Megjegyzés: A 2. generációs letöltések esetében minden felső szintű adatelemet egy adattömb (record array) reprezentál, akkor is ha az csak egy rekordot tartalmaz. Az adattömb egy fejrésszel kezdődik; ez a fejrész magában foglalja a rekordtípust, a rekordméretet és a rekordok számát. Az alábbi táblázatokban az adattömbök „…RecordArray” (fejrésszel) elnevezéssel szerepelnek.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 A „Positive Response Transfer Data Overview” üzenet adatmezője biztosítja a következő adatokat, az alábbi sorrendben, az SID 76 Hex, a TREP 01 Hex és az alüzenetek megfelelő felosztása és számozása alapján:

▼B

1. generációs adatstruktúra

Adatelem	Megjegyzés
MemberStateCertificate VUCertificate	VU biztonsági tanúsítvány
VehicleIdentificationNumber VehicleRegistrationIdentification	A jármű azonosítása
CurrentDateTime	VU aktuális dátuma és ideje
VuDownloadablePeriod	Letöltendő időszak
CardSlotsStatus	VU-ba behelyezett kártyák típusa
VuDownloadActivityData	Előző VU letöltése
VuCompanyLocksData	Valamennyi tárolt, vállalkozás általi lezárás. Ha a szakasz üres, csak ez kerül elküldésre: noOfLocks = 0.
VuControlActivityData	A járműegységben tárolt minden ellenőrzési rekord. Ha a szakasz üres, csak ez kerül elküldésre: noOfControls = 0.
Signature	A tanúsítványok kivételével valamennyi adat RSA aláírása kezdve a VehicleIdentificationNumber adattól egészen az utolsó VuControlActivityData utolsó bájtjáig.

2. generációs adatstruktúra

Adatelem	Megjegyzés
MemberStateCertificateRecordArray	Tagállami tanúsítvány
VUCertificateRecordArray	VU tanúsítvány
VehicleIdentificationNumberRecordArray	A jármű azonosítása
VehicleRegistrationNumberRecordArray	A jármű rendszáma
CurrentDateTimeRecordArray	VU aktuális dátuma és ideje
VuDownloadablePeriodRecordArray	Letöltendő időszak
CardSlotsStatusRecordArray	VU-ba behelyezett kártyák típusa
VuDownloadActivityDataRecordArray	Előző VU letöltése
VuCompanyLocksRecordArray	Valamennyi tárolt, vállalkozás általi lezárás. Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuControlActivityRecordArray	A járműegységben tárolt minden ellenőrzési rekord. Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
SignatureRecordArray	Minden előző adat ECC aláírása a tanúsítványok kivételével.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 A „Positive Response Transfer Data Activities” üzenet adatmezője biztosítja a következő adatokat, az alábbi sorrendben, az SID 76 Hex, a TREP 02 Hex és az alüzenetek megfelelő felosztása és számozása alapján:

▼B

1. generációs adatstruktúra

Adatelem	Megjegyzés
TimeReal	A letöltött nap dátuma
OdometerValueMidnight	Kilométer-számláló és a letöltött nap vége
VuCardIWData	Adatok a kártyabehelyezési/kivételi eljáráshoz. — Ha ehhez a szakaszhoz nem áll rendelkezésre adat, csak ez kerül elküldésre: noOfVuCardIWRecords = 0. — Ha egy VuCardIWRecord áthalad 00:00 órán (kártyabehelyezés előző nap) vagy 24:00 órán (kártyakivétel következő nap), akkor teljes egészében meg kell jelennie mindkét érintett nap tekintetében.
VuActivityDailyData	Kártyaleolvasó egység 00:00 állapot és rögzített tevékenységváltás a letöltött nap tekintetében.
VuPlaceDailyWorkPeriodData	A letöltött nap tekintetében rögzített adatokkal kapcsolatos helyek Ha a szakasz üres, csak ez kerül elküldésre: noOfPlaceRecords = 0.
VuSpecificConditionData	A letöltött nap tekintetében rögzített, különleges körülményekre vonatkozó adatok Ha a szakasz üres, csak ez kerül elküldésre: noOfSpecificConditionRecords = 0.
Signature	Valamennyi adat RSA aláírása kezdve a TimeReal adattól egészen a különleges körülménnyel kapcsolatos utolsó rekord utolsó bájtjáig.

2. generációs adatstruktúra

Adatelem	Megjegyzés
DateOfDayDownloadedRecordArray	A letöltött nap dátuma
OdometerValueMidnightRecordArray	Kilométer-számláló és a letöltött nap vége
VuCardIWRecordArray	Adatok a kártyabetételi/kivételi eljáráshoz. — Ha ez a szakasz nem tartalmaz elérhető adatot, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0. — Ha egy VuCardIWRecord áthalad 00:00 órán (kártyabehelyezés előző nap) vagy 24:00 órán (kártyakivétel következő nap), akkor teljes egészében meg kell jelennie mindkét érintett nap tekintetében.
VuActivityDailyRecordArray	Kártyaleolvasó egység 00:00 állapot és rögzített tevékenységváltás a letöltött nap tekintetében.
VuPlaceDailyWorkPeriodRecordArray	A letöltött nap tekintetében rögzített adatokkal kapcsolatos helyek Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuGNSSCDRecordArray	A jármű GNSS-pozíciói, ha a járművezető megszakítás nélküli járművezetési ideje eléri a három órahossza többszörösét. Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuSpecificConditionRecordArray	A letöltött nap tekintetében rögzített, különleges körülményekre vonatkozó adatok Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
SignatureRecordArray	Minden előző adat ECC aláírása.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 A „Positive Response Transfer Data Events and Faults” üzenet adatmezője biztosítja a következő adatokat, az alábbi sorrendben, az SID 76 Hex, a TREP 03 Hex és az alüzenetek megfelelő felosztása és számozása alapján:

1. generációs adatstruktúra

Adatelem	Megjegyzés
VuFaultData	A járműegységben tárolt vagy folyamatban lévő minden hiba. Ha a szakasz üres, csak ez kerül elküldésre: noOfVuFaults = 0.
VuEventData	A járműegységben tárolt vagy folyamatban lévő minden hiba (a gyorshajtás kivételével) Ha a szakasz üres, csak ez kerül elküldésre: noOfVuEvents = 0.
VuOverSpeedingControlData	A gyorshajtás legutóbbi ellenőrzésére vonatkozó adatok (ha nincs adat, alapértelmezett érték).
VuOverSpeedingEventData	A járműegységben tárolt minden gyorshajtási esemény. Ha a szakasz üres, csak ez kerül elküldésre: noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	A járműegységben tárolt minden időbeállítási esemény (a teljes körű kalibrálás keretein kívül). Ha a szakasz üres, csak ez kerül elküldésre: noOfVuTimeAdjRecords = 0.
Signature	Valamennyi adat RSA aláírása kezdve a noOfVuFaults adattól egészen az időbeállítással kapcsolatos utolsó rekord utolsó bájtjáig.

2. generációs adatstruktúra

Adatelem	Megjegyzés
VuFaultRecordArray	A járműegységben tárolt vagy folyamatban lévő minden hiba. Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuEventRecordArray	A járműegységben tárolt vagy folyamatban lévő minden hiba (a gyorshajtás kivételével). Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	A gyorshajtás legutóbbi ellenőrzésére vonatkozó adatok (ha nincs adat, alapértelmezett érték).
VuOverSpeedingEventRecordArray	A járműegységben tárolt minden gyorshajtási esemény. Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuTimeAdjustmentRecordArray	A járműegységben tárolt minden időbeállítási esemény (a teljes körű kalibrálás keretein kívül). Ha a szakasz üres, csak ez kerül elküldésre: egy adattömb-fejrész, valamint noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Minden előző adat ECC aláírása.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 A „Positive Response Transfer Data Detailed Speed” üzenet adatmezője biztosítja a következő adatokat, az alábbi sorrendben, az SID 76 Hex, a TREP 04 Hex és az alüzenetek megfelelő felosztása és számozása alapján:

1. generációs adatstruktúra

Adatelem	Megjegyzés
VuDetailedSpeedData	A járműegységben tárolt minden részletes sebesség (percenként egy sebességblokk, amely alatt a jármű mozgásban volt). Percenként 60 gyorsasági érték (másodpercenként egy).
Signature	Valamennyi adat RSA aláírása kezdve a noOfSpeedBlocks adattól egészen az utolsó sebességblokk utolsó bájtjáig.

2. generációs adatstruktúra

Adatelem	Megjegyzés
VuDetailedSpeedBlockRecordArray	A járműegységben tárolt minden részletes sebesség (percenként egy sebességblokk, amely alatt a jármű mozgásban volt). Percenként 60 gyorsasági érték (másodpercenként egy).
SignatureRecordArray	Minden előző adat ECC aláírása.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 A „Positive Response Transfer Data Technical Data” üzenet adatmezője biztosítja a következő adatokat, az alábbi sorrendben, az SID 76 Hex, a TREP 05 Hex és az alüzenetek megfelelő felosztása és számozása alapján:

1. generációs adatstruktúra

Adatelem	Megjegyzés
VuIdentification	
SensorPaired	
VuCalibrationData	A járműegységben tárolt minden kalibrálási rekord.
Signature	Valamennyi adat RSA aláírása kezdve a vuManufacturerName adattól egészen az utolsó VuCalibrationRecord utolsó bájtjáig.

▼B

2. generációs adatstruktúra

Adatelem	Megjegyzés
VuIdentificationRecordArray	
VuSensorPairedRecordArray	A járműegységben tárolt minden MS párosítás.
VuSensorExternalGNSSCoupledRecordArray	A járműegységben tárolt minden külső GNSS-eszköz csatlakozás.
VuCalibrationRecordArray	A járműegységben tárolt minden kalibrálási rekord.
VuCardRecordArray	A járműegységben tárolt minden kártyabehelyezési adat.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Minden előző adat ECC aláírása.

2.3. **ESM fájlok tárolása**

DDP_034 Ha a letöltési munkamenet tartalmazott egy, a járműegységről való adatátviteli műveletet, az IDE egyetlen fizikai fájlban tárolja az összes olyan adatot, amelyet a járműegységtől kapott a letöltési munkamenet során, „Positive Response Transfer Data” üzenetekben. A tárolt adatok nem tartalmazzák az üzenet fejrészét, az alüzenetek számlálóit, az üres alüzeneteket és az ellenőrző összegeket, de tartalmazzák a SID-et és TREP-et (több alüzenetnél csak az első alüzenetet).

3. A TACHOGRÁFKÁRTYÁK LETÖLTÉSÉNEK PROTOKOLLJA

3.1. **Alkalmazási kör**

Ez a pont a tachográfkártya adatainak egy IDE-re történő közvetlen letöltését ismerteti. Az IDE nem része a biztonságos környezetnek; ezért nincs hitelesítés a kártya és az IDE között.

3.2. **Fogalommeghatározások**

Letöltési munkamenet: Minden olyan alkalom, amikor a rendszer végrehajtja az ICC adatok letöltését. A munkamenet átfogja a teljes eljárást, az ICC alaphelyzetbe való visszaállításától az ICC dezaktiválásáig (a kártya kivétele vagy a következő visszaállítás).

Aláírt adatfájl: Egy fájl az ICC-ről. A fájl normál szövegként kerül átvitelre az IFD-re. Az integrált áramkörös kártyán a fájl hasított és aláírt, az aláírást átviszik az IFD-re.

3.3. **Kártyaletöltés**

DDP_035 A tachográfkártya letöltése a következő lépéseket foglalja magában:

— A kártya közös információinak letöltése az ICC és IC EF-ekbe. Ezen információk választhatók, és nem védi őket digitális aláírás.

▼B

— A Card_Certificate (vagy CardSignCertificate) és CA_Certificate EF-ek letöltése. Ezen információkat nem védi digitális aláírás.

E fájlokat minden letöltési munkamenetben kötelező letölteni.

— Az egyéb alkalmazási adatok EF-jeinek letöltése (a Tachograph DF-en vagy – ha szükséges – a Tachograph_G2 DF-en belül), a Card_Download EF kivételével. Ezen információt digitális aláírás védi.

— Minden egyes letöltési munkamenetben kötelező letölteni legalább az Application_Identification és ID EF-eket.

— A járművezetői kártya adatainak letöltése során a következő EF-ek letöltése kötelező:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions.

— A járművezetői kártya adatainak letöltése során fel kell frissíteni a LastCardDownload dátumát a Card_Download EF-ben.

— A műhelykártya adatainak letöltése során alaphelyzetbe kell visszaállítani a kalibrálási számlálót a Card_Download EF-ben.

— A műhelykártya adatainak letöltése során a Sensor_Installation_Data EF nem letöltendő.

3.3.1 *Inicializálási szekvencia*

DDP_036 Az IDE a következők szerint kezdeményezi a szekvenciát:

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	Hardver visszaállítása alaphelyzetbe	
ATR	⇨		

A PPS választhatóan felhasználható egy magasabb átviteli sebességre történő átváltáshoz mindaddig, amíg ezt az ICC támogatja.

3.3.2 *Az alá nem írt adatfájlok szekvenciája*

DDP_037 Az ICC, IC, Card_Certificate (vagy CardSignCertificate) és a CA_Certificate EF-ek letöltési szekvenciája a következő:

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	**Fájl kiválasztása**	Kiválasztás fájlazonosítók alapján
OK	⇨		

▼B

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	**Read Binary**	Ha a fájl több adatot tartalmaz, mint amennyit a leolvasó vagy a kártya puffere tárolni képes, a parancsot meg kell ismételni mindaddig, amíg a teljes fájl beolvasása meg nem történik.
Fájladatok OK	⇨	Adatok tárolása ESM-en	a **3.4**. pont szerint (Az adatok tárolási formátuma)

1. megjegyzés: A Card_Certificate (vagy CardSignCertificate) EF kiválasztása előtt ki kell választani a tachográf-alkalmazást (kiválasztás az AID útján).

2. megjegyzés: Egy fájl kiválasztása és olvasása egy lépésben is elvégezhető egy rövid EF azonosítóval rendelkező Read Binary paranccsal.

3.3.3 *Az aláírt adatfájlok szekvenciája*

DDP_038 Az alábbi szekvenciát kell felhasználni a következő fájlok mindegyikéhez, amelyeket aláírásukkal együtt kell letölteni:

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	**Fájl kiválasztása**	
OK	⇨		
	⇦	**Hash of File végrehajtása**	Az előírt hasítási algoritmus felhasználásával kiszámítja a kiválasztott fájl adattartalmának tördelési értékét a 11. függelékkel összhangban. E parancs nem ISO-parancs.
A fájl hasításának kiszámítása és a tördelési érték ideiglenes tárolása			
OK	⇨		
	⇦	**Read Binary**	Ha a fájl több adatot tartalmaz, mint amennyit a leolvasó vagy a kártya puffere tárolni képes, a parancsot meg kell ismételni mindaddig, amíg a teljes fájl beolvasása meg nem történik.
File Data OK	⇨	A kapott adatok eltárolása külső tárolóeszközön	a **3.4**. pont szerint (Az adatok tárolási formátuma)

▼B

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	**PSO: Compute Digital Signature**	
A „digitális aláírás kiszámítása” biztonsági művelet végrehajtása az ideiglenesen eltárolt hasítási érték felhasználásával			
Signature OK	⇨	Az adatok hozzáfűzése a külső tárolóeszközön korábban tárolt adatokhoz	a **3.4**. pont szerint (Az adatok tárolási formátuma)

Megjegyzés: Egy fájl kiválasztása és olvasása egy lépésben is elvégezhető egy rövid EF azonosítóval rendelkező Read Binary paranccsal. Ilyen esetben az EF már a Perform Hash of File parancs alkalmazása előtt kiválasztható és olvasható.

3.3.4 *A kalibrálási számláló alaphelyzetbe történő visszaállításának szekvenciája*

DDP_039 A műhelykártya `Card_Download` EF-jében szereplő `NoOfCalibrationsSinceDownload` számláló alaphelyzetbe történő visszaállításának szekvenciája a következő:

Kártya	Irány	IDE/IFD	Jelentés/Megjegyzések
	⇦	**Select File** EF Card_Download	Kiválasztás fájlazonosítók alapján
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = ‘00 00’	
A kártya letöltési számlálójának alaphelyzetbe állítása			
OK	⇨		

Megjegyzés: Egy fájl kiválasztása és frissítése egy lépésben is elvégezhető egy rövid EF azonosítóval rendelkező Update Binary paranccsal.

3.4. **Az adatok tárolási formátuma**

3.4.1 *Bevezetés*

DDP_040 A letöltött adatokat a következő feltételeknek megfelelően kell tárolni:

— Az adatokat átláthatóan kell tárolni. Ez azt jelenti, hogy a bájtok sorrendjét, valamint a bitek sorrendjét a kártyáról átvitt bájtokon belül meg kell őrizni a tárolás során.

— A kártya összes fájlját, amelynek letöltése egy adott letöltési munkamenet során történt, egyetlen fájlban kell tárolni az ESM-en.

▼B

3.4.2 *A fájlok formátuma*

DDP_041 A fájlformátum több TLV-objektum konkatenációja.

DDP_042 Az EF-eket jelző címke a FID, valamint a „00” függelék.

DDP_043 Az EF-ek aláírását jelző címke a fájl FID-je, valamint a „01” függelék.

DDP_044 A hossz egy kétbájtos érték. Az érték meghatározza az értékmezőben szereplő bájtok számát. A hosszmezőben szereplő „FF FF” érték jövőbeni használat céljából fenntartott.

DDP_045 Ha a fájl nem kerül letöltésre, egyetlen, a fájllal kapcsolatos adatot sem kell tárolni (nincs címke és nincs zéróhossz).

DDP_046 Az aláírást a következő TLV objektumként kell tárolni, közvetlenül azon TLV objektum után, amely a fájl adatait tartalmazza.

Meghatározás	Jelentés	Hossz
FID (2 bájt) ‖ „00”	Címke az EF-hez (FID)	3 bájt
FID (2 bájt) ‖ „01”	Címke az EF-hez tartozó aláíráshoz (FID)	3 bájt
xx xx	Az értékmező hossza	2 bájt

Példa az ESM letöltési fájljában lévő adatokra:

Címke	Hossz	Érték
00 02 00	00 11	Az ICC EF adatai
C1 00 00	00 C2	A Card_Certificate EF adatai
		…
05 05 00	0A 2E	A EF adataiVehicles_Used
05 05 01	00 80	A EF aláírá-saVehicles_Used

4. A TACHOGRÁFKÁRTYA LETÖLTÉSE A JÁRMŰEGYSÉGEN KERESZTÜL

DDP_047 A járműegységnek lehetővé kell tennie a hozzákapcsolt IDE-be behelyezett járművezetői kártya tartalmának letöltését.

DDP_048 Az IDE egy „Transfer Data Request Card Download” üzenetet küld a járműegységnek ezen átviteli mód kezdeményezésére (lásd: 2.2.2.9. pont).

DDP_049 Ezután a járműegység letölti a kártya teljes tartalmát fájlonként, a 3. pontban meghatározott kártyaletöltési protokollal összhangban, és az összes olyan adatot, amelyet a kártyától kapott, továbbítja az IDE-hez, a megfelelő TLV fájlformátumban (lásd: 3.4.2. pont), és beágyazva egy „Positive Response Transfer Data” üzenetbe.

▼B

DDP_050 Az IDE visszakeresi a kártyaadatokat a „Positive Response Transfer Data” üzenetből (eltávolítva az összes fejrészt, SID-et, TREP-et, az alüzenetek számlálóit és az ellenőrző összegeket), és eltárolja az összes adatot a 2.3. pontban leírt egyetlen fizikai fájlban.

DDP_051 Ezután a járműegység adott esetben aktualizálja a járművezetői kártya `Control_Activity_Data` vagy `Card_Download` fájlját.

▼B

8. függelék

KALIBRÁLÁSI PROTOKOLL

TARTALOMJEGYZÉK

1. BEVEZETÉS

2. KIFEJEZÉSEK, MEGHATÁROZÁSOK ÉS HIVATKOZÁSOK

3. A SZOLGÁLTATÁSOK ÁTTEKINTÉSE

3.1. Rendelkezésre álló szolgáltatások

3.2. Válaszkódok

4. KOMMUNIKÁCIÓS SZOLGÁLTATÁSOK

4.1. A StartCommunication szolgáltatás

4.2. StopCommunication szolgáltatás

4.2.1 Az üzenet leírása

4.2.2 Az üzenet formátuma

4.2.3 A paraméterek meghatározása

4.3. TesterPresent szolgáltatás

4.3.1 Az üzenet leírása

4.3.2 Az üzenet formátuma

5. KEZELÉSI SZOLGÁLTATÁSOK

5.1. StartDiagnosticSession szolgáltatás

5.1.1 Az üzenet leírása

5.1.2 Az üzenet formátuma

5.1.3 A paraméterek meghatározása

5.2. SecurityAccess szolgáltatás

5.2.1 Az üzenet leírása

5.2.2 Az üzenetek formátuma – SecurityAccess – requestSeed

5.2.3 Az üzenetek formátuma – SecurityAccess – sendKey

6. ADATÁTVITELI SZOLGÁLTATÁSOK

6.1. ReadDataByIdentifier szolgáltatás

6.1.1 Az üzenet leírása

6.1.2 Az üzenet formátuma

6.1.3 A paraméterek meghatározása

6.2. WriteDataByIdentifier szolgáltatás

6.2.1 Az üzenet leírása

6.2.2 Az üzenet formátuma

6.2.3 A paraméterek meghatározása

▼B

7. A VIZSGÁLATI IMPULZUSOK ELLENŐRZÉSE – INPUT/OUTPUT VEZÉRLŐ FUNKCIONÁLIS EGYSÉG

7.1. InputOutputControlByIdentifier service

7.1.1 Az üzenet leírása

7.1.2 Az üzenet formátuma

7.1.3 A paraméterek meghatározása

8. DATARECORDS FORMÁTUMOK

8.1. Az átvitt paraméterek tartományai

8.2. dataRecords formátumok

1. BEVEZETÉS

E függelék a járműegység és a vizsgálókészülék között a K-vonalon keresztül történő adatcsere módját ismerteti, amely vonal a 6. függelékben leírt kalibrálási interfész részét alkotja. A függelék leírja továbbá az input/output jelvonal vezérlését a kalibrálási csatlakozón.

A K-vonalon történő kommunikáció létrehozása a 4. pontban (Communication Services) található.

E függelék a diagnosztikai „munkamenetek” gondolatát használja fel a K-vonal vezérlése hatókörének meghatározására különböző feltételek között. Az alapértelmezett munkamenet a StandardDiagnosticSession, amelynél valamennyi adat leolvasható a járműegységről, de nem lehet adatokat írni a járműegységre.

A diagnosztikai munkamenet kiválasztását az 5. pont (Kezelési szolgáltatások) (Management Services) írja le.

Ezt a függeléket a VU-k és műhelykártyák mindkét generációjára érvényesnek kell tekinteni az e rendeletben meghatározott interoperabilitási követelményeknek megfelelően.

CPR_001 Az „ECUProgrammingSession” lehetővé teszi adatok bevitelét a járműegységbe. Kalibrálási adatok bevitele esetén a járműegységnek ezenkívül KALIBRÁLÁSI üzemmódban kell lennie.

A K-vonalon át történő adatátvitel leírása a 6. pontban (Data Transmission Services) található. Az átvitt adatok formátumának részletezése a 8. pontban (dataRecords formats) található.

CPR_002 Az „ECUAdjustmentSession” lehetővé teszi a kalibrálási I/O jelvonal I/O üzemmódjának kiválasztását a K-vonal interfészén keresztül. A kalibrálási I/O jelvonal vezérlését a 7. pont (Control of Test Pulses – Input/Output Control functional unit) írja le.

CPR_003 Az egész dokumentumban a vizsgálókészülékre a „tt” rövidítés utal. Annak ellenére, hogy a vizsgálókészülékeknek lehetnek preferált címei, a VU a vizsgálókészülék bármely címére megfelelő módon válaszol. A VU fizikai címe: 0xEE.

▼B

2. KIFEJEZÉSEK, MEGHATÁROZÁSOK ÉS HIVATKOZÁSOK

A protokollok, üzenetek és hibakódok alapvetően az ISO 14229-1 szabványtervre épülnek (Közúti járművek – Diagnosztikai rendszerek – 1. rész: Diagnosztikai szolgáltatások, 6. változat, 2001. február 22.).

A szolgáltatásazonosítókhoz, a szolgáltatási kérésekhez és válaszokhoz, valamint a szabványos paraméterekhez bájtkódolást és hexadecimális értékeket kell használni.

A „vizsgálókészülék” kifejezés arra a berendezésre vonatkozik, amelyet a programozási/kalibrálási adatok VU-ba történő bevitelére kell alkalmazni.

A „kliens” és a „szerver” kifejezés a vizsgálókészülékre, illetve a VU-ra vonatkozik.

Az ECU kifejezés jelentése: „Elektronikus vezérlőegység”, és a VU-ra vonatkozik.

Hivatkozások:

ISO 14230-2: Road Vehicles -Diagnostic Systems – Keyword Protocol 2000- Part 2: Data Link Layer.

First edition: 1999.

Vehicles – Diagnostic.

3. A SZOLGÁLTATÁSOK ÁTTEKINTÉSE

3.1. **Rendelkezésre álló szolgáltatások**

A következő táblázat áttekintést nyújt azon szolgáltatásokról, amelyek a menetíró készülékben rendelkezésre állnak, és amelyek meghatározására ezen dokumentumban kerül sor.

CPR_004 A táblázat jelzi azon szolgáltatásokat, amelyek egy aktivált diagnosztikai munkamenetben rendelkezésre állnak.

— Az **első oszlop** felsorolja a rendelkezésre álló szolgáltatásokat.

— A **második oszlop** jelzi azon pont számát, amely részletesebben leírja az adott szolgáltatást e függelékben.

— A **harmadik oszlop** meghatározza a szolgáltatásazonosító értékeit a kérésüzenetekben.

— A **negyedik oszlop** meghatározza a **„StandardDiagnosticSession” (SD)** azon szolgáltatásait, amelyeket minden járműegységben alkalmazni kell.

— Az **ötödik oszlop** meghatározza az **„ECUAdjustmentSession” (ECUAS)** azon szolgáltatásait, amelyeket alkalmazni kell ahhoz, hogy lehetővé váljon az I/O jelvonal vezérlése a járműegység előlapján található kalibrálási csatlakozón.

— A **hatodik oszlop** meghatározza az **„ECUProgrammingSession” (ECUPS)** azon szolgáltatásait, amelyeket alkalmazni kell ahhoz, hogy lehetővé váljon a paraméterek programozása a járműegységben.

▼B

1. táblázat

A szolgáltatásazonosítók értékeinek összefoglaló táblázata

			Diagnosztikai munkamenetek		
Diagnosztikai szakasz neve	Pont száma	Szolgáltatás-azonosító érték	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Ez a szimbólum azt jelzi, hogy a szolgáltatás kötelező e diagnosztikai munkamenetben.
A szimbólum hiánya azt jelzi, hogy e szolgáltatás nem megengedett e diagnosztikai munkamenetben.

3.2. **Válaszkódok**

Minden szolgáltatáshoz válaszkódokat kell meghatározni.

4. KOMMUNIKÁCIÓS SZOLGÁLTATÁSOK

A kommunikáció létrehozásához és fenntartásához szükség van bizonyos szolgáltatásokra. Ezek nem jelennek meg az alkalmazási rétegen. A rendelkezésre álló szolgáltatásokat a következő táblázat részletezi:

2. táblázat

Kezelési szolgáltatások

A szolgáltatás neve	Leírás
StartCommunication	A kliens kéri egy kommunikációs munkamenet megindítását egy (vagy több) szerverrel.
StopCommunication	A kliens kéri az aktuális kommunikációs munkamenet leállítását.
TesterPresent	A kliens jelzi a szervernek, hogy a kapcsolat még mindig aktív.

CPR_005 A StartCommunication szolgáltatás a kommunikáció elindítására szolgál. Bármilyen szolgáltatás végrehajtása érdekében inicializálni kell a kommunikációt, és a kommunikációs paramétereket a kívánt üzemmódnak megfelelően kell beállítani.

4.1. **A StartCommunication szolgáltatás**

CPR_006 A StartCommunication bejelentésprimitív vétele után a járműegység ellenőrzi, hogy a kért kommunikációs kapcsolat inicializálható-e az aktuális feltételek mellett. A kommunikációs kapcsolat inicializálásának érvényes feltételei az ISO 14230-2 dokumentumban találhatók.

▼B

CPR_007 Ezután a járműegység lefolytat minden olyan tevékenységet, amely a kommunikációs kapcsolat inicializálásához szükséges, és elküld egy StartCommunication válaszprimitívet a kiválasztott pozitívválasz-paraméterekkel együtt.

CPR_008 Amennyiben a már inicializált (és egy diagnosztikai munkamenetbe belépett) járműegység egy új StartCommunication kérést kap (például a vizsgálókészülékben történő hibajavítás következtében), a kérést elfogadja, és sor kerül a járműegység újrainicializálására.

CPR_009 Amennyiben a kommunikációs kapcsolatot bármilyen ok miatt nem lehet inicializálni, úgy a járműegység tovább működik a kommunikációs kapcsolat inicializálási kísérletét közvetlenül megelőző módon.

CPR_010 A StartCommunication kérésüzenetet fizikailag meg kell címezni.

CPR_011 A járműegység szolgáltatások céljából történő inicializálását egy „gyors inicializálási” módszerrel kell elvégezni:

— minden tevékenység előtt van egy buszinaktív idő;

— ezután a vizsgálókészülék elküld egy inicializálási mintát;

— a járműegység válasza tartalmazza az összes olyan információt, amely szükséges a kommunikáció létrehozásához.

CPR_012 Az inicializálás befejezése után:

— az összes kommunikációs paramétert a 4. táblázatban megadott értékekre kell beállítani, a kulcsbájtoknak megfelelően;

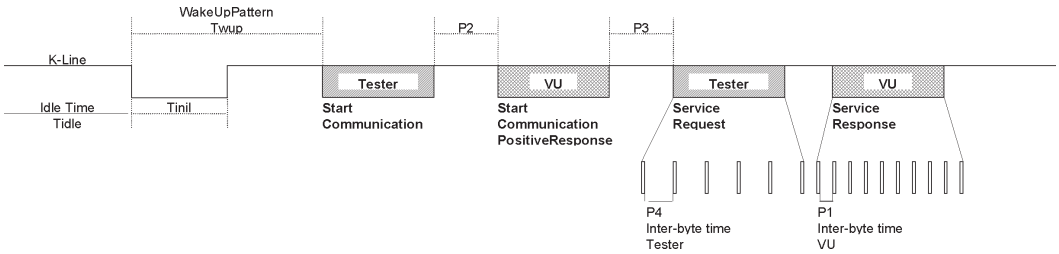
— a járműegység várja a vizsgálókészülék első kérését;

— a járműegység alapértelmezett diagnosztikai üzemmódban, vagyis StandardDiagnosticSession üzemmódban van;

— a kalibrálási I/O jelvonal alapértelmezett állapotban, vagyis dezaktivált állapotban van.

CPR_014 A K-vonal adatáramlási sebességét 10 400 Baudra kell állítani.

CPR_016 A gyors inicializálás úgy indul el, hogy a vizsgálókészülék átküld egy *Wake up pattern*-t (Wup) a K-vonalon. Ez a minta az inaktív idő után kezdődik a K-vonalon, egy alacsony idejű Tinil-lel. A vizsgálókészülék átküldi a StartCommunication szolgáltatás első bitjét egy olyan Twup taktus után kapcsolódva, amely az első lefutó él után kezdődik.



▼B

CPR_017 Az alábbi táblázat részletezi a gyors inicializáláshoz és általában a kommunikációhoz szükséges időértékeket. Az inaktív idő (Tidle) tekintetében három különböző lehetőség képzelhető el:

— első átvitel az áram bekapcsolása után: Tidle = 300 ms.

— a StopCommunication szolgáltatás befejezése után: Tidle = P3 min.

— a kommunikáció megszakítása után, ami az engedélyezett P3 max idő túllépése miatt következett be: Tidle = 0.

3. táblázat

A gyors inicializálás időértékei

Paraméter		Minimumérték	Maximumérték
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

4. táblázat

Kommunikációs időértékek

Idő-paraméter	A paraméterek leírása	Alsó határértékek [ms]	Felső határértékek [ms]
		min.	max.
P1	A bájtok áramlása között eltelt idő a járműegységválasznál.	0	20
P2	A vizsgálókészülék kérése és a járműegység válasza között vagy a járműegység két válasza között eltelt idő	25	250
P3	A járműegység válaszai és a vizsgálókészülék új kérései között eltelt idő	55	5 000
P4	A bájtok áramlása között eltelt idő, a vizsgálókészülék kérésére várva	5	20

CPR_018 A gyors inicializálás üzenetformátumát a következő táblázatok részletezik: (MEGJEGYZÉS: a hex jelentése hexadecimális)

5. táblázat

StartCommunication Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	81	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC

▼B

Bájt #	Paraméter neve	Hex érték	Kódszó
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Ellenőrző összeg	00-FF	CS

6. táblázat

StartCommunication Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	1. kulcsbájt	EA	KB1
#7	2. kulcsbájt	8F	KB2
#8	Ellenőrző összeg	00-FF	CS

CPR_019 Nincs negatív válasz a StartCommunication kérésüzenetre. Ha nincs továbbítandó pozitív válaszüzenet, akkor a járműegység nem inicializált, nincs továbbítandó adat és a VU normál üzemmódban marad.

4.2. **StopCommunication szolgáltatás**

4.2.1 *Az üzenet leírása*

E kommunikációs rétegszolgáltatás célja a kommunikációs munkamenet lezárása.

CPR_020 A StopCommunication bejelentésprimitív vételekor a járműegység ellenőrizi, hogy az aktuális körülmények lehetővé teszik-e e kommunikáció befejezését. Ebben az esetben a járműegység végrehajt minden olyan műveletet, amely e kommunikáció befejezéséhez szükséges.

CPR_021 Ha a kommunikációt be lehet fejezni, a járműegység a kommunikáció befejezése kiadja a StopCommunication válaszprimitívet a kiválasztott pozitívválasz-paraméterek segítségével.

CPR_022 Amennyiben a kommunikációt bármely ok miatt nem lehet befejezni, a járműegység kiadja a StopCommunication válaszprimitívet a kiválasztott negatív válasz-paraméterekkel együtt.

CPR_023 Amennyiben a járműegység P3max időtúllépést észlel, a kommunikációt válaszprimitív kiadása nélkül be kell fejezni.

▼B

4.2.2 *Az üzenet formátuma*

CPR_024 A StopCommunication primitívek üzenetformátumát az alábbi táblázatok részletezik:

7. táblázat

StopCommunication Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Ellenőrző összeg	00-FF	CS

8. táblázat

StopCommunication Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Ellenőrző összeg	00-FF	CS

9. táblázat

StopCommunication Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN

▼B

Bájt #	Paraméter neve	Hex érték	Kódszó
#5	**Negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Ellenőrző összeg	00-FF	CS

4.2.3 *A paraméterek meghatározása*

E szolgáltatáshoz egyetlen paraméter meghatározása sem szükséges.

4.3. **TesterPresent szolgáltatás**

4.3.1 *Az üzenet leírása*

A TesterPresence szolgáltatást a vizsgálókészülék használja, hogy jelezze a szervernek azt, hogy vele továbbra is aktív kapcsolatban van, annak megelőzése érdekében, hogy a szerver automatikusan visszaálljon normál üzemmódra, és esetleg megszakítsa a kommunikációt. E rendszeres időközönként elküldött szolgáltatás aktív állapotban tartja a diagnosztikai munkamenetet/kommunikációt olyan módon, hogy minden szolgáltatáskérésnél visszaállítja a P3 óraregisztert.

4.3.2 *Az üzenet formátuma*

CPR_079 A TesterPresent primitívek üzenetformátumát az alábbi táblázatok részletezik.

10. táblázat

TesterPresent Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**
#6	Alfunkció = responseRequired = [igen	01	RESPREQ_Y
	nem]	02	RESPREQ_NO
#7	Ellenőrző összeg	00-FF	CS

CPR_080 Ha a responseRequired paraméter „igen” értékre van állítva, a szerver a következő pozitív válaszüzenettel felel. Ha „nem” értékre van állítva, a szerver nem küld választ.

▼B

11. táblázat

TesterPresent Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Ellenőrző összeg	00-FF	CS

CPR_081 A szolgáltatás a következő negatív válaszkódokat támogatja:

12. táblázat

TesterPresent Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**Negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Ellenőrző összeg	00-FF	CS

▼B

5. KEZELÉSI SZOLGÁLTATÁSOK

A rendelkezésre álló szolgáltatásokat a következő táblázat részletezi:

13. táblázat

Kezelési szolgáltatások

A szolgáltatás neve	Leírás
StartDiagnosticSession	A kliens diagnosztikai munkamenet elindítását kéri a járműegységgel.
SecurityAccess	A kliens hozzáférést kér a felhatalmazott felhasználók számára fenntartott funkciókhoz.

5.1. **StartDiagnosticSession szolgáltatás**

5.1.1 *Az üzenet leírása*

CPR_025 A StartDiagnosticSession szolgáltatás a különféle diagnosztikai munkamenetek aktiválására szolgál a szerveren. A diagnosztikai munkamenetek engedélyezik a szolgáltatások valamely konkrét összetételét a 17. táblázatnak megfelelően. A munkamenet engedélyezheti a jármű gyártójának speciális szolgáltatásait is, amelyek nem részei e dokumentumnak. A végrehajtási szabályoknak meg kell felelniük a következő követelményeknek:

— Mindig csak pontosan egy diagnosztikai munkamenet lehet aktív a járműegységben,

— A járműegység mindig elindítja a StandardDiagnosticSession munkamenetet, amennyiben az feszültség alá kerül. Ha egyetlen más diagnosztikai munkamenetet sem indítanak el, a StandardDiagnosticSession mindaddig fut, amíg a járműegység feszültség alatt van,

— Ha a vizsgálókészülék olyan diagnosztikai munkamenetet kér, amely már fut, a járműegység pozitív válaszüzenetet küld,

— Amennyiben a vizsgálókészülék új diagnosztikai munkamenetet kér, a járműegység előbb StartDiagnosticSession pozitív válaszüzenetet küld, mielőtt az új munkamenet aktiválódik a járműegységben. Ha a járműegység nem képes elindítani a kért új diagnosztikai munkamenetet, StartDiagnosticSession negatív válaszüzenettel válaszol, és az aktuális munkamenet folytatódik.

CPR_026 A diagnosztikai munkamenet csak akkor indulhat el, miután létrejött a kommunikáció a kliens és a járműegység között.

CPR_027 A 4. táblázatban meghatározott szinkronozási paramétereknek aktívaknak kell lenniük egy sikeres StartDiagnosticSession után, amennyiben a diagnosticSession paraméter „StandardDiagnosticSession” értékre van beállítva a kérésüzenetben, és ha korábban egy másik diagnosztikai munkamenet volt aktív.

5.1.2 *Az üzenet formátuma*

CPR_028 A StartDiagnosticSession primitívek üzenetformátumait az alábbi táblázatok részletezik:

▼B

14. táblázat

StartDiagnosticSession kérés üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = (a 17. táblázat egyik értéke)	xx	DS_…
#7	Ellenőrző összeg	00-FF	CS

15. táblázat

StartDiagnosticSession Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	DiagnosticSession = (megegyezik a 14. táblázat #6 bájt értékével)	xx	DS_…
#7	Ellenőrző összeg	00-FF	CS

16. táblázat

StartDiagnosticSession Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC

▼B

Bájt #	Paraméter neve		Hex érték	Kódszó
#4	Kiegészítőhossz-bájt		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	Response-Code =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
#8	Ellenőrző összeg		00-FF	CS

([a]) – a kérésüzenet #6 bájtjánál beillesztett érték nem támogatott, vagyis nem szerepel a 17. táblázatban,
([b]) – az üzenet hossza rossz,
([c]) – a StartDiagnosticSession kérés kritériumai nem teljesültek.

5.1.3 *A paraméterek meghatározása*

CPR_029 A StartDiagnosticSession szolgáltatás a ***diagnosticSession (DS_)*** paramétert használja a szerver(ek) különleges viselkedésének kiválasztására. E dokumentumban a következő diagnosztikai munkamenetek kerülnek meghatározásra:

17. táblázat

A diagnosticSession értékeinek meghatározása

Hex	Leírás	Kódszó
81	**StandardDiagnosticSession** E diagnosztikai munkamenet az **1. táblázat 4., „SD” oszlopában** meghatározott összes szolgáltatás aktiválását engedélyezi. E szolgáltatások lehetővé teszik adatok leolvasását egy szerverről (járműegység). E diagnosztikai munkamenet azt követően válik aktívvá, miután az inicializálás sikeresen befejeződik a kliens (vizsgálókészülék) és a szerver (járműegység) között. E diagnosztikai munkamenet felülírható az e munkamenetben meghatározott más diagnosztikai munkamenetekkel.	**SD**
85	**ECUProgrammingSession** E diagnosztikai munkamenet az **1. táblázat 6., „ECUPS” oszlopában** meghatározott összes szolgáltatás aktiválását engedélyezi. E szolgáltatások támogatják a szerver (járműegység) memóriájának programozását. E diagnosztikai munkamenet felülírható az e szakaszban meghatározott más diagnosztikai munkamenetekkel.	**ECUPS**

▼B

Hex	Leírás	Kódszó
87	**ECUAdjustmentSession** E diagnosztikai munkamenet az **1. táblázat 5., „ECUAS” oszlopában** meghatározott összes szolgáltatás aktiválását engedélyezi. E szolgáltatások támogatják a szerver (járműegység) input/output vezérlését. E diagnosztikai munkamenet felülírható az e munkamenetben meghatározott más diagnosztikai munkamenetekkel.	**ECUAS**

5.2. **SecurityAccess szolgáltatás**

Kalibrálási adatok beírása csak akkor lehetséges, ha a járműegység KALIBRÁLÁSI üzemmódban van. Egy érvényes műhelykártya járműegységbe történő behelyezése mellett a járműegységbe be kell írni a megfelelő PIN-kódot ahhoz, hogy a KALIBRÁLÁSI üzemmódhoz való hozzáférés biztosítva legyen.

Ha a járműegység KALIBRÁLÁSI vagy ELLENŐRZÉSI üzemmódban van, lehetséges a a kalibrálási input/output vonalhoz való hozzáférés is.

A SecutityAccess szolgáltatás lehetővé teszi a PIN-kód beírását és annak jelzését a vizsgálókészülék számára, hogy a járműegység KALIBRÁLÁSI üzemmódban van-e vagy sem.

A rendszer lehetővé teszi a PIN-kód más módon való bevitelét.

5.2.1 *Az üzenet leírása*

A SecurityAccess szolgáltatás tartalmaz egy SecurityAccess requestSeed üzenetet, amelyet adott esetben egy SecurityAccess sendKey üzenet követ. A SecurityAccess szolgáltatást a StartDiagnosticSession szolgáltatást követően kell végrehajtani.

CPR_033 A vizsgálókészülék a SecurityAccess requestSeed üzenetet használja annak ellenőrzésére, hogy a járműegység készen áll-e a PIN-kód fogadására.

CPR_034 Ha a járműegység már KALIBRÁLÁSI üzemmódban van, akkor úgy válaszol a kérésre, hogy a SecurityAccess kérésre adott pozitív válasz szolgáltatás felhasználásával elküld egy 0x0000 értékű „seed”-et.

CPR_035 Ha a járműegység készen áll a PIN-kód fogadására a műhelykártya ellenőrzése céljából, akkor úgy kell válaszolnia a kérésre, hogy a SecurityAccess kérésre adott pozitívválasz-szolgáltatás felhasználásával elküld egy „seed”-et, amelynek értéke nagyobb mint 0x0000.

CPR_036 Ha a járműegység nem áll készen arra, hogy fogadja a PIN-kódot a vizsgálókészüléktől – vagy azért, mert a behelyezett műhelykártya érvénytelen, vagy azért, mert nem illesztettek be műhelykártyát, vagy pedig azért, mert a járműegység arra számít, hogy más módon fogja megkapni a PIN-kódot –, akkor negatív választ ad a kérésre a conditionsNotCorrectOrRequestSequenceError válaszkód beállításával.

CPR_037 Ezután a vizsgálókészülék adott esetben SecurityAccess sendKey üzenetet használ ahhoz, hogy a PIN-kódot továbbítsa a járműegységnek. Annak érdekében, hogy időt adjon a kártyahitelesítési eljárás végrehajtásához, a járműegység felhasználja a requestCorrectlyReceived-ResponsePending negatív válaszkódot a válaszadási idő meghosszabbításához. A maximális válaszadási idő azonban nem haladhatja meg

▼B

az öt percet. Mihelyt a kért szolgáltatás befejeződik, a járműegység pozitív válaszüzenetet vagy negatív válaszüzenetet küld az említett kódtól eltérő válaszkóddal. A járműegység megismételheti a requestCorrectlyReceived-ResponsePending negatív válaszkódot, amíg a kért szolgáltatás végrehajtása be nem fejeződik, és amíg az utolsó válaszüzenet elküldése meg nem történik.

CPR_038 A járműegység csak akkor válaszol e kérdésre a SecurityAccess Positive Response szolgáltatás felhasználásával, ha KALIBRÁLÁSI üzemmódban van.

CPR_039 A következő esetekben a járműegység negatív választ ad e kérésre a következőképpen beállított válaszkódokkal:

— subFunctionNot supported: az alfunkció paraméterének érvénytelen formátuma (accessType),

— conditionsNotCorrectOrRequestSequenceError: a járműegység nem áll készen a PIN-kód bevitelének fogadására,

— invalidKey: a PIN-kód érvénytelen és a PIN-ellenőrzési kísérletek száma nem került túllépésre,

— exceededNumberOfAttempts: a PIN-kód érvénytelen és a PIN-ellenőrzési kísérletek száma túllépésre került,

— generalReject: A PIN-kód helyes, de a kölcsönös hitelesítés a műhelykártyával sikertelen volt.

5.2.2 *Az üzenetek formátuma – SecurityAccess – requestSeed*

CPR_040 A SecurityAccess requestSeed primitívek üzenetformátumait a következő táblázatok részletezik:

18. táblázat

SecurityAccess Request- requestSeed üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Ellenőrző összeg	00-FF	CS

▼B

19. táblázat

SecurityAccess – requestSeed Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Magas seed	00-FF	SEEDH
#8	Alacsony seed	00-FF	SEEDL
#9	Ellenőrző összeg	00-FF	CS

20. táblázat

SecurityAccess Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Ellenőrző összeg	00-FF	CS

▼B

5.2.3 *Az üzenetek formátuma – SecurityAccess – sendKey*

CPR_041 A SecurityAccess sendKey primitívek üzenetformátumait az alábbi táblázatok részletezik:

21. táblázat

SecurityAccess Request – sendKey üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	m + 2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 – (#m + 6)	Key #1 (Magas) … Key #m (alacsony, az „m” értéke legalább 4, legfeljebb 8)	xx … xx	KEY
#m+7	Ellenőrző összeg	00-FF	CS

22. táblázat

SecurityAccess – sendKey Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Ellenőrző összeg	00-FF	CS

▼B

23. táblázat

SecurityAccess Negative Response üzenet

Bájt #	Paraméter neve		Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés		80	FMT
#2	Célcím-bájt		tt	TGT
#3	Forráscím-bájt		EE	SRC
#4	Kiegészítőhossz-bájt		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSup-ported	12	RC_SFNS
		incorrectMessage-Length	13	RC_IML
		conditionsNotCorrect OrRequestSequence-Error	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOf Attempts	36	RC_ENA
		requestCorrectlyRecei ved-ResponsePen-ding]	78	RC_RCR_RP
#8	Ellenőrző összeg		00-FF	CS

6. ADATÁTVITELI SZOLGÁLTATÁSOK

A rendelkezésre álló szolgáltatásokat a következő táblázat részletezi:

24. táblázat

Adatátviteli szolgáltatások

A szolgáltatás neve	Leírás
ReadDataByIdentifier	A kliens egy rekord aktuális értékének átvitelét kéri a recordDataIdentifier általi hozzáféréssel.
WriteDataByIdentifier	A kliens egy rekord megírását kéri a record-DataIdentifier általi hozzáféréssel.

▼B

6.1. **ReadDataByIdentifier szolgáltatás**

6.1.1 *Az üzenet leírása*

CPR_050 A ReadDataByIdentifier szolgáltatást a kliens arra használja, hogy adatrekordértékeket kérjen egy szervertől. Az adatokat egy recordDataIdentifier azonosítja. A járműegység gyártója tartozik felelősséggel azért, hogy e szolgáltatás igénybevételekor teljesüljenek a szervervonatkozású feltételek.

6.1.2 *Az üzenet formátuma*

CPR_051 A ReadDataIdentifier primitívek üzenetformátumait a következő táblázatok részletezik:

25. táblázat

ReadDataByIdentifier Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 – #7	recordDataIdentifier = [a value from 28]	xxxx	RDI_…
#8	Ellenőrző összeg	00-FF	CS

26. táblázat

ReadDataByIdentifier Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 és #7	recordDataIdentifier = [megegyezik a 25. táblázat #6 és #7 bájtjainak értékével]	xxxx	RDI_…

▼B

Bájt #	Paraméter neve		Hex érték	Kódszó
#8 – (#m+7)	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Ellenőrző összeg		00-FF	CS

27. táblázat

ReadDataByIdentifier Negative Response üzenet

Bájt #	Paraméter neve		Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés		80	FMT
#2	Célcím-bájt		tt	TGT
#3	Forráscím-bájt		EE	SRC
#4	Kiegészítőhossz-bájt		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Ellenőrző összeg		00-FF	CS

6.1.3 *A paraméterek meghatározása*

CPR_052 A ReadDataByIdentifier kérésüzenetben szereplő ***recordDataIdentifier (RDI_)*** paraméter egy adatrekordot azonosít.

CPR_053 Az e dokumentumban meghatározott recordDataIdentifier értékeket az alábbi táblázat mutatja be.

A recordDataIdentifier táblázat négy oszlopból és több sorból áll.

— Az **első oszlop (Hex)** a harmadik oszlopban meghatározott recordDataIdentifierhez hozzárendelt „hex értéket” tartalmazza.

— A **második oszlop (Adatelem)** meghatározza az 1. függeléknek azon adatelemét, amelyen a recordDataIdentifier alapul (adott esetben konvertálás szükséges).

▼B

— A **harmadik oszlop (Leírás)** meghatározza a megfelelő recordDataIdentifier nevét.

— A **negyedik oszlop (Kódszó)** meghatározza az e recordDataIdentifier-hez tartozó kódszót.

28. táblázat

A recordDataIdentifier értékeinek meghatározása

Hex	Adatelem	A recordDataIdentifier megnevezése (a formátumot lásd a 8.2. pontban)	Kódszó
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 A ReadDataByIdentifier pozitív válaszüzenet a ***dataRecord (DREC_)*** paramétert használja a recordDataIdentifier által meghatározott adatrekord érték közlésére a kliens (vizsgálókészülék) felé. Az adatok formátumait a 8. pont részletezi. A felhasználó választása szerint olyan egyéb dataRecords paramétereket is alkalmazni lehet, mint a járműegység különleges input, belső és output adatai, de ezeket e dokumentum nem határozza meg.

6.2. **WriteDataByIdentifier szolgáltatás**

6.2.1 *Az üzenet leírása*

CPR_056 A WriteDataByIdentifier szolgáltatást a kliens arra használja, hogy adatrekordértékeket írjon fel a szerverre. Az adatokat egy recordDataIdentifier azonosítja. A járműegység gyártója tartozik felelősséggel azért, hogy e szolgáltatás igénybevételekor teljesüljenek a szervervonatkozású feltételek. A 28. táblázatban felsorolt paraméterek aktualizálásához a járműegységnek KALIBRÁLÁSI üzemmódban kell lennie.

6.2.2 *Az üzenet formátuma*

CPR_057 A WriteDataByIdentifier primitívek üzenetformátumait az alábbi táblázatok részletezik:

▼B

29. táblázat

WriteDataByIdentifier Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	m+3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 – #7	recordDataIdentifier = [a value from 28]	xxxx	RDI_…
#8 – m + 7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Ellenőrző összeg	00-FF	CS

30. táblázat

WriteDataByIdentifier Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 – #7	recordDataIdentifier = [megegyezik a 29. táblázat #6 és #7 bájtjainak értékével]	xxxx	RDI_…
#8	Ellenőrző összeg	00-FF	CS

▼B

31. táblázat

WriteDataByIdentifier Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI
#7	ResponseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Ellenőrző összeg	00-FF	CS

6.2.3 *A paraméterek meghatározása*

A ***recordDataIdentifier (RDI_)*** paramétert a 28. táblázat határozza meg.

A WriteDataByIdentifier kérésüzenet a ***dataRecord (DREC_)*** paramétert használja arra, hogy közölje a szerverrel (járműegység) a recordDataIdentifier által azonosított adatrekord értékeket. Az adatok formátumait a 8. pont részletezi.

7. A VIZSGÁLATI IMPULZUSOK ELLENŐRZÉSE – INPUT/OUTPUT VEZÉRLŐ FUNKCIONÁLIS EGYSÉG

A rendelkezésre álló szolgáltatásokat a következő táblázat részletezi:

32. táblázat

Input/Output vezérlő funkcionális egység

A szolgáltatás neve	Leírás
InputOutputControlByIdentifier	A kliens a szerverre jellemző inputok/outputok ellenőrzését kéri.

7.1. **InputOutputControlByIdentifier service**

7.1.1 *Az üzenet leírása*

Megfelelő vizsgálókészülék alkalmazásával az elülső csatlakozón keresztül létrejozott kapcsolat lehetővé teszi a vizsgálati impulzusok ellenőrzését vagy megfigyelését.

▼B

CPR_058 E kalibrálási I/O jelvonal egy K-vonali paranccsal, az InputOutputControlByIdentifier szolgáltatás felhasználásával konfigurálható annak érdekében, hogy a vonal tekintetében kiválasztásra kerüljön a kívánt input vagy output funkció. A vonal lehetséges állapotai a következők:

— dezaktivált,

— speedSignalInput, ahol a kalibrálási I/O jelvonalat egy sebességjel (vizsgálati jel) bevitelére kell használni, lecserélve ezzel a mozgásérzékelő sebességjelét (ez a funkció ELLENŐRZÉSI üzemmódban nem áll rendelkezésre),

— realTimeSpeedSignalOutputSensor, ahol a kalibrálási I/O jelvonalat a mozgásérzékelő sebességjelének kimenetére kell használni,

— RTCOutput, ahol a kalibrálási I/O jelvonalat az UTC órajel kimenetére kell használni (ez a funkció ELLENŐRZÉSI üzemmódban nem áll rendelkezésre).

CPR_059 A vonal állapotának konfigurálásához a járműegységnek beállítási munkamenetben kell lennie, és azt KALIBRÁLÁSI vagy ELLENŐRZÉSI üzemmódba kell állítani. Ha a járműegység KALIBRÁLÁSI üzemmódban van, négy vonalállapot áll rendelkezésre (dezaktivált, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Ha a járműegység ELLENŐRZÉSI üzemmódban van, csak két vonalállapot áll rendelkezésre (dezaktivált, realTimeSpeedOutputSensor). A beállítási munkamenetből vagy a KALIBRÁLÁSI vagy ELLENŐRZÉSI üzemmódból való kilépésnél a járműegység gondoskodik arról, hogy a kalibrálási I/O jelvonal visszatérjen a „dezaktivált” (alapértelmezett) állapotba.

CPR_060 Amennyiben sebességimpulzusok érkeznek a járműegység valós idejű sebességjel input vonalára mialatt az I/O jelvonal inputra van állítva, a kalibrálási I/O jelvonalat át kell állítani outputra, vagy vissza kell állítani a dezaktivált állapotba.

CPR_061 A folyamat a következő:

— Kommunikáció létrehozása a StartCommunication szolgáltatás segítségével.

— Beállítási munkamenet megnyitása a StartDiagnosticSession szolgáltatással és belépés KALIBRÁLÁSI vagy ELLENŐRZÉSI üzemmódba (a két művelet sorrendjének nincs jelentősége).

— Átállás output állapotra az InputOutputControlByIdentifier szolgáltatás segítségével.

7.1.2 *Az üzenet formátuma*

CPR_062 Az InputOutputControlByidentifier primitívek üzenetformáit az alábbi táblázatok részletezik:

▼B

33. táblázat

InputOutputControlByIdentifier Request üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	EE	TGT
#3	Forráscím-bájt	tt	SRC
#4	Kiegészítőhossz-bájt	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 és #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 vagy #8 – #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – a 36. táblázat egyik értéke	xx	IOCP_…
	controlState – a 37. táblázat egyik értéke (lásd a lenti megjegyzést)]	xx	CS_…
#9 vagy #10	Ellenőrző összeg	00-FF	CS

Megjegyzés: A controlState paraméter csak bizonyos esetekben szerepel (lásd a 7.1.3. pontot).

34. táblázat

InputOutputControlByIdentifier Positive Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 és #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 vagy #8 – #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (megegyezik a 33. táblázat 8. bájtjának értékével)	xx	IOCP_…
	controlState (megegyezik a 33. táblázat 9. bájtjának értékével)] (adott esetben)	xx	CS_…
#9 vagy #10	Ellenőrző összeg	00-FF	CS

▼B

35. táblázat

InputOutputControlByIdentifier Negative Response üzenet

Bájt #	Paraméter neve	Hex érték	Kódszó
#1	Formátum-bájt – fizikai címzés	80	FMT
#2	Célcím-bájt	tt	TGT
#3	Forráscím-bájt	EE	SRC
#4	Kiegészítőhossz-bájt	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Ellenőrző összeg	00-FF	CS

7.1.3 *A paraméterek meghatározása*

CPR_064 Az ***inputOutputControlParameter (IOCP_)*** paramétert a következő táblázat határozza meg:

36. táblázat

Az inputOutputControlParameter értékeinek meghatározása

Hex	Leírás	Kódszó
00	**ReturnControlToECU** Ezen érték azt jelezi a szerver (járműegység) felé, hogy a vizsgálókészülék már nem vezérli a kalibrálási I/O jelvonalat.	RCTECU
01	**ResetToDefault** Ezen érték azon kérést jelzi a szerver (járműegység) felé, hogy a kalibrálási I/O jelvonalat vissza kell állítani az alapértelmezett állapotába.	RTD

▼B

Hex	Leírás	Kódszó
03	**ShortTermAdjustment** Ezen érték azon kérést jelzi a szerver (járműegység) felé, hogy a kalibrálási I/O jelvonalat be kell állítani a controlState paraméterben foglalt értékre.	STA

CPR_065 A ***controlState*** paraméter csak akkor jelenik meg, ha az inputOutputControlParameter ShortTermAdjustment értékre van beállítva; a paramétert a következő táblázat határozza meg:

37. táblázat

A controlState értékeinek meghatározása

Üzemmód	Hex érték	Leírás
Dezaktiválás	00	Az I/O vonal dezaktivált (alapértelmezett állapot)
Aktiválás	01	A kalibrálási I/O vonal speedSignalInput-ként aktiválva
Aktiválás	02	A kalibrálási I/O vonal realTimeSpeedSignalOutputSensor-ként aktiválva
Aktiválás	03	A kalibrálási I/O vonal mint RTCOutput aktiválva

8. DATARECORDS FORMÁTUMOK

E szakasz a következőket részletezi:

— általános szabályok, amelyeket azon paraméterek tartományaira kell alkalmazni, amelyeket a járműegységről átvisznek a vizsgálókészülékre,

— azon formátumok, amelyeket a 6. pontban leírt adatátviteli szolgáltatások útján továbbított adatok esetében használni kell.

CPR_067 A járműegység támogatja az összes azonosított paramétert.

CPR_068 Azon adatoknak, amelyeket a járműegységről átvisznek a vizsgálókészülékre a kérésüzenetre adott válaszként, mért adatoknak kell lenniük (vagyis a kért paraméter aktuális értéke, amint azt a járműegység mérte vagy megfigyelte).

8.1. **Az átvitt paraméterek tartományai**

CPR_069 A 38. táblázat meghatározza azon tartományokat, amelyeket fel kell használni az átvitt paraméterek érvényességének megállapításához.

CPR_070 A „error indicator” tartományban szereplő értékek lehetővé teszik a járműegység számára annak azonnali jelzését, hogy az adott pillanatban nem állnak rendelkezésre érvényes paraméteradatok a menetíró készülék bizonyos típusú hibái miatt.

CPR_071 A „not available” tartományban szereplő értékek lehetővé teszik a járműegység számára olyan üzenet továbbítását, amely tartalmaz egy olyan paramétert, amely nem áll rendelkezésre vagy nem támogatott az adott modulban. A „not requested” tartományban szereplő értékek lehetővé teszik a járműegység számára parancsüzenet továbbítását, és azon paraméterek meghatározását, amelyekre a fogadó eszköznek nem kell válaszolnia.

▼B

CPR_072 Amennyiben valamely összetevő elem hibája megakadályozza az egyik paraméterre vonatkozó érvényes adatok átvitelét, a 38. táblázatban leírt hibajelzőt kell használni a kérdéses paraméter adatai helyett. Ha azonban a mért vagy számított adatok olyan értéket adnak meg, amely érvényes ugyan, de amely e paraméter meghatározott tartományán kívül esik, nem kell használni a hibajelzőt. Az adatokat a megfelelő minimális vagy maximális paraméterérték felhasználásával kell továbbítani.

38. táblázat

dataRecords tartományok

A tartomány megnevezése	1 bájt (hex érték)	2 bájt (hex érték)	4 bájt (hex érték)	ASCII
Érvényes jel	00 – FA	0000 – FAFF	00000000 – FAFFFFFF	1–254
Paraméter-specifikus indikátor	FB	FB00 – FBFF	FB000000 – FBFFFFFF	nincs
Jövőbeni indikátor bitek számára fenntartott tartomány	FC – FD	FC00 – FDFF	FC000000 – FDFFFFFF	nincs
Hibajelző	FE	FE00 – FEFF	FE000000 – FEFFFFFF	0
Nem áll rendelkezésre vagy nem kérték	FF	FF00 – FFFF	FF000000 – FFFFFFFF	FF

CPR_073 Az ASCII-ben kódolt paraméterek esetében a „*” ASCII karaktert határolójelnek kell fenntartani.

8.2. **dataRecords formátumok**

Az alábbi 39–42. táblázat részletezi azon formátumokat, amelyeket a ReadDataByIdentifier és a WriteDataByIdentifier szolgáltatáson keresztül használni kell.

CPR_074 A 39. táblázat közli a recordDataIdentifier által meghatározott egyes paraméterek hosszát, felbontását és működési tartományát:

39. táblázat

dataRecords formátum

Paraméter neve	Az adat hossza (bájt)	Felbontás	Működési tartomány
TimeDate	8	Részleteket lásd a 40. táblázatban	
HighResolutionTotalVehicle-Distance	4	5 m/bit nyereség, 0 m eltolási érték	0 – 21 055 406 km
Kfactor	2	0,001 impulzus/m/bit nyereség, 0 m eltolási érték	0 – 64,255 impulzus/m
LfactorTyreCircumference	2	$0{,}125\ 10^{-3}$ m/bit nyereség, 0 m eltolási érték	0 – 8,031 m
WvehicleCharacteristicFactor	2	0,001 impulzus/m/bit nyereség, 0 m eltolási érték	0 – 64,255 impulzus/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Részleteket lásd a 41. táblázatban	
SpeedAuthorised	2	1/256 km/h/bit nyereség, 0 m eltolási érték	0 – 250,996 km/h

▼B

Paraméter neve	Az adat hossza (bájt)	Felbontás	Működési tartomány
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Részleteket lásd a 42. táblázatban	
VIN	17	ASCII	ASCII

CPR_075 A 40. táblázat részletezi a TimeDate paraméter különféle bájtjainak formátumait:

40. táblázat

TimeDate részletes formátuma (recordDataIdentifier érték # F90B)

Bájt	A paraméterek meghatározása	Felbontás	Működési tartomány
1	Másodpercek	0,25 s/bit nyereség, 0 s eltolási érték	0 – 59,75s
2	Percek	1 min/bit nyereség, 0 min eltolási érték	0 – 59 min
3	Órák	1 h/bit nyereség, 0 h eltolási érték	0–23 h
4	Hónap	1 hónap/bit nyereség, 0 hónap eltolási érték	1–12 hónap
5	Nap	0,25 nap/bit nyereség, 0 nap eltolási érték (lásd a 41. táblázat alatti megjegyzést)	0,25–31,75 nap
6	Év	1 év/bit nyereség, + 1985 év eltolási érték (lásd a 41. táblázat alatti megjegyzést)	1985–2235 év
7	Helyi idő percértékének eltolási értéke	1 min/bit nyereség, – 125 min eltolási érték	– 59 – + 59 min
8	Helyi idő óraértékének eltolási értéke	1 h/bit nyereség, –125 h eltolási érték	– 23 – + 23 h

CPR_076 A 41. táblázat részletezi a NextCalibrationDate paraméter különféle bájtjainak formátumait:

41. táblázat

NextCalibrationDate részletes formátum (recordDataIdentifier érték # F922)

Bájt	A paraméterek meghatározása	Felbontás	Működési tartomány
1	Hónap	1 hónap/bit nyereség, 0 hónap eltolási érték	1–12 hónap
2	Nap	0,25 nap/bit nyereség, 0 nap eltolási érték (lásd a lenti megjegyzést)	0,25–31,75 nap
3	Év	1 év/bit nyereség, + 1985 év eltolási érték (lásd a lenti megjegyzést)	1985–2235 év

▼B

Megjegyzés a „nap” paraméter használatához:

1) A 0 dátumérték érvénytelen. Az 1, 2, 3, és 4 értékeket a hónap első napjának azonosítására kell használni; az 5, 6, 7 és 8 értékek a hónap második napjának azonosítására szolgálnak; stb.

2) E paraméter nem befolyásolja és nem változtatja meg a fenti órapar-amétert.

Megjegyzés az „év” paraméter használatához:

A 0 érték az 1985. évre vonatkozik; az 1 érték az 1986. évre vonatkozik; stb.

CPR_078 A 42. táblázat részletezi a NextCalibrationDate paraméter különféle bájtjainak formátumait:

42. táblázat

VehicleRegistrationNumber részletes formátum (recordDataIdentifier érték # F97E)

Bájt	A paraméterek meghatározása	Felbontás	Működési tartomány
1	Kódlap (az 1. függeléknek megfelelően)	ASCII	01 – 0 A
2–14	A jármű rendszáma (az 1. függeléknek megfelelően)	ASCII	ASCII

▼B

9. függelék

TÍPUSJÓVÁHAGYÁS A MINIMÁLISAN ELŐÍRT TESZTEK JEGYZÉKE

TARTALOMJEGYZÉK

1. BEVEZETÉS

2. A JÁRMŰEGYSÉGEK MŰKÖDÉSI TESZTJEI

3. A MOZGÁSÉRZÉKELŐ MŰKÖDÉSI TESZTJEI

4. A TACHOGRÁFKÁRTYÁK MŰKÖDÉSI TESZTJEI

5. A KÜLSŐ GNSS-ESZKÖZ TESZTJEI

6. A TÁVOLI KOMMUNIKÁCIÓS ESZKÖZ TESZTJEI

7. A PAPÍR MŰKÖDÉSI TESZTJEI

8. INTEROPERABILITÁSI TESZTEK

1. BEVEZETÉS

1.1. **Típusjóváhagyás**

Az adatrögzítő készülékek (vagy azok alkatrészei) vagy a tachográfkártyák EU-típusjóváhagyása a következő tanúsításokon alapszik:

— **biztonsági tanúsítás** a Common Criteria szabvány előírásainak megfelelően, az e melléklet 10. függelékének teljes mértékben megfelelő biztonsági cél alapján (később kiegészítendő/módosítandó);

— valamely tagállami hatóság által elvégzett **működési tanúsítás**, amely igazolja, hogy a tesztelt elem teljesíti az e mellékletben szereplő követelményeket az általa elvégzett funkciók, a mérési pontosság és a környezetvédelmi jellemzők tekintetében;

— valamely illetékes szerv által elvégzett **interoperabilitási tanúsítás**, amely igazolja, hogy az adatrögzítő készülék (vagy a tachográfkártya) teljes mértékben képes együttműködni a szükséges tachográfkártya-modellekkel (vagy adatrögzítőkészülék-modellekkel) (lásd e melléklet 8. fejezetét).

E függelék azokat a teszteket határozza meg, amelyeket a tagállami illetékes hatóságoknak a működési tesztek, illetve az illetékes szerveknek az interoperabilitási tesztek során minimálisan el kell végezniük. A tesztek elvégzése során követendő eljárások és a tesztek típusai további részletezésre nem kerülnek.

E függelék nem foglalkozik a biztonsági tanúsítás szempontjaival. Ha bizonyos, a típusjóváhagyáshoz szükséges teszteket a biztonsági értékelési és tanúsítási eljárás során elvégeznek, e teszteket nem szükséges megismételni. Ebben az esetben csak e biztonsági tesztek eredményeinek ellenőrzésére lehet szükség. Tájékoztatási célból „*” jelzi e függelékben azon követelményeket, amelyeket a biztonsági tanúsítás során várhatóan tesztelni kell (vagy amelyek a várhatóan végrehajtandó tesztekkel szoros kapcsolatban vannak).

A számozott követelmények a melléklet alapszövegére, az egyéb követelmények pedig a többi függelékre utalnak (pl. a PIC_001 hivatkozás a 3. számú, Piktogramok című függelék PIC_001 számú követelményét jelenti).

E függelék külön tárgyalja a mozgásérzékelőnek, a járműegységnek és a külső GNSS-eszköznek – mint az adatrögzítő készülék alkatrészeinek – típusjóváhagyását. Valamennyi alkatrészre külön típusbizonyítványt kell

▼B

kiállítani, amelyben fel kell tüntetni a többi, ezzel kompatibilis alkatrészt. A mozgásérzékelő (vagy a külső GNSS-eszköz) működési tesztjét a járműegységgel együtt kell elvégezni, és fordítva.

A mozgásérzékelő (illetve a külső GNSS-eszköz) valamennyi modellje és a járműegység valamennyi modellje közötti interoperabilitás megléte nem kötelező. Ebben az esetben a mozgásérzékelő (illetve a külső GNSS-eszköz) típusjóváhagyását csak a vonatkozó járműegység típusjóváhagyásával együtt lehet megadni, és fordítva.

1.2. **Hivatkozások**

E függelékben az alábbi hivatkozások szerepelnek:

IEC 60068-2-1: Környezetállósági vizsgálatok – 2-1. rész: Vizsgálatok – A. vizsgálat: Hideg

IEC 60068-2-2: Alapvető környezetállósági vizsgálati eljárások; 2. rész: vizsgálatok; B. vizsgálatok: száraz meleg (szinuszos).

IEC 60068-2-6: Környezetállósági vizsgálatok – 2. rész: Vizsgálatok – Fc. vizsgálat: Rázás

IEC 60068-2-14: Környezetállósági vizsgálatok – 2-14. rész: Vizsgálatok; N. vizsgálat: Hőmérséklet-változás

IEC 60068-2-27: Környezetállósági vizsgálatok – 2. rész: Vizsgálatok. Ea. vizsgálat és irányelv: Ütés

IEC 60068-2-30: Környezetállósági vizsgálatok – 2-30. rész: Vizsgálatok – Db. vizsgálat: Ciklikus nedves meleg (12+12 órás ciklus)

IEC 60068-2-64: Környezetállósági vizsgálatok – 2-64. rész: Vizsgálatok – Fh. vizsgálat: Széles sávú, véletlenszerű rázás és irányelvei

IEC 60068-2-78: Környezetállósági vizsgálatok – 2-78. rész: Vizsgálatok – Cab. vizsgálat: Tartós nedves meleg

ISO 16750-3: Mechanikus terhelések (2012-12)

ISO 16750-4: Éghajlati terhelések (2010-04)

ISO 20653: Közúti járművek – Védettségi fokozat (IP kód) – Elektromos berendezések idegen tárgyakkal, vízzel és hozzáféréssel szembeni védelme

ISO 10605:2008 + Műszaki helyesbítés: 2010 + AMD1:2014 Közúti járművek – Az elektromos kisülésből adódó elektromos zavarokra vonatkozó vizsgálati módszerek

ISO 7637-1:2002 + AMD1: 2008 Közúti járművek – Vezetésből és csatolásból adódó elektromos zavarok – 1. rész: Fogalommeghatározások és általános szempontok

ISO 7637-2 Közúti járművek – Vezetésből és csatolásból adódó elektromos zavarok – 2. rész: Elektromos tranziens vezetés csak a tápvezetékek mentén

ISO 7637-3 Közúti járművek – Vezetésből és csatolásból adódó elektromos zavarok – 3. rész: Elektromos tranziens vezetés a nem tápvezetéknek számító vezetékek kapacitív és induktív csatolásai mentén

ISO/IEC 7816-1 Azonosító kártyák – Érintkezős, integrált áramkörös kártyák – 1. rész: Fizikai jellemzők

▼B

ISO/IEC 7816-2 Információtechnológia – Azonosító kártyák – Érintkezős, integrált áramkörös kártyák – 2. rész: Az érintkezők méretei és elhelyezkedése

ISO/IEC 7816-3 Információtechnológia – Azonosító kártyák – Érintkezős, integrált áramkörös kártyák – 3. rész: Elektronikus jelek és adatátviteli protokoll

ISO/IEC 10373-1: 2006 + AMD1:2012 Azonosító kártyák – Vizsgálati módszerek – 1. rész: Általános jellemzők

ISO/IEC 10373-3: 2010 + Műszaki helyesbítés: 2013 Azonosító kártyák – Vizsgálati módszerek – 3. rész: Intelligens kártyák érintkezőkkel és a kapcsolódó interfészberendezések

ISO 16844-3:2004, Jav. 1:2006 Közúti járművek – Menetíró rendszerek – 3. rész: Mozgásérzékelő-interfész (járműegységekkel)

ISO 16844-4 Közúti járművek – Menetíró rendszerek – 4. rész: CAN interfész

ISO 16844-6 Közúti járművek – Menetíró rendszerek – 6. rész: Diagnosztika

ISO 16844-7 Közúti járművek – Menetíró rendszerek – 7. rész: Paraméterek

ISO 534 Papír és karton – A vastagság, a sűrűség és a fajlagos térfogat meghatározása

10. sz. ENSZ EGB-előírás Egységes rendelkezések gépjárművek elektromágneses összeférhetőségük tekintetében történő jóváhagyásáról (az Egyesült Nemzetek Európai Gazdasági Bizottsága)

2. A JÁRMŰEGYSÉGEK MŰKÖDÉSI TESZTJEI

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
1.2.	Gyártói teszteredmények	Az integráció során elvégzett gyártói teszt eredménye. Dokumentumalapú igazolás.	88, 89, 91
2.	**Szemrevételezés**		
2.1.	A dokumentációnak való megfelelés		
2.2.	Azonosítás/jelölések		224–226
2.3.	Anyagok		219–223
2.4.	Plombálás		398, 401–405
2.5.	Külső interfészek		
3.	**Működési tesztek**		
3.1.	Elérhető funkciók		03, 04, 05, 07, 382
3.2.	Üzemmódok		09–11*, 132, 133
3.3.	Funkciók és adat-hozzáférési jogok		12* 13*, 382, 383, 386–389
3.4.	A kártya behelyezésének és kivételének nyomon követése		15, 16, 17, 18, 19*, 20*, 132
3.5.	Sebesség-és távolságmérés		21–31

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
3.6.	Időmérés (20 °C hőmérsékleten elvégzett vizsgálat)		38–43
3.7.	A járművezető tevékenységének nyomon követése		44–53, 132
3.8.	A járművezetési állapot nyomon követése		54, 55, 132
3.9.	Manuálisan bevitt adatok		56–62
3.10.	A vállalkozás általi lezárás kezelése		63–68
3.11.	Az ellenőrzési tevékenység nyomon követése		69, 70
3.12.	Események és/vagy hibák észlelése		71–88, 132
3.13.	Készülékazonosítási adatok		93*, 94*, 97, 100
3.14.	A járművezetői kártya behelyezési és kivételi adatai		102*–104*
3.15.	A járművezető tevékenységére vonatkozó adatok		105*–107*
3.16.	Hely- és helyzetadatok		108*–112*
3.17.	A kilométer-számláló adatai		113*–115*
3.18.	Részletes sebességadatok		116*
3.19.	Eseményadatok		117*
3.20.	Hibaadatok		118*
3.21.	Kalibrálási adatok		119*–121*
3.22.	Időbeállítási adatok		124*, 125*
3.23.	Az ellenőrzési tevékenységgel kapcsolatos adatok		126*, 127*
3.24.	A vállalkozás általi lezárással kapcsolatos adatok		128*
3.25.	Tevékenységadatok letöltése		129*
3.26.	Különleges körülményekre vonatkozó adatok		130*, 131*
3.27.	Rögzítés és tárolás a tachográfkártyán		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28.	Kijelzés		90, 132, 149–166 PIC_001, DIS_001
3.29.	Nyomtatás		90, 132, 167–179, PIC_001, PRT_001–PRT_014
3.30.	Figyelmeztetés		132, 180–189, PIC_001
3.31.	Adatletöltés külső adathordozókra		90, 132, 190–194
3.32.	Távoli kommunikáció a célzott közúti ellenőrzések céljára		195–197
3.33.	Kimeneti adatok kiegészítő külső eszközökre		198, 199

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
3.34.	Kalibrálás		202–206*, 383, 384, 386–391
3.35.	Közúti kalibrálási ellenőrzés		207–209
3.36.	Időbeállítás		210–212*
3.37.	A kiegészítő funkciók zavarmentessége		06, 425
3.38.	Mozgásérzékelő-interfész		02, 122
3.39.	Külső GNSS-eszköz		03, 123
3.40.	Meg kell bizonyosodni arról, hogy a járműegység észleli, feljegyzi és tárolja a járműegység gyártója által meghatározott esemény(eke)t és/vagy hibá(ka)t, amikor a párosított mozgásérzékelő reagál a jármű mozgásának érzékelését zavaró mágneses terekre.		217
3.41.	Titkosítási eszközkészlet (cypher suite) és szabványos tartományparaméterek		CSM_48, CSM_50
4.	**Környezetállósági tesztek**		
4.1.	Hőmérséklet	Működés-ellenőrzés az alábbiak révén: Az ISO 16750-4 szabvány 5.1.1.2. fejezete szerinti vizsgálat: működési vizsgálat alacsony hőmérsékleten (72 óra –20 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-1: Környezetállósági vizsgálatok – 2-1. rész: Vizsgálatok – A. vizsgálat: Hideg Az ISO 16750-4 szabvány 5.1.2.2. fejezete szerinti vizsgálat: működési vizsgálat magas hőmérsékleten (72 óra 70 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-2: Alapvető környezetállósági vizsgálati eljárások; 2. rész: vizsgálatok; B. vizsgálatok: száraz meleg Az ISO 16750-4 szabvány 5.3.2. fejezete szerinti vizsgálat: gyors hőmérséklet-változás meghatározott átmeneti időszakokkal (– 20 °C/70 °C, 20 ciklus, 2 órás tartózkodási idő mindegyik hőmérsékleten) A legalacsonyabb és a legmagasabb feltüntetett hőmérsékleten és a hőmérsékleti ciklusok alatt csökkentett számú teszt végezhető (az e táblázat 3. részében meghatározottak közül).	213
4.2.	Páratartalom	Ellenőrizni kell, hogy a járműegység ellenáll-e a ciklikus párásodásnak (hőellenállási vizsgálat) az IEC 60068-2-30 szabvány szerinti Db. vizsgálattal a következő feltételek mellett: hat 24 órás ciklus, minden ciklusban + 25 °C és + 55 °C között változó hőmérséklet, a relatív páratartalom 97 % + 25 °C-on és 93 % + 55 °C-on.	214

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
4.3.	Mechanikai	1. Szinuszos rezgés: annak ellenőrzése, hogy a járműegység ellenáll-e az alábbi jellemzőkkel rendelkező szinuszos rezgésnek: állandó kitérés 5 és 11 Hz között: 10 mm-es csúcs állandó gyorsulás 11 és 300 Hz között: 5g E követelményt az IEC 60068-2-6 szabvány Fc. vizsgálatával kell ellenőrizni, e vizsgálat minimális időtartama 3 × 12 óra (tengelyenként 12 óra). Az ISO 16750-3 szabvány a leválasztott vezetőfülkében található eszközökre nem írja elő a szinuszos rezgés vizsgálatát. 2. Véletlenszerű rezgés: Az ISO 16750-3 szabvány 4.1.2.8. fejezete szerinti vizsgálat: VIII. vizsgálat: Haszonjármű leválasztott vezetőfülkével A véletlenszerű rezgés vizsgálata, 10–2 000 Hz, függőleges RMS: 21,3 m/s^2, hosszirányú RMS: 11,8 m/s^2, oldalirányú RMS: 13,1 m/s^2, 3 tengely, 32 óra tengelyenként, beleértve a – 20 °C – 70 °C-os hőmérsékleti ciklust. Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-64: Környezetállósági vizsgálatok – 2-64. rész: Vizsgálatok – Fh. vizsgálat: Széles sávú, véletlenszerű rázás és irányelvei 3. Ütések: mechanikai ütés 3g-s félszinusszal az ISO 16750 szabvány szerint. A fent leírt teszteket a tesztelt készüléktípus különböző mintáin kell elvégezni	219
4.4.	Víz és idegen testek elleni védelem	Az ISO 20653 szabvány szerinti vizsgálat: Közúti járművek – Védettségi fokozat (IP kód) – Elektromos berendezések idegen tárgyakkal, vízzel és hozzáféréssel szembeni védelme (Változatlan paraméterek); IP legkisebb értéke: 40	220, 221
4.5.	Túlfeszültség-védelem	Ellenőrizni kell, hogy a járműegység ellenáll-e az alábbi feszültségeknek: 24 V-os modellek esetében: 34 V + 40 °C mellett 1 órán át 12 V-os modellek esetében: 17 V + 40 °C mellett 1 órán át (ISO 16750-2)	216

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
4.6.	Fordított polaritás elleni védelem	Ellenőrizni kell, hogy a járműegység ellenáll-e az áramellátás megfordításának. (ISO 16750-2)	216
4.7.	Rövidzárlat-védelem	Ellenőrizni kell, hogy a bemeneti-kimeneti jelek védettek-e az áramellátás felőli rövidzárlattal és a földzárlattal szemben. (ISO 16750-2)	216
5.	**Elektromágneses összeférhetőségi tesztek**		
5.1.	Sugárzáskibocsátás és szuszceptibilitás	A 10. sz. ENSZ EGB-előírásnak való megfelelés	218
5.2.	Elektromos kisülés	Az ISO 10605:2008 + szabványnak való megfelelés: műszaki helyesbítés: 2010 + AMD1:2014: +/– 4 kV az érintkezési és +/– 8 kV a légköri kisülés vonatkozásában	218
5.3.	Vezetett tranziens szuszceptibilitás az áramellátáson	A 24 V-os modellek esetében: az ISO 7637-2 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1a. impulzus: Vs = – 450 V Ri = 50 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 20 V Ri = 0,05 ohm 3a. impulzus: Vs = – 150 V Ri = 50 ohm 3b. impulzus: Vs = + 150 V Ri = 50 ohm 4. impulzus: Vs = – 16V Va = – 12V t6 = 100ms 5. impulzus: Vs = + 120V Ri = 2,2 ohm td = 250ms A 12 V-os modellek esetében: az ISO 7637-1 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1. impulzus: Vs = – 75 V Ri = 10 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 10 V Ri = 0,05 ohm 3a. impulzus: Vs = – 112 V Ri = 50 ohm 3b. impulzus: Vs = + 75 V Ri = 50 ohm 4. impulzus: Vs = – 6V Va = – 5V t6 = 15 ms 5. impulzus: Vs = + 65V Ri = 3 ohm td = 100 ms Az 5. impulzust csak azon járműegységeken kell tesztelni, amelyeket olyan járművekbe szerelnek be, amelyeknél nem alkalmaznak túlfeszültség elleni közös külső védelmet. A túlfeszültséggel kapcsolatos javaslat tekintetében lásd az ISO 16750-2 szabvány 4. kiadásának 4.6.4. fejezetét.	218

▼B

3. A MOZGÁSÉRZÉKELŐ MŰKÖDÉSI TESZTJEI

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
2.	**Szemrevételezés**		
2.1.	A dokumentációnak való megfelelés		
2.2.	Azonosítás/jelölések		225, 226,
2.3	Anyagok		219–223
2.4.	Plombálás		398, 401–405
3.	**Működési tesztek**		
3.1.	Az érzékelő azonosítási adatai		95–97*
3.2.	A mozgásérzékelő és a járműegység párosítása		122*, 204
3.3.	Mozgásészlelés A mozgás mérésének pontossága		30–35
3.4.	Járműegység-interfész		02
3.5.	Ellenőrizni kell, hogy a mozgásérzékelő védett-e az állandó mágneses térrel szemben. Alternatív megoldásként ellenőrizni kell, hogy a mozgásérzékelő úgy reagál-e a járműmozgás érzékelését zavaró állandó mágneses terekre, hogy a csatlakoztatott járműegység képes legyen észlelni, rögzíteni és tárolni az érzékelőhibákat		217
4.	**Környezetállósági tesztek**		
4.1.	Üzemi hőmérséklet	A működés ellenőrzése (a 3.3. tesztben meghatározottak szerint) a [– 40 °C – + 135 °C] hőmérsékleti tartományban, a következő vizsgálatok végrehajtásával: az IEC 60068-2-1 szabvány szerinti Ad. vizsgálat, 96 órás időtartammal, a To_{min} legalacsonyabb hőmérsékleten, az IEC 60068-2-2 szabvány szerinti Bd. vizsgálat, 96 órás időtartammal, a To_{max} legmagasabb hőmérsékleten Az ISO 16750-4 szabvány 5.1.1.2. fejezete szerinti vizsgálat: működési vizsgálat alacsony hőmérsékleten (24 óra – 40 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-1: Környezetállósági vizsgálatok – 2-1. rész: Vizsgálatok – A. vizsgálat: Hideg. Az IEC 68-2-2 szabvány szerinti Bd. vizsgálat, 96 órás időtartammal, – 40 °C legalacsonyabb hőmérsékleten. Az ISO 16750-4 szabvány 5.1.2.2. fejezete szerinti vizsgálat: működési vizsgálat magas hőmérsékleten (96 óra 135 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-2: Alapvető környezetállósági vizsgálati eljárások; 2. rész: vizsgálatok; B. vizsgálatok: száraz meleg	213

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
4.2.	Hőmérsékleti ciklusok	Az ISO 16750-4 szabvány 5.3.2. fejezete szerinti vizsgálat: gyors hőmérséklet-változás meghatározott átmeneti időszakokkal (– 40 °C/ 135 °C, 20 ciklus, 30 perces tartózkodási idő mindegyik hőmérsékleten) IEC 60068-2-14: Környezetállósági vizsgálatok; 2-14. rész: Vizsgálatok; N. vizsgálat: Hőmérséklet-változás	213
4.3.	Párásodási ciklusok	A működés ellenőrzése (a 3.3. sz. tesztben meghatározottak alapján) az IEC 60068-2-30 szabvány szerinti Db. vizsgálattal a következő feltételek mellett: hat 24 órás ciklus, minden ciklusban + 25 °C és + 55 °C között változó hőmérséklet, a relatív páratartalom 97 % + 25 °C-on és 93 % + 55 °C-on.	214
4.4.	Rezgés	ISO 16750-3: 4.1.2.6. fejezet: VI. vizsgálat: Haszonjármű, motor, sebességváltó Vegyes rezgésvizsgálat, beleértve a következőket: a) Szinuszos rezgés vizsgálata, 20–520 Hz, 11,4–120 m/s^2, <= 0,5 oktáv/perc b) Véletlenszerű rezgés vizsgálata, 10–2 000 Hz, RMS: 177 m/s^2 94 óra tengelyenként, beleértve a – 20 °C – 70 °C-os hőmérsékleti ciklust Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-80: Környezetállósági vizsgálatok – 2-80. rész: Vizsgálatok – Fi. vizsgálat: Rezgés – vegyes mód	219
4.5.	Mechanikai ütés	ISO 16750-3: 4.2.3. fejezet: VI. vizsgálat: A sebességváltóban vagy a sebességváltón található berendezések vizsgálata félszinuszos ütés, később megállapítandó gyorsulás a 3 000–15 000 m/s^2-es tartományban, később megállapítandó, de 1 ms-nél rövidebb impulzusidő, ütések száma: később megállapítandó Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-27: Környezetállósági vizsgálatok. 2. rész: Vizsgálatok. Ea. vizsgálat és irányelv: Ütés	219
4.6.	Víz és idegen testek elleni védelem	Az ISO 20653 szabvány szerinti vizsgálat: Közúti járművek – Védettségi fokozat (IP kód) – Elektromos berendezések idegen tárgyakkal, vízzel és hozzáféréssel szembeni védelme (IP célértéke: 64)	220, 221
4.7.	Fordított polaritás elleni védelem	Ellenőrizni kell, hogy a mozgásérzékelő ellenáll-e az áramellátás megfordításának.	216
4.8.	Rövidzárlat-védelem	Ellenőrizni kell, hogy a bemeneti-kimeneti jelek védettek-e az áramellátás felőli rövidzárlattal és a földzárlattal szemben.	216

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
5.	**Elektromágneses összeférhetőség**		
5.1.	Sugárzáskibocsátás és szuszceptibilitás	A 10. sz. ENSZ EGB-előírásnak való megfelelés ellenőrzése	218
5.2.	Elektromos kisülés	Az ISO 10605:2008 + szabványnak való megfelelés: műszaki helyesbítés: 2010 + AMD1:2014: +/– 4 kV az érintkezési és +/– 8 kV a légköri kisülés vonatkozásában	218
5.3.	Vezetett tranziens szuszceptibilitás az adatvezetékeken	A 24 V-os modellek esetében: az ISO 7637-2 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1a. impulzus: Vs = – 450 V Ri = 50 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 20 V Ri = 0,05 ohm 3a. impulzus: Vs = – 150 V Ri = 50 ohm 3b. impulzus: Vs = + 150 V Ri = 50 ohm 4. impulzus: Vs = – 16V Va = – 12V t6 = 100 ms 5. impulzus: Vs = + 120V Ri = 2,2 ohm td = 250 ms A 12 V-os modellek esetében: az ISO 7637-1 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1. impulzus: Vs = – 75 V Ri = 10 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 10 V Ri = 0,05 ohm 3a. impulzus: Vs = – 112 V Ri = 50 ohm 3b. impulzus: Vs = + 75 V Ri = 50 ohm 4. impulzus: Vs = – 6V Va = – 5V t6 = 15 ms 5. impulzus: Vs = + 65 V Ri = 3 ohm td = 100 ms Az 5. impulzust csak azon járműegységeken kell tesztelni, amelyeket olyan járművekbe szerelnek be, amelyeknél nem alkalmaznak túlfeszültség elleni közös külső védelmet. A túlfeszültséggel kapcsolatos javaslat tekintetében lásd az ISO 16750-2 szabvány 4. kiadásának 4.6.4. fejezetét.	218

4. A TACHOGRÁFKÁRTYÁK MŰKÖDÉSI TESZTJEI

Az e szakasz (4. szakasz) szerinti, következő teszteket:

5. Protokolltesztek

6. A kártya struktúrája

7. Működési tesztek

az értékelő vagy a tanúsító elvégezheti a chipmodulnak a Common Criteria szabvány szerinti biztonsági tanúsítási eljárása során.

A 2.3. és a 4.2. teszt azonos. Ezek a kártyatest és a chipmodul kombinációjának mechanikai tesztjei. Ha ezen alkotóelemek valamelyikét (a kártyatestet vagy a chipmodult) módosítják, akkor el kell végezni ezeket a teszteket.

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
2.	**Kártyatest**		
2.1.	Nyomtatott minta	Ellenőrizni kell, hogy az összes védelmi jellemzőt és látható adatot helyesen nyomtatták-e a kártyára, és ezek megfelelők-e. [Megjelölés] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 227) Az elülső oldalnak a következőket kell tartalmaznia: a kártya típusának megfelelően a „Járművezetői kártya” vagy „Ellenőrzőkártya” vagy „Műhelykártya” vagy „Vállalkozáskártya” szavak nagybetűvel írva a kártyát kiállító tagállam hivatalos nyelvén vagy nyelvein. [A tagállam neve] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 228) Az elülső oldalnak a következőket kell tartalmaznia: a kártyát kiállító tagállam neve (opcionális). [Jel] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 229) Az elülső oldalnak a következőket kell tartalmaznia: a kártyát kiállító tagállam megkülönböztető jele, kék négyszögben, negatívan nyomtatva, 12 sárga csillaggal körülvéve. [Felsorolás] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 232) A hátsó oldalnak a következőket kell tartalmaznia: a kártya elülső oldalán feltüntetett számozott adatok magyarázata. [Szín] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 234) A tachográfkártyákat a következő fő háttérszínekkel kell nyomtatni: — járművezetői kártya: fehér, — műhelykártya: piros, — ellenőrzőkártya: kék, — vállalkozáskártya: sárga.	227–229, 232, 234–236

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Biztonság] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 235) A tachográfkártyákat a hamisítás és a jogosulatlan változtatások ellen legalább a következőkkel kell ellátni: — biztonsági háttérnyomtatás, finom gilosmintával és írisznyomtatással, — legalább egy kétszínű mikronyomtatású sor.	
		[Jelölések] (1C. melléklet, 4.1. fejezet: „Látható adatok”, 236) A tagállamok kiegészítő színeket és jelöléseket is használhatnak, például nemzeti szimbólumukat vagy biztonsági elemeket.	
		[Jóváhagyási jel] A tachográfkártyákon fel kell tüntetni a jóváhagyási jelet. A jóváhagyási jelnek a következőkből kell állnia: — egy téglalap, amelyben egy „e” betű szerepel, amelyet a jóváhagyást megadó ország megkülönböztető száma vagy betűje követ, — a jóváhagyási szám, amely megegyezik a tachográfkártya típusbizonyítványának számával, és amely tetszés szerinti helyen helyezendő el a téglalap közvetlen közelében.	
2.2.	Mechanikai tesztek	[A kártya mérete] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [5] A kártya térbeli kiterjedése, [5.1] Méret, [5.1.1] Méretek és tűrések, ID-1 típusú, nem használt kártya	240–243 ISO/IEC 7810
		[A kártya szélei] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [5] A kártya térbeli kiterjedése, [5.1] Méret, [5.1.2] A kártya szélei	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[A kártya szerkezete] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [6] A kártya szerkezete	
		[A kártya anyaga] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [7] A kártya anyaga	
		[Hajlítómerevség] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.1] Hajlítómerevség	
		[Toxicitás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.3] Toxicitás	
		[Vegyi anyagokkal szembeni ellenálló képesség] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.4] Vegyi anyagokkal szembeni ellenálló képesség	
		[A kártya szilárdsága] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.5] A kártya méreteinek tartóssága, a kártya deformációja hőmérséklet és páratartalom hatására	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Fény] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.6] Fény	
		[Tartósság] (1C. melléklet, 4.4. fejezet: „Környezeti és elektromos előírások”, 241) A tachográfkártyáknak öt éven át rendeltetésszerűen kell működniük, amennyiben a környezeti és elektromos előírásoknak megfelelően használják őket.	
		[Rétegszilárdság] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.8] Rétegszilárdság	
		[Adhézió vagy tapadás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.9] Adhézió vagy tapadás	
		[Deformáció] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.11] A kártya általános deformációja	
		[Hőállóság] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.12] Hőállóság	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Felületi torzulások] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.13] Felületi torzulások	
		[Szennyeződés] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810 Azonosító kártyák – Fizikai jellemzők, [8] A kártya tulajdonságai [8.14] Szennyeződés és a kártya alkotóelemei közötti interakció	
2.3.	Mechanikai tesztek beépített chipmodul esetében	[Hajlítás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.2] Dinamikus hajlítófeszültség Az összes hajlítási ciklus száma: 4 000	ISO/IEC 7810
		[Csavarás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.3] Dinamikus csavarófeszültség Az összes csavarási ciklus száma: 4 000	
3.	**Modul**		
3.1.	Modul	A modul a chip tokját és az érintkezőlemezt foglalja magában.	ISO/IEC 7816
		[Felületi profil] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7816-1:2011, Azonosító kártyák – Integrált áramkörös kártyák – 1. rész: Érintkezőkkel rendelkező kártyák – Fizikai jellemzők [4.2] Az érintkezők felületi profilja	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Mechanikai szilárdság] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7816-1:2011, Azonosító kártyák – Integrált áramkörös kártyák – 1. rész: Érintkezőkkel rendelkező kártyák – Fizikai jellemzők [4.3] Mechanikai szilárdság (a kártyák és az érintkezők tekintetében)	
		[Elektromos ellenállás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7816-1:2011, Azonosító kártyák – Integrált áramkörös kártyák – 1. rész: Érintkezőkkel rendelkező kártyák – Fizikai jellemzők [4.4] Elektromos ellenállás (az érintkezők tekintetében)	
		[Méretek] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7816-2:2007, Azonosító kártyák – Integrált áramkörös kártyák – 2. rész: Érintkezőkkel rendelkező kártyák – Az érintkezők méretei és elhelyezkedése [3] Az érintkezők méretei	
		[Elhelyezkedés] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7816-2:2007, Azonosító kártyák – Integrált áramkörös kártyák – 2. rész: Érintkezőkkel rendelkező kártyák – Az érintkezők méretei és elhelyezkedése [4] Az érintkezők száma és elhelyezkedése A hat érintkezővel rendelkező modulok esetében a C4 és C8 számú érintkezőkre nem vonatkozik ez a tesztkövetelmény.	
4.	**Chip**		
4.1.	Chip	[Üzemi hőmérséklet A tachográfkártya chipjének – 25 °C és + 85 °C közötti környezeti hőmérsékleti tartományon belül kell működnie.	241–244 10. sz. ENSZ EGB-előírás ISO/IEC 7810 ISO/IEC 10373

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Hőmérséklet és páratartalom] (1C. melléklet, 4.4. fejezet: „Környezeti és elektromos előírások”, 241) A tachográfkártyáknak rendeltetésszerűen kell működniük a Közösség területén rendszerint előforduló éghajlati viszonyok között, és legalább a – 25 °C-tól + 70 °C-ig terjedő hőmérséklet-tartományban, + 85 °C-os esetenkénti csúcsokkal; az „esetenkénti” kifejezés legfeljebb 4 órás időtartamot és a kártya élettartama alatt legfeljebb 100 alkalmat jelent. A tachográfkártyákat egymást követő lépésekben a meghatározott ideig kell kitenni az alábbi hőmérsékleteknek és páratartalmaknak. Minden lépés után tesztelni kell a tachográfkártyák elektromos működését. 1. – 20 °C 2 órán át 2. +/– 0 °C 2 órán át 3. + 20 °C, 50 % relatív páratartalom 2 órán át 4. + 50 °C, 50 % relatív páratartalom 2 órán át 5. + 70 °C, 50 % relatív páratartalom 2 órán át A hőmérsékletet szakaszosan +85 °C-ra kell emelni, és 60 percig ezen a szinten kell tartani 50 % relatív páratartalom mellett. 6. 70 °C, 85 % relatív páratartalom 2 órán át A hőmérsékletet szakaszosan + 85 °C-ra kell emelni, és 30 percig ezen a szinten kell tartani 85 % relatív páratartalom mellett.	
		[Páratartalom] (1C. melléklet, 4.4. fejezet: „Környezeti és elektromos előírások”, 242) A tachográfkártyáknak a 10 %-tól 90 %-ig terjedő páratartalom-tartományban rendeltetésszerűen kell működniük.	
		[Elektromágneses összeférhetőség] (1C. melléklet, 4.4. fejezet: „Környezeti és elektromos előírások”, 244) A működés során a tachográfkártyáknak teljesíteniük kell a 10. sz. ENSZ EGB-előírásban foglalt, az elektromágneses összeférhetőségre vonatkozó követelményeket.	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		[Statikus elektromosság] (1C. melléklet, 4.4. fejezet: „Környezeti és elektromos előírások”, 244) Működés közben a tachográfkártyáknak elektromos kisülés elleni védelemmel kell rendelkezniük. A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.4] Statikus elektromosság [9.4.1] Érintkezőkkel rendelkező kártyák Vizsgálati feszültség: 4 000 V	
		[Röntgensugár] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.1] Röntgensugár	
		[Ultraibolya fény] ISO/IEC 10373-1:2006, Azonosító kártyák – Vizsgálati módszerek – 1. rész: Általános jellemzők [5.11] Ultraibolya fény	
		[Háromkerekes vizsgálat] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 10373-1:2006/Amd. 1:2012, Azonosító kártyák – Vizsgálati módszerek – 1. rész: Általános jellemzők, 1. módosítás [5.22] Intelligens kártyák – Mechanikai szilárdság: Az érintkezőkkel rendelkező intelligens kártyák háromkerekes vizsgálata	
		[Burkolat] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: A burkolat tartósságának vizsgálata [13.2.1.32] TM-422: Mechanikai megbízhatóság: A burkolat vizsgálata	

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
4.2.	Mechanikai tesztek a kártyatestbe épített chipmodul esetében > ugyanaz, mint a 2.3. pontban	[Hajlítás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.2] Dinamikus hajlítófeszültség Az összes hajlítási ciklus száma: 4 000 [Csavarás] A tachográfkártyáknak teljesíteniük kell a következő szabvány követelményeit: ISO/IEC 7810:2003/Amd. 1:2009 Azonosító kártyák – Fizikai jellemzők, 1. módosítás: Az integrált áramkört tartalmazó kártyákra vonatkozó kritériumok [9.3] Dinamikus csavarófeszültség Az összes csavarási ciklus száma: 4 000	ISO/IEC 7810
5.	**Protokolltesztek**		
5.1.	ATR	Az ATR megfelelőségének ellenőrzése	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2.	T=0	A T=0 protokoll megfelelőségének ellenőrzése	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3.	PTS	A PTS parancs megfelelőségének ellenőrzése a T=1-nek a T=0-ra való átállításával	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4.	T=1	A T=1 protokoll megfelelőségének ellenőrzése	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6.	**A kártya szerkezete**		
6.1.		Ellenőrizni kell, hogy a kártya fájlszerkezete megfelelő-e a kötelező fájlok meglétének és azok hozzáférési feltételeinek ellenőrzésével.	TCS_22-től TCS_28-ig TCS_140-től TCS_179-ig
7.	**Működési tesztek**		
7.1.	Normál feldolgozás	Legalább egyszer tesztelni kell valamennyi parancs valamennyi megengedett használatát (pl.: az UPDATE BINARY parancs tesztelése CLA = ‘00’, CLA = ‘0C’ mellett és különböző P1, P2 és Lc paraméterekkel). Ellenőrizni kell, hogy a műveletek végrehajtása valóban megtörtént-e a kártyán (pl. azon fájl olvasásával, amelyen a parancs végrehajtásra került).	TCS_29-től TCS_139-ig

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
7.2.	Hibaüzenetek	Legalább egyszer tesztelni kell valamennyi hibaüzenetet (a 2. függelékben megadottak szerint) valamennyi parancs esetében. Legalább egyszer tesztelni kell valamennyi általános hibát (a biztonsági tanúsítás során ellenőrzött '**6400**' integritási hibák kivételével).	
7.3.	Titkosítási eszközkészlet (cypher suite) és szabványos tartományparaméterek		CSM_48, CSM_50
8.	**Személyre szabás**		
8.1.	Optikai személyre szabás	(1C. melléklet, 4.1. fejezet: „Látható adatok", 230) Az elülső oldalnak a következőket kell tartalmaznia: a kibocsátott kártyára vonatkozó egyedi információk. (1C. melléklet, 4.1. fejezet: „Látható adatok", 231) Az elülső oldalnak a következőket kell tartalmaznia: „nn/hh/éééé" vagy „nn.hh.éééé" (nap, hónap, év) formátumú dátumok. (1C. melléklet, 4.1. fejezet: „Látható adatok", 235) A tachográfkártyákat a hamisítás és a jogosulatlan változtatások ellen legalább a következőkkel kell ellátni: — a fénykép területén a biztonsági háttérnyomtatásnak és a fényképnek át fednie kell egymást.	230, 231, 235

5. A KÜLSŐ GNSS-ESZKÖZ TESZTJEI

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
2.	**A külső GNSS-eszköz szemrevételezése**		
2.1.	A dokumentációnak való megfelelés		
2.2.	Azonosítás/jelölések		224–226
2.3.	Anyagok		219–223
3.	**Működési tesztek**		
3.1.	Az érzékelő azonosítási adatai		98, 99
3.2.	A külső GNSS-modul és a járműegység összekapcsolása		123, 205

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
3.3.	GNSS-helyzet		36, 37
3.4.	Járműegység-interfész a járműegységen kívüli GNSS-vevők esetében		03
3.5.	Titkosítási eszközkészlet (cypher suite) és szabványos tartományparaméterek		CSM_48, CSM_50
4.	**Környezetállósági tesztek**		
4.1.	Hőmérséklet	Működés-ellenőrzés az alábbiak révén: Az ISO 16750-4 szabvány 5.1.1.2. fejezete szerinti vizsgálat: működési vizsgálat alacsony hőmérsékleten (72 óra – 20 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-1: Környezetállósági vizsgálatok – 2-1. rész: Vizsgálatok – A. vizsgálat: Hideg Az ISO 16750-4 szabvány 5.1.2.2. fejezete szerinti vizsgálat: működési vizsgálat magas hőmérsékleten (72 óra 70 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-2: Alapvető környezetállósági vizsgálati eljárások; 2. rész: vizsgálatok; B. vizsgálatok: száraz meleg Az ISO 16750-4 szabvány szerinti vizsgálat: 5.3.2. fejezet: gyors hőmérséklet-változás meghatározott átmeneti időszakokkal (– 20 °C/70 °C, 20 ciklus, 1 órás tartózkodási idő mindegyik hőmérsékleten) A legalacsonyabb és a legmagasabb feltüntetett hőmérsékleten és a hőmérsékleti ciklusok alatt csökkentett számú teszt végezhető (az e táblázat 3. részében meghatározottak közül).	213
4.2.	Páratartalom	Ellenőrizni kell, hogy a járműegység ellenáll-e a ciklikus párásodásnak (hőellenállási vizsgálat) az IEC 60068-2-30 szabvány szerinti Db. vizsgálattal a következő feltételek mellett: hat 24 órás ciklus, minden ciklusban + 25 °C és + 55 °C között változó hőmérséklet, a relatív páratartalom 97 % + 25 °C-on és 93 % + 55 °C-on.	214
4.3.	Mechanikai	1. Szinuszos rezgés: annak ellenőrzése, hogy a járműegység ellenáll-e az alábbi jellemzőkkel rendelkező szinuszos rezgésnek: állandó kitérés 5 és 11 Hz között: 10 mm-es csúcs állandó gyorsulás 11 és 300 Hz között: 5g E követelményt az IEC 60068-2-6 szabvány Fc. vizsgálatával kell ellenőrizni, e vizsgálat minimális időtartama 3 × 12 óra (tengelyenként 12 óra). Az ISO 16750-3 szabvány a leválasztott vezetőfülkében található eszközökre nem írja elő a szinuszos rezgés vizsgálatát.	219

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		2. Véletlenszerű rezgés: Az ISO 16750-3 szabvány 4.1.2.8. fejezete szerinti vizsgálat: VIII. vizsgálat: Haszonjármű leválasztott vezetőfülkével A véletlenszerű rezgés vizsgálata, 10–2 000 Hz, függőleges RMS: 21,3 m/s^2, hosszirányú RMS: 11,8 m/s^2, oldalirányú RMS: 13,1 m/s^2, 3 tengely, 32 óra tengelyenként, beleértve a – 20 °C – 70 °C-os hőmérsékleti ciklust. Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-64: Környezetállósági vizsgálatok – 2-64. rész: Vizsgálatok – Fh. vizsgálat: Széles sávú, véletlenszerű rázás és irányelvei 3. Ütések: mechanikai ütés 3g-s félszinusszal az ISO 16750 szabvány szerint. A fent leírt teszteket a tesztelt készüléktípus különböző mintáin kell elvégezni	
4.4.	Víz és idegen testek elleni védelem	Az ISO 20653 szabvány szerinti vizsgálat: Közúti járművek – Védettségi fokozat (IP kód) – Elektromos berendezések idegen tárgyakkal, vízzel és hozzáféréssel szembeni védelme (Változatlan paraméterek)	220, 221
4.5.	Túlfeszültségvédelem	Ellenőrizni kell, hogy a járműegység ellenáll-e az alábbi feszültségeknek:	216
		24 V-os modellek esetében: — 34 V + 40 °C mellett 1 órán át	
		12 V-os modellek esetében: — 17 V + 40 °C mellett 1 órán át	
		(ISO 16750-2 szabvány, 4.3. fejezet)	
4.6.	Fordított polaritás elleni védelem	Ellenőrizni kell, hogy a járműegység ellenáll-e az áramellátás megfordításának. (ISO 16750-2 szabvány, 4.7. fejezet)	216
4.7.	Rövidzárlatvédelem	Ellenőrizni kell, hogy a bemeneti-kimeneti jelek védettek-e az áramellátás felőli rövidzárlattal és a földzárlattal szemben. (ISO 16750-2 szabvány, 4.10. fejezet)	216
5.	**Elektromágneses összeférhetőségi tesztek**		
5.1.	Sugárzáskibocsátás és szuszceptibilitás	A 10. sz. ENSZ EGB-előírásnak való megfelelés	218

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
5.2.	Elektromos kisülés	Az ISO 10605:2008 + szabványnak való megfelelés: műszaki helyesbítés: 2010 + AMD1:2014: +/– 4 kV az érintkezési és +/– 8 kV a légköri kisülés vonatkozásában	218
5.3.	Vezetett tranziens szuszceptibilitás az áramellátáson	A 24 V-os modellek esetében: az ISO 7637-2 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1a. impulzus: Vs = – 450 V Ri = 50 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 20 V Ri = 0,05 ohm 3a. impulzus: Vs = – 150 V Ri = 50 ohm 3b. impulzus: Vs = + 150 V Ri = 50 ohm 4. impulzus: Vs = – 16V Va = – 12V t6 = 100 ms 5. impulzus: Vs = + 120 V Ri = 2,2 ohm td = 250 ms A 12 V-os modellek esetében: az ISO 7637-1 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1. impulzus: Vs = – 75 V Ri = 10 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 10 V Ri = 0,05 ohm 3a. impulzus: Vs = – 112 V Ri = 50 ohm 3b. impulzus: Vs = + 75 V Ri = 50 ohm 4. impulzus: Vs = – 6V Va=–5V t6=15 ms 5. impulzus: Vs = + 65V Ri = 3 ohm td = 100 ms Az 5. impulzust csak azon járműegységeken kell tesztelni, amelyeket olyan járművekbe szerelnek be, amelyeknél nem alkalmaznak túlfeszültség elleni közös külső védelmet. A túlfeszültséggel kapcsolatos javaslat tekintetében lásd az ISO 16750-2 szabvány 4. kiadásának 4.6.4. fejezetét.	218

6. A TÁVOLI KOMMUNIKÁCIÓS ESZKÖZ TESZTJEI

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
2.	**Szemrevételezés**		
2.1.	A dokumentációnak való megfelelés		
2.2.	Azonosítás/jelölések		225, 226
2.3.	Anyagok		219–223
4.	**Környezetállósági tesztek**		
4.1	Hőmérséklet	Működés-ellenőrzés az alábbiak révén: Az ISO 16750-4 szabvány 5.1.1.2. fejezete szerinti vizsgálat: működési vizsgálat alacsony hőmérsékleten (72 óra – 20 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-1: Környezetállósági vizsgálatok – 2-1. rész: Vizsgálatok – A. vizsgálat: Hideg	213

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
		Az ISO 16750-4 szabvány 5.1.2.2. fejezete szerinti vizsgálat: működési vizsgálat magas hőmérsékleten (72 óra 70 °C-on) Ez a teszt a következő szabvánnyal kapcsolatos: IEC 60068-2-2: Alapvető környezetállósági vizsgálati eljárások; 2. rész: vizsgálatok; B. vizsgálatok: száraz meleg Az ISO 16750-4 szabvány 5.3.2. fejezete szerinti vizsgálat: gyors hőmérséklet-változás meghatározott átmeneti időszakokkal (– 20 °C/70 °C, 20 ciklus, 1 órás tartózkodási idő mindegyik hőmérsékleten) A legalacsonyabb és a legmagasabb feltüntetett hőmérsékleten és a hőmérsékleti ciklusok alatt csökkentett számú teszt végezhető (az e táblázat 3. részében meghatározottak közül).	
4.4.	Víz és idegen testek elleni védelem	Az ISO 20653 szabvány szerinti vizsgálat: Közúti járművek – Védettségi fokozat (IP kód) – Elektromos berendezések idegen tárgyakkal, vízzel és hozzáféréssel szembeni védelme (célérték: IP40)	220, 221
5.	**Elektromágneses összeférhetőségi tesztek**		
5.1.	Sugárzáskibocsátás és szuszceptibilitás	A 10. sz. ENSZ EGB-előírásnak való megfelelés	218
5.2.	Elektromos kisülés	Az ISO 10605:2008 + szabványnak való megfelelés: műszaki helyesbítés: 2010 + AMD1:2014: +/– 4 kV az érintkezési és +/– 8 kV a légköri kisülés vonatkozásában	218
5.3.	Vezetett tranziens szuszceptibilitás az áramellátáson	A 24 V-os modellek esetében: az ISO 7637-2 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1a. impulzus: Vs = – 450 V Ri = 50 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 20 V Ri = 0,05 ohm 3a. impulzus: Vs = – 150 V Ri = 50 ohm 3b. impulzus: Vs = + 150 V Ri = 50 ohm 4. impulzus: Vs = – 16V Va = – 12V t6 = 100 ms 5. impulzus: Vs = + 120 V Ri = 2,2 ohm td = 250 ms A 12 V-os modellek esetében: az ISO 7637-1 szabványnak és a 10. sz. ENSZ EGB-előírás 3. módosításának való megfelelés: 1. impulzus: Vs = – 75 V Ri = 10 ohm 2a. impulzus: Vs = + 37 V Ri = 2 ohm 2b. impulzus: Vs = + 10 V Ri = 0,05 ohm 3a. impulzus: Vs = – 112 V Ri = 50 ohm 3b. impulzus: Vs = + 75 V Ri = 50 ohm 4. impulzus: Vs = – 6V Va = – 5V t6= 15 ms 5. impulzus: Vs = + 65 V Ri =3 ohm td = 100 ms Az 5. impulzust csak azon járműegységeken kell tesztelni, amelyeket olyan járművekbe szerelnek be, amelyeknél nem alkalmaznak túlfeszültség elleni közös külső védelmet. A túlfeszültséggel kapcsolatos javaslat tekintetében lásd az ISO 16750-2 szabvány 4. kiadásának 4.6.4. fejezetét.	218

▼B

7. A PAPÍR MŰKÖDÉSI TESZTJEI

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	A dokumentáció helytállósága	
2.	**Általános tesztek**		
2.1.	Karakterek száma soronként	A kinyomat szemrevételezése.	172
2.2.	Minimális karaktermé-ret.	A kinyomat és a karakterek szemrevételezése.	173
2.3.	Támogatott karakterkészletek	A nyomtatónak képesnek kell lennie az 1. függelék 4. fejezetében („Karakterkészletek”) meghatározott karakterek kinyomtatására.	174
2.4.	A kinyomatok felbontása	A menetíró készülék típusjóváhagyásának ellenőrzése és a kinyomatok szemrevételezése.	174
2.5.	A kinyomatok olvashatósága és azonosíthatósága	A kinyomatok szemrevételezése. A gyártónak vizsgálati jelentésekkel és vizsgálati protokollokkal kell igazolnia a megfelelést. Valamennyi olyan menetíró készülék jóváhagyási számának (számainak) szerepelnie kell a papíron, amellyel a nyomtatópapír használható.	175, 177, 178
2.6.	Kézzel írott feljegyzések hozzáadása	Szemrevételezés: A járművezető aláírásának helye szerepel a papíron. Egyéb kézzel írott feljegyzések számára külön hely van a papíron.	180
2.7.	A papír elülső oldalának további részletei.	A papír elülső és hátsó oldala további részleteket és információkat tartalmazhat. Ezek a részletek és információk nem befolyásolhatják a kinyomatok olvashatóságát. Szemrevételezés.	177, 178
3.	**Tárolási tesztek**		
3.1.	Száraz meleg	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 72 óra + 70 °C ± 2 °C hőmérsékleten Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178 IEC 60068-2-2-Bb
2.2.	Nedves meleg	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 144 óra + 55 °C ± 2 °C hőmérsékleten, 93 % ± 3 % relatív páratartalom mellett Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178 IEC 60068-2-78-Cab

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
4.	**A papír használat közbeni tesztjei**		
4.1.	Nedvességállóság – háttér (nem nyomtatott papír)	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 144 óra + 55 °C ± 2 °C hőmérsékleten, 93 % ± 3 % relatív páratartalom mellett Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178 IEC 60068-2-78-Cab
4.2.	Nyomtathatóság	Előkondicionálás: 24 óra + 40 °C ± 2 °C hőmérsékleten, 93 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: + 23 °C ± 2 °C hőmérsékleten nyomtatott kinyomat Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178
4.3.	Hőállóság	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 2 óra + 70 °C ± 2 °C hőmérsékleten, száraz meleg Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178 IEC 60068-2-2-Bb
4.4.	Alacsony hőmérséklettel szembeni ellenálló-képesség	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 24 óra – 20 °C ± 3 °C hőmérsékleten, száraz hideg Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178 ISO 60068-2-1-Ab
4.5.	Fényállóság	Előkondicionálás: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Tesztkörnyezet: 100 óra 5 000 luxos megvilágítással, + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett Regeneráció: 16 óra + 23 °C ± 2 °C hőmérsékleten, 55 % ± 3 % relatív páratartalom mellett	176, 178

Olvashatósági kritériumok a 3.x. és 4.x. tesztek esetében:

A kinyomat olvashatósága akkor biztosított, ha az optikai sűrűség megfelel a következő határértékeknek:

Nyomtatott karakterek: legalább 1,0

Háttér (nem nyomtatott papír): legalább 0,2

Az elkészült kinyomatok optikai sűrűségét a DIN EN ISO 534 szabvány szerint kell mérni.

A kinyomatok nem mutathatnak méretváltozást és jól olvashatónak kell maradniuk.

8. INTEROPERABILITÁSI TESZTEK

Szám	Teszt	Leírás
9.1. A járműegységek és a tachográfkártyák interoperabilitásának tesztjei		
1.	Kölcsönös hitelesítés	Ellenőrizni kell, hogy rendesen végbemegy-e a járműegység és a tachográfkártya közötti kölcsönös hitelesítés.

▼B

Szám	Teszt	Leírás
2.	Írási/olvasási tesztek	El kell végezni egy jellemző tevékenységi sort a járműegységen. A tevékenységi sort a tesztelt kártya típusához kell igazítani, és a kártyán található lehető legtöbb EF-be való írást kell tartalmaznia. A járműegység adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. A kártya adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. Napi kinyomatok készítésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzített adat megfelelően olvasható-e.
9.2. A járműegységek és a mozgásérzékelők interoperabilitásának tesztjei		
1.	Párosítás	Ellenőrizni kell, hogy rendesen végbemegy-e a járműegység és a mozgásérzékelő közötti kölcsönös hitelesítés.
2.	Működési tesztek	El kell végezni egy jellemző tevékenységi sort a mozgásérzékelőn. A tevékenységi sornak egy normál műveletet és a lehető legtöbb eseményt vagy hibát kell tartalmaznia. A járműegység adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. A kártya adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. Napi kinyomat készítésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzített adat megfelelően olvasható-e.
9.3. A járműegység és a külső GNSS-eszköz interoperabilitásának tesztjei (adott esetben)		
1.	Kölcsönös hitelesítés	Ellenőrizni kell, hogy rendesen végbemegy-e a járműegység és a külső GNSS-eszköz közötti kölcsönös hitelesítés (párosítás).
2.	Működési tesztek	El kell végezni egy jellemző tevékenységi sort a külső GNSS-eszközön. A tevékenységi sornak egy normál műveletet és a lehető legtöbb eseményt vagy hibát kell tartalmaznia. A járműegység adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. A kártya adatainak letöltésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzítés megfelelően megtörtént-e. Napi kinyomat készítésével ellenőrizni kell, hogy a tevékenységgel kapcsolatos minden rögzített adat megfelelően olvasható-e.

▼B

10. függelék

BIZTONSÁGI KÖVETELMÉNYEK

Ez a függelék az intelligens menetíró rendszerek (második generációs menetíró készülékek) alkatrészeire vonatkozó informatikai biztonsági követelményeket határozza meg.

SEC_001 Az intelligens menetíró rendszerek következő alkatrészeinek a Common Criteria szabvány szerinti rendszernek megfelelő biztonsági tanúsítvánnyal kell rendelkeznie:

— járműegység;

— tachográfkártya;

— mozgásérzékelő;

— külső GNSS-eszköz.

SEC_002 A biztonsági tanúsítvánnyal ellátandó alkatrészekre vonatkozó informatikai biztonsági minimumkövetelményeket az alkatrész védelmi profiljában kell meghatározni a Common Criteria szabvány szerinti rendszernek megfelelően.

SEC_003 Az Európai Bizottság gondoskodik arról, hogy az európai SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates – Az információtechnológiai biztonsági értékelési tanúsítványok kölcsönös elismeréséről szóló megállapodás) égisze alatt a tanúsítványok kölcsönös elismerését támogató közös értelmezési munkacsoportban (JIWG, Joint Interpretation Working Group) részt vevő, informatikai biztonsági tanúsítással foglalkozó kormányzati szervek támogassák, fejlesszék és jóváhagyják az e mellékletnek megfelelő, alábbi négy védelmi profilt, továbbá arról, hogy azok nyilván legyenek tartva:

— a járműegység védelmi profilja;

— a tachográfkártya védelmi profilja;

— a mozgásérzékelő védelmi profilja;

— a külső GNSS-eszköz védelmi profilja.

A járműegység védelmi profiljának vonatkoznia kell azokra az esetekre, amelyekben a járműegységet külső GNSS-eszközzel való vagy anélküli használatra tervezték. Az előbbi esetben a külső GNSS-eszközre vonatkozó biztonsági követelményeknek ezen eszköz saját védelmi profiljában kell szerepelniük.

SEC_004 Azon biztonsági cél meghatározása érdekében, amelyet egy alkatrésznek a biztonsági tanúsításhoz teljesítenie kell, az alkatrész gyártóinak szükség szerint pontosítaniuk kell és ki kell egészíteniük a megfelelő alkatrész védelmi profilját anélkül, hogy módosítanák vagy törölnék a meglévő kockázatokat, célkitűzéseket, eljárási eszközöket és a biztonságérvényesítési funkciókra vonatkozó előírásokat.

SEC_005 Az értékelési folyamat során megállapítást kell nyernie, hogy ez a konkrét biztonsági cél pontosan megfelel a vonatkozó védelmi profilnak.

SEC_006 Valamennyi védelmi profil esetében az ATE.DPT.2 és AVA_VAN.5 biztonsági elemekkel bővített EAL4 biztonsági szintet kell teljesíteni.

▼B

11. függelék

KÖZÖS BIZTONSÁGI MECHANIZMUSOK

TARTALOMJEGYZÉK

PREAMBULUM

A. RÉSZ ELSŐ GENERÁCIÓS MENETÍRÓ RENDSZER

1. BEVEZETÉS

1.1. Hivatkozások

1.2. Jelzések és rövidítések

2. TITKOSÍTÁSI RENDSZEREK ÉS ALGORITMUSOK

2.1. Titkosítási rendszerek

2.2. Titkosítási algoritmusok

2.2.1. RSA algoritmus

2.2.2. Hasító algoritmus

2.2.3. Adattitkosítási algoritmus

3. KULCSOK ÉS TANÚSÍTVÁNYOK

3.1. Kulcsok generálása és elosztása

3.1.1. RSA-kulcsok generálása és elosztása

3.1.2. RSA-tesztkulcsok

3.1.3. Mozgásérzékelő kulcsok

3.1.4. T-DES tevékenységi kulcsok generálása és elosztása

3.2. Kulcs

3.3. Tanúsítványok

3.3.1. A tanúsítványok tartalma

3.3.2. Kiállított tanúsítványok

3.3.3. A tanúsítvány ellenőrzése és kicsomagolása

4. KÖLCSÖNÖS HITELESÍTÉSI MECHANIZMUS

5. A JÁRMŰEGYSÉGKÁRTYÁK ADATÁTVITELLEL KAPCSOLATOS TITKOSSÁGI, INTEGRITÁSI ÉS HITELESÍTÉSI MECHANIZMUSA

5.1. Biztonságos üzenetküldés

5.2. A biztonságos üzenetküldéssel kapcsolatos hibák kezelése

5.3. A titkosítási ellenőrző összeget kiszámító algoritmus

5.4. A titkossági DO-utasítások kriptogramjait kiszámító algoritmus

6. AZ ADATLETÖLTÉS DIGITÁLIS ALÁÍRÁSI MECHANIZMUSAI

6.1. Aláírások generálása

▼B

6.2.	Aláírások ellenőrzése
B. RÉSZ	MÁSODIK GENERÁCIÓS MENETÍRÓ RENDSZER
7.	BEVEZETÉS
7.1.	Hivatkozások
7.2.	Jelzések és rövidítések
7.3.	Fogalommeghatározások
8.	TITKOSÍTÁSI RENDSZEREK ÉS ALGORITMUSOK
8.1.	Titkosítási rendszerek
8.2.	Titkosítási algoritmusok
8.2.1.	Szimmetrikus algoritmusok
8.2.2.	Aszimmetrikus algoritmusok és szabványosított tartományparaméterek
8.2.3.	Hasító algoritmusok
8.2.4.	Titkosítási készletek
9.	KULCSOK ÉS TANÚSÍTVÁNYOK
9.1.	Aszimmetrikus kulcspárok és nyilvánoskulcs-tanúsítványok
9.1.1.	Általános tudnivalók
9.1.2.	Európai szint
9.1.3.	Tagállami szint
9.1.4.	Berendezési szint: Járműegységek
9.1.5.	Berendezési szint: Tachográfkártyák
9.1.6.	Berendezési szint: Külső GNSS-eszközök
9.1.7.	Áttekintés: Tanúsítványok cseréje
9.2.	Szimmetrikus kulcsok
9.2.1.	A járműegységek és mozgásérzékelők közötti kommunikáció biztonságossá tételét szolgáló kulcsok
9.2.2.	Kulcsok a DSRC-kommunikáció biztonságossá tételéhez
9.3.	Tanúsítványok
9.3.1.	Általános tudnivalók
9.3.2.	A tanúsítvány tartalma
9.3.3.	Tanúsítványok igénylése
10.	JÁRMŰEGYSÉG ÉS KÁRTYA KÖZÖTTI KÖLCSÖNÖS HITELESÍTÉS ÉS BIZTONSÁGOS ÜZENETKÜLDÉS
10.1.	Általános tudnivalók
10.2.	Kölcsönös tanúsítványláncolat-ellenőrzés
10.2.1.	A kártyatanúsítvány-láncolat járműegység által végzett ellenőrzése

▼B

10.2.2. A járműegység tanúsítványláncolatának kártya általi ellenőrzése

10.3. Járműegység-hitelesítés

10.4. Chiphitelesítés és munkamenetkulcs-egyeztetés

10.5. Biztonságos üzenetküldés

10.5.1. Általános tudnivalók

10.5.2. Biztonságos üzenetstruktúra

10.5.3. Biztonságos üzenetküldési munkamenet megszakítása

11. JÁRMŰEGYSÉG ÉS KÜLSŐ GNSS-ESZKÖZ ÖSSZEKAPCSOLÁSA, KÖLCSÖNÖS HITELESÍTÉSE ÉS BIZTONSÁGOS ÜZENETKÜLDÉSE

11.1. Általános tudnivalók

11.2. A járműegység és a külső GNSS-eszköz összekapcsolása

11.3. Kölcsönös tanúsítványláncolat-ellenőrzés

11.3.1. Általános tudnivalók

11.3.2. A járműegység és az EGF összekapcsolásakor

11.3.3. Működés normál üzemben

11.4. Járműegység-hitelesítés, chiphitelesítés és munkamenetkulcs-egyeztetés

11.5. Biztonságos üzenetküldés

12. JÁRMŰEGYSÉG ÉS MOZGÁSÉRZÉKELŐ KÖZÖTTI PÁROSÍTÁS ÉS KOMMUNIKÁCIÓ

12.1. Általános tudnivalók

12.2. Járműegység és mozgásérzékelő párosítása különböző kulcsgenerációk használatával

12.3. Járműegység és mozgásérzékelő közötti párosítás és kommunikáció AES használatával

12.4. Járműegység és mozgásérzékelő párosítása különböző készülékgenerációk esetében

13. A DSRC-N KERESZTÜLI TÁVOLI KOMMUNIKÁCIÓ BIZTONSÁGA

13.1. Általános tudnivalók

13.2. A tachográfterhelés titkosítása és a MAC létrehozása

13.3. A tachográfterhelés ellenőrzése és visszafejtése

14. AZ ADATLETÖLTÉSEK ALÁÍRÁSA ÉS AZ ALÁÍRÁSOK ELLENŐRZÉSE

14.1. Általános tudnivalók

14.2. Aláírások generálása

14.3. Aláírások ellenőrzése

▼B

PREAMBULUM

E függelék az alábbiakat biztosító biztonsági mechanizmusokat határozza meg:

— kölcsönös hitelesítés a menetíró rendszer különböző részegységei között;

— a menetíró rendszer különböző részegységei között átvitt vagy külső tároló-eszközre letöltött adatok titkossága, integritása, hitelessége és/vagy letagadhatatlansága.

Ez a függelék két részből áll. Az A. részben az első generációs menetíró rendszer biztonsági mechanizmusainak leírása található (digitális menetíró készülék). A B. részben a második generációs menetíró rendszer biztonsági mechanizmusainak leírása található (intelligens menetíró készülék).

Az e függelék A. részében ismertetett mechanizmusok akkor alkalmazandók, ha a kölcsönös hitelesítésben és/vagy adatátvitelben érintett menetíró rendszer legalább egyik részegysége első generációs.

Az e függelék B. részében ismertetett mechanizmusok akkor alkalmazandók, ha a kölcsönös hitelesítésben és/vagy adatátvitelben érintett menetíró rendszer mindkét részegysége második generációs.

A 15. függelék további információkkal szolgál az első és második generációs részegységek együttes használatáról.

A. RÉSZ

ELSŐ GENERÁCIÓS MENETÍRÓ RENDSZER

1. BEVEZETÉS

1.1. **Hivatkozások**

E függelék az alábbi hivatkozásokat használja:

SHA-1	National Institute of Standards and Technology (Amerikai Nemzeti Szabványügyi és Technológiai Hivatal, NIST). *FIPS Publication 180-1: Secure Hash Standard*. 1995. április
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. 1998. október
TDES	National Institute of Standards and Technology (Amerikai Nemzeti Szabványügyi és Technológiai Hivatal, NIST). *FIPS Publication 46-3: Data Encryption Standard*. 1999-es tervezet
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Információtechnológia. Azonosító kártyák. Érintkezős, integrált áramkörös kártyák. 4. rész: Ágazatközi parancsok információcseréhez Első kiadás: 1995. + 1. módosítás: 1997.
ISO/IEC 7816-6	Információtechnológia. Azonosító kártyák. Érintkezős, integrált áramkörös kártyák. 6. rész: Ágazatközi adatelemek. Első kiadás: 1996. + 1. javítás: 1998.
ISO/IEC 7816-8	Információtechnológia. Azonosító kártyák. Érintkezős, integrált áramkörös kártyák. 8. rész: Biztonsággal kapcsolatos ágazatközi parancsok. Első kiadás: 1999.
ISO/IEC 9796-2	Információtechnológia. Biztonsági technikák. Az üzenet helyreállítását lehetővé tevő digitális aláírási rendszerek. 2. rész: Hasítófunkciót használó mechanizmusok. Első kiadás: 1997.

▼B

ISO/IEC 9798-3	Információtechnológia. Biztonsági technikák. Entitáshitelesítési mechanizmusok. 3. rész: Entitáshitelesítés nyilvános kulcsú algoritmus segítségével. Második kiadás: 1998.
ISO 16844-3	Közúti járművek. Tachográfrendszerek. 3. rész: Mozgásérzékelő-interfész.

1.2. **Jelzések és rövidítések**

E függelék az alábbi jelzéseket és rövidítéseket használja:

(K_a, K_b, K_c)	A key bundle for use by the Triple Data Encryption Algorithm – Kulcscsomag a háromszoros adattitkosítási algoritmus általi használatra
CA	Certification Authority – Tanúsító hatóság
CAR	Certification Authority Reference – A tanúsító hatóság hivatkozása
CC	Cryptographic Checksum – Titkosítási ellenőrző összeg
CG	Cryptogram – Kriptogram
CH	Command Header – Parancsfej
CHA	Certificate Holder Authorisation – A tanúsítvány tulajdonosának engedélye
CHR	Certificate Holder Reference – A tanúsítvány tulajdonosának hivatkozása
D()	Decryption with DES – Visszafejtés a DES segítségével
DE	Data Element – Adatelem
DO	Data Object – Adatobjektum
d	RSA private key, private exponent – RSA privát kulcs, saját kitevő
e	RSA public key, public exponent – RSA nyilvános kulcs, nyilvános kitevő
E()	Encryption with DES – Titkosítás a DES segítségével
EQT	Equipment – Berendezés
Hash()	Hash value, an output of *Hash* – Hasító érték, a *hasítás* eredménye
Hash	Hash function – Hasító funkció
KID	Key Identifier – Kulcsazonosító
Km	TDES key. Master Key defined in ISO 16844-3. – TDES-kulcs. Az ISO 16844-3. sz. szabvány által meghatározott mesterkulcs
Km_{VU}	TDES key inserted in vehicle units – A járműegységbe helyezett TDES-kulcs
Km_{WC}	TDES key inserted in workshop cards – A műhelykártyába helyezett TDES-kulcs
m	Message representative, an integer between 0 and *n*-1 – Az üzenetet képviselő, 0 és *n*-1 közötti egész szám
n	RSA keys, modulus – RSA-kulcs, modulus
PB	Padding Bytes – Kitöltőbájtok
PI	Padding Indicator byte (for use in Cryptogram for confidentiality DO) – Kitöltésjelző bájt (a titkossági DO kriptogramjában való használatra)
PV	Plain Value – Egyszerű érték
s	Signature representative, an integer between 0 and *n*-1 – Az aláírást képviselő, 0 és *n*-1 közötti egész szám
SSC	Send Sequence Counter – Küldési sorrendszámláló
SM	Secure Messaging – Biztonságos üzenetküldés
TCBC	TDEA Cipher Block Chaining Mode of Operation – TDEA titkosított blokkok láncolatán alapuló üzemmód

▼B

TDEA	Triple Data Encryption Algorithm – Háromszoros adattitkosítási algoritmus
TLV	Tag Length Value – A címke hosszának értéke
VU	Vehicle Unit – Járműegység
X.C	The certificate of user X issued by a certification authority – X felhasználó tanúsítványa, amelyet valamely tanúsító hatóság bocsátott ki
X.CA	A certification authority of user X – X felhasználó tanúsító hatósága
X.CA.PK $_{o}$ X.C	The operation of unwrapping a certificate to extract a public key – A nyilvános kulcs kiemelését célzó tanúsítványkicsomagolási művelet. Infix műveleti jel, amelynek bal oldali operandusa valamely tanúsító hatóság nyilvános kulcsa, és amelynek jobb oldali operandusa az említett tanúsító hatóság által kibocsátott tanúsítvány. Az eredmény X felhasználó nyilvános kulcsa, akinek a tanúsítványa a jobb oldali operandus.
X.PK	RSA public key of a user X – A felhasználó nyilvános RSA-kulcsa
X.PK[I]	RSA encipherment of some information I, using the public key of user X – Valamilyen I információ RSA titkosítása, X felhasználó nyilvános kulcsának segítségével
X.SK	RSA private key of a user X – X felhasználó privát RSA-kulcsa
X.SK[I]	RSA encipherment of some information I, using the private key of user X – Valamilyen I információ RSA titkosítása, X felhasználó privát kulcsának segítségével
xx	A hexadecimal value – Hexadecimális érték
||	Concatenation operator – Összefűzési operátor

2. TITKOSÍTÁSI RENDSZEREK ÉS ALGORITMUSOK

2.1. **Titkosítási rendszerek**

CSM_001 A járműegységeknek és a tachográfkártyáknak egy klasszikus RSA nyilvános kulcsú titkosítási rendszer segítségével az alábbi biztonsági mechanizmusokat kell nyújtaniuk:

— a járműegységek és a kártyák közötti hitelesítés;

— háromszoros DES-munkamenetkulcsok átvitele a járműegységek és a tachográfkártyák között;

— a járműegységekről vagy a tachográfkártyákról külső tárolóeszközre letöltött adatok digitális aláírása.

CSM_002 A járműegységek és a tachográfkártyák háromszoros DES szimmetrikus titkosítási rendszer használata révén gondoskodnak az adatok integritását biztosító mechanizmusról a járműegységek és a tachográfkártyák közötti felhasználói adatcsere során, valamint adott esetben gondoskodnak a járműegységek és a tachográfkártyák közötti adatcsere titkosságáról.

2.2. **Titkosítási algoritmusok**

2.2.1 *RSA algoritmus*

CSM_003 Az RSA algoritmust teljes mértékben az alábbi relációk határozzák meg:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Az RSA-funkció még részletesebb leírása a PKCS1 számú hivatkozásban található. Az RSA algoritmusban alkalmazott „e” nyilvános kitevő 3 és n-1 közötti egész szám, amely teljesíti a következő feltételt: gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hasító algoritmus*

CSM_004 A digitális aláírási mechanizmusok az SHA-1 hivatkozásban meghatározott SHA-1 hasító algoritmust használják.

2.2.3 *Adattitkosítási algoritmus*

CSM_005 A titkosított blokkok láncolatán alapuló üzemmódban DES-alapú algoritmust kell használni.

3. KULCSOK ÉS TANÚSÍTVÁNYOK

3.1. **Kulcsok generálása és elosztása**

3.1.1 *RSA-kulcsok generálása és elosztása*

CSM_006 Az RSA-kulcsok generálása a funkcionális hierarchia három szintjén történik:

— európai szint;

— tagállami szint;

— berendezési szint.

CSM_007 Európai szinten egy egységes európai kulcspárt (EUR.SK és EUR.PK) kell generálni. Az európai privát kulcs segítségével kell tanúsítani a tagállami nyilvános kulcsokat. Az összes tanúsított kulcs adatait meg kell őrizni. E feladatokat egy, az Európai Bizottság felügyelete alá tartozó és annak felelős európai tanúsító hatóság végzi el.

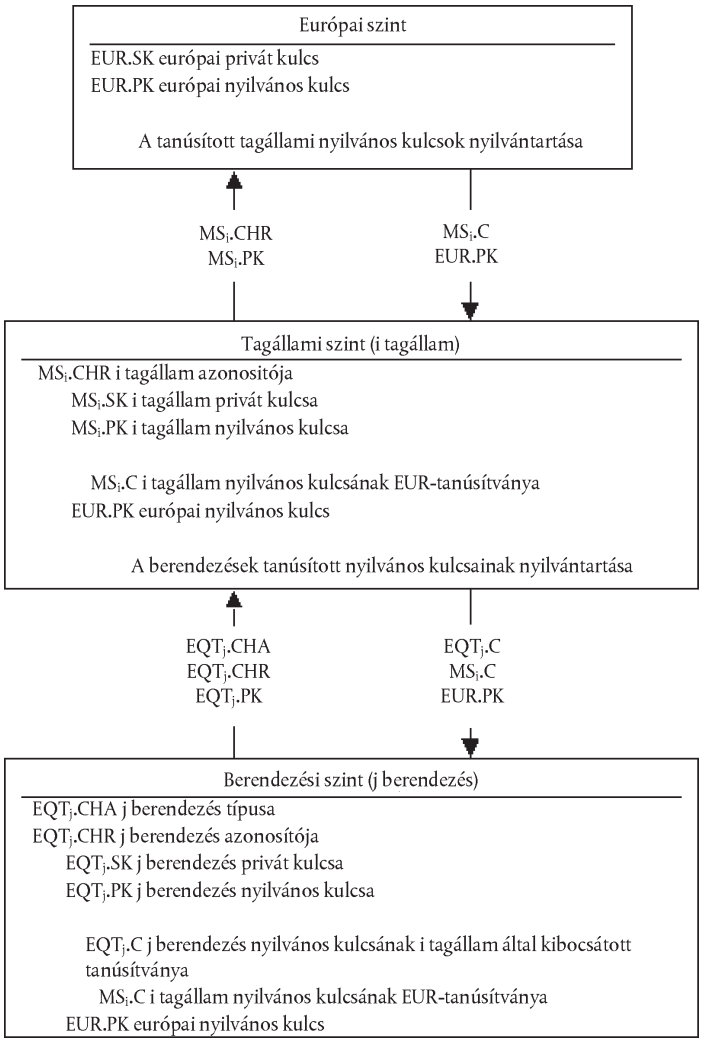
CSM_008 Tagállami szinten egy tagállami kulcspárt (MS.SK és MS.PK) kell generálni. A tagállami nyilvános kulcsok tanúsítását az európai tanúsító hatóság végzi. A tagállami privát kulcs segítségével kell tanúsítani a berendezésbe (járműegység vagy tachográfkártya) behelyezendő nyilvános kulcsokat. Az összes tanúsított nyilvános kulcs adatait meg kell őrizni azon berendezés azonosító adataival együtt, amelybe behelyezték. E feladatokat a tagállami tanúsító hatóságok látják el. A tagállamok rendszeresen megváltoztathatják a kulcspárjukat.

CSM_009 Berendezési szinten egyetlen kulcspárt (EQT.SK és EQT.PK) kell generálni és behelyezni minden berendezésbe. A berendezési nyilvános kulcsok tanúsítását a tagállami tanúsító hatóságok végzik. E feladatokat a berendezések gyártói, a testreszabást végző személyek vagy a tagállami hatóságok végzik el. E kulcspárt hitelesítési, digitális aláírási és titkosítási célokra kell használni.

CSM_010 Generálás, (adott esetben) továbbítás és tárolás közben meg kell őrizni a privát kulcsok titkosságát.

▼B

Az alábbi ábra e folyamat adatáramlását foglalja össze:



3.1.2 *RSA-tesztkulcsok*

CSM_011 A berendezés vizsgálata céljából (az interoperabilitási vizsgálatokat is ideértve) az európai tanúsító hatóság egy másik egyetlen európai vizsgálati kulcspárt és legalább két tagállami vizsgálati kulcspárt generál, amelyek nyilvános kulcsait az európai privát tesztkulccsal együtt kell tanúsítani. A gyártók elhelyezik az ilyen tagállami vizsgálati kulcsok által tanúsított tesztkulcsokat a típus-jóváhagyási vizsgálat alá vont berendezésben.

3.1.3 *Mozgásérzékelő kulcsok*

A generálás, továbbítás (adott esetben) és tárolás közben az alább leírt három TDES-kulcs titkosságát megfelelő módon meg kell őrizni.

Az ISO 16844. sz. szabványnak megfelelő menetíró-alkatrészek támogatására ezenkívül az európai tanúsító hatóság és a tagállami tanúsító hatóságok gondoskodnak az alábbiakról:

CSM_036 Az európai tanúsító hatóság KmVU-t és KmWC-t, két független és egyedi hármas DES-kulcsot, valamint Km-kulcsot generál az alábbiak szerint: $Km = Km_{VU} XOR Km_{WC}$. Az európai tanúsító hatóság kellően biztonságos eljárással továbbítja ezeket a kulcsokat a tagállamok tanúsító hatóságai számára, a hatóságok kérésére.

▼B

CSM_037 A tagállami tanúsító hatóságoknak:

— a Km segítségével titkosítaniuk kell a mozgásérzékelő-gyártók által kért mozgásérzékelő-adatokat (a Km-mel titkosítandó adatokat az ISO 16844-3. sz. szabvány határozza meg);

— megfelelően biztonságos eljárással továbbítaniuk kell a Km_{VU}-t a járműegységek gyártói számára, a járműegységekben való elhelyezés céljából;

— gondoskodniuk kell arról, hogy a kártya személyre szabása közben minden műhelykártyában elhelyezzék a Km_{WC} -t (`SensorInstallationSecData` a `Sensor_Installation_Data` elemi állományban).

3.1.4 *T-DES tevékenységi kulcsok generálása és elosztása*

CSM_012 A járműegységek és a tachográfkártyák a kölcsönös hitelesítési eljárás részeként létrehozzák és kicserélik a közös hármas DES munkamenetkulcs kidolgozásához szükséges adatokat. Az adatcsere titkosságát egy RSA titkosítási mechanizmus védi.

CSM_013 E kulcsot kell használni minden további, biztonságos üzenetküldést használó titkosítási művelet során. Érvényessége a munkamenet végén (a kártya kivétele vagy visszaállítása), illetve 240 használat után lejár (a kulcs egy használata = biztonságos üzenetküldés segítségével a kártyának küldött egyetlen parancs és az ahhoz tartozó válasz).

3.2. **Kulcs**

CSM_014 Az RSA-kulcsoknak az alábbi hosszúságúaknak kell lenniük (szinttől függetlenül): *n* modulus: 1 024 bit, *e* nyilvános kitevő: legfeljebb 64 bit, *d* saját kitevő: 1 024 bit.

CSM_015 A hármas DES-kulcs formája (K_a, K_b, K_a), ahol K_a és K_b független, 64 bit hosszúságú kulcs. Nem kell beállítani paritáshiba-észlelő bitet.

3.3. **Tanúsítványok**

CSM_016 Az RSA nyilvánoskulcs-tanúsítványoknak „non self-descriptive”, „Card Verifiable” tanúsítványoknak kell lenniük (hiv.: ISO/IEC 7816-8. sz. szabvány)

3.3.1 *A tanúsítványok tartalma*

CSM_017 Az RSA nyilvánoskulcs-tanúsítványok az alábbi adatokból épülnek fel, a következő sorrendben:

Adatok	Formátum	Bájt	Obs
CPI	INTEGER	1	Tanúsítványprofil-azonosító („01” ebben a változatban)
CAR	OCTET STRING	8	A tanúsító hatóság hivatkozása
CHA	OCTET STRING	7	A tanúsítvány tulajdonosának engedélye

▼B

Adatok	Formátum	Bájt	Obs
EOV	TimeReal	4	A tanúsítvány érvényességének vége. Választható, használaton kívül „FF”-fel kitöltve
CHR	OCTET STRING	8	A tanúsítvány tulajdonosának hivatkozása
n	OCTET STRING	128	Nyilvános kulcs (modulus)
e	OCTET STRING	8	Nyilvános kulcs (nyilvános kitevő)
		164	

Megjegyzések:

1. A „tanúsítványprofil-azonosító” (CPI) a hitelesítési tanúsítvány pontos szerkezetét határozza meg. A vonatkozó fejrészlista berendezési belső azonosítójaként használható, amely lista az adatelemek tanúsítványon belüli összefűzését írja le.

   Az e tanúsítványtartalommal társított fejrészlista a következő:

4D	16	5F 29	01	42	08	5F 4B	07	5F 24	04	5F 20	08	7F 49	05	81	81 80	82	08
Kiterjesztett fejrészlista címkéje	A fejrészlista hossza	CPI-címke	CPI-hossz	CAR-címke	CAR-hossz	CHA-címke	CHA-hossz	EOV-címke	EOV-hossz	CHR-címke	CHR-hossz	Nyilvános kulcs címkéje (létrehozott)	A következő DO-k hossza	moduluscímke	modulushossz	nyilvános kitevő címkéje	nyilvános kitevő hossza

2. A „tanúsító hatóság hivatkozása” (CAR) célja, hogy a tanúsítványt kiadó tanúsító hatóságot olyan módon azonosítsa, hogy az adatelemek egyidejűleg hatósági kulcsazonosítóként is felhasználhatók legyenek a tanúsító hatóság nyilvános kulcsára való hivatkozás során (a kódoláshoz lásd az alábbi kulcsazonosítót).

3. A „tanúsítvány tulajdonosának engedélye” (CHA) célja, hogy azonosítsa a tanúsítvány tulajdonosának jogosultságát. Ez a tachográf-alkalmazás azonosítójából és azon berendezés típusából áll, amelyhez a tanúsítványt szánták (az `EquipmentType` adatelemmel összhangban, tagállamok esetében ‘00’).

▼B

4. A „tanúsítvány tulajdonosának hivatkozása” (CHR) célja, hogy egyértelműen azonosítsa a tanúsítvány tulajdonosát olyan módon, hogy az adatelemek egyidejűleg alanyi kulcsazonosítóként is felhasználhatók legyenek a tanúsítvány tulajdonosának nyilvános kulcsára való hivatkozás során.

5. A kulcsazonosítók egyértelműen azonosítják a tanúsítvány tulajdonosát vagy a tanúsító hatóságokat. Kódolásuk az alábbiak szerint történik:

5.1. Berendezés (járműegység vagy kártya):

Adat	A berendezés sorozatszáma	Dátum	Típus	Gyártó
Hossz	4 bájt	2 bájt	1 bájt	1 bájt
Érték	Egész szám	hh éé BCD-kódolás	Gyártóra jellemző	Gyártói kód

A járműegység esetében a gyártó a tanúsítványok bekérésekor nem feltétlenül ismeri annak a berendezésnek az azonosítóját, amelybe a kulcsokat be kell helyezni.

Ha a gyártó ismeri a berendezés azonosítóját, a nyilvános kulccsal együtt megküldi a tagállami hatóságnak, hogy tanúsítsa. A tanúsítvány ekkor tartalmazza a berendezés azonosítóját, és a gyártónak gondoskodnia kell arról, hogy a kulcsokat és a tanúsítványt a megfelelő berendezésbe helyezzék be. A kulcsazonosító formátuma megfelel a fent ismertetett adatsornak.

Ha a gyártó nem ismeri a berendezés azonosítóját, egyedileg kell azonosítania minden egyes tanúsítási kérelmet, és ezen azonosítót a nyilvános kulccsal együtt meg kell küldenie a tagállama hatóságának, hogy hitelesítsék. A tanúsítvány tartalmazza a kért azonosítót. A gyártónak közölnie kell a tagállama hatóságával a berendezéshez tartozó kulcs hozzárendelését (azaz a tanúsítási kérelem és a berendezés azonosítását), miután a kulcsot behelyezték a berendezésbe. A kulcsazonosító alakja:

Adat	A tanúsítási kérelem sorozatszáma	Dátum	Típus	Gyártó
Hossz	4 bájt	2 bájt	1 bájt	1 bájt
Érték	Egész szám	hh éé BCD-kódolás	FF	Gyártói kód

▼B

5.2. Tanúsító hatóság

Adat	A hatóság azonosítója	A kulcs sorozatszáma	Kiegészítő információ	Azonosító
Hossz	4 bájt	1 bájt	2 bájt	1 bájt
Érték	1 bájtos nemzeti numerikus kód 3 bájtos nemzeti alfanumerikus kód	Egész szám	Kiegészítő kódolás (Tanúsító hatóságra jellemző) használaton kívül: FF FF	01

A kulcs sorozatszáma segítségével kell megkülönböztetni a különféle tagállami kulcsokat abban az esetben, ha a kulcs megváltozik.

6. A tanúsítvány ellenőrzői számára közvetve ismert, hogy a tanúsított nyilvános kulcs esetében a hitelesítés, a digitális aláírás ellenőrzése és a titkossági titkosítás szempontjából releváns RSA-kulcsról van szó (a tanúsítvány nem tartalmazza az azt meghatározó objektumazonosítót).

3.3.2 *Kiállított tanúsítványok*

CSM_018 A kiállított tanúsítvány olyan digitális aláírás, amely az ISO/IEC 9796-2. sz. szabvánnyal összhangban részben tartalmazza a tanúsítvány tartalmát (kivéve annak A4. mellékletét) a hozzáfűzött „tanúsító hatóság hivatkozásával” együtt.

$$X.C = X.CA.SK[\text{‘6A’} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{‘BC’}] \parallel C_n \parallel X.CAR$$

Az alábbi tanúsítványtartalommal: = Cc = C_r || C_n

106 bájt 58 bájt

Megjegyzések:

1. Ez a tanúsítvány 194 bájt hosszú.

2. Az aláírás által elrejtett CAR-t is hozzá kell fűzni az aláíráshoz olyan módon, hogy a tanúsító hatóság nyilvános kulcsa kiválasztható legyen a tanúsítvány hitelesítésére.

3. A tanúsítvány ellenőrzőjének közvetve ismernie kell a tanúsító hatóság által a tanúsítvány aláírására használt algoritmust.

4. A kiállított tanúsítványhoz társított fejrészlista a következő:

7F 21	09	5F 37	81 80	5F 38	3A	42	08
Kártya tanúsító bizonyítványának címkéje (létrehozott)	A következő DO-k hossza	Aláírás címke	Aláírás hossza	Maradék címke	Maradék hossza	CAR-címke	CAR-hossz

▼B

3.3.3 *A tanúsítvány ellenőrzése és kicsomagolása*

A tanúsítvány ellenőrzése és kicsomagolása kiterjed az aláírás ISO/IEC 9796-2. sz. szabvánnyal összhangban történő ellenőrzésére, amivel a tanúsítvány tartalma és a benne lévő X.PK = X.CA.PK $_o$ X.C nyilvános kulcs kiemelhető, valamint a tanúsítvány érvényességének ellenőrzésére.

CSM_019 Az alábbi lépéseket tartalmazza:

az aláírás ellenőrzése és a tartalom kiemelése:

— az X.C-ből ki kell emelni a Sign-t, a C_n'-t és a CAR' értéket: X.C = Sign || C_n' || CAR'

Sign	C_n'	CAR'
128 bájt	58 bájt	8 bájt

— a CAR' értékből ki kell választani a megfelelő tanúsító hatóság nyilvános kulcsát (ha ez eddig más módon még nem történt meg),

— meg kell nyitni a Sign-t a tanúsító hatóság nyilvános kulcsával: Sr'= X.CA.PK [Sign],

— ellenőrizni kell, hogy az Sr' '6A'-val kezdődik és 'BC'-vel végződik,

— ki kell számítani a C_r' és a H' értéket az alábbiakból: Sr' = 6A || C_r' || H' || BC

C_r'	H'
106 bájt	20 bájt

— helyre kell állítani a tanúsítvány tartalmát: C_r' || C_n',

— ellenőrizni kell, hogy *Hash*(C') = H'.

Ha az ellenőrzések rendben vannak, a tanúsítvány eredeti, és a tartalma C'.

Az érvényesség ellenőrzése. A C'-ből:

— ha alkalmazható, ellenőrizni kell az érvényességi dátum végét.

A nyilvános kulcs, a kulcsazonosító, a tanúsítványtulajdonos engedélyének és a tanúsítványérvényesség végének visszakeresése C'-ből, illetve tárolása:

— X.PK = *n* || *e*

— X.KID = CHR,

— X.CHA = CHA,

— X.EOV = EOV.

4. KÖLCSÖNÖS HITELESÍTÉSI MECHANIZMUS

A kártyák és a járműegységek közötti kölcsönös hitelesítés az alábbi elven alapul:

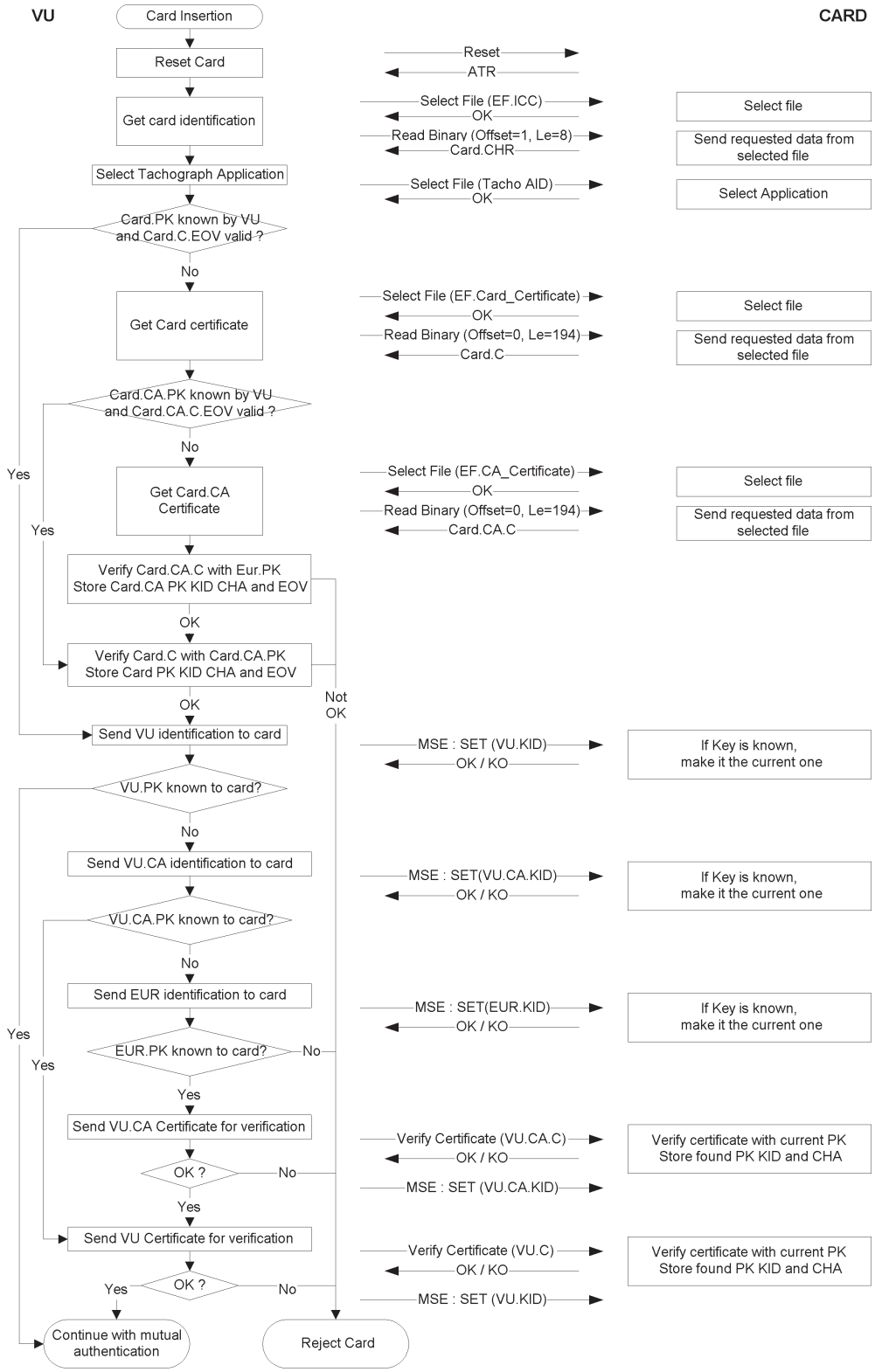
Mindkét résztvevő tanúsítja a másik résztvevőnek, hogy olyan érvényes kulcspárral rendelkezik, amelynek nyilvános kulcsát az európai tanúsító hatóság által tanúsított tagállami tanúsító hatóság tanúsította.

A tanúsítás a másik fél által küldött véletlen számnak a saját kulccsal történő aláírásával történik; a másik félnek ezen aláírás ellenőrzésekor vissza kell állítania a véletlenszerű számot.

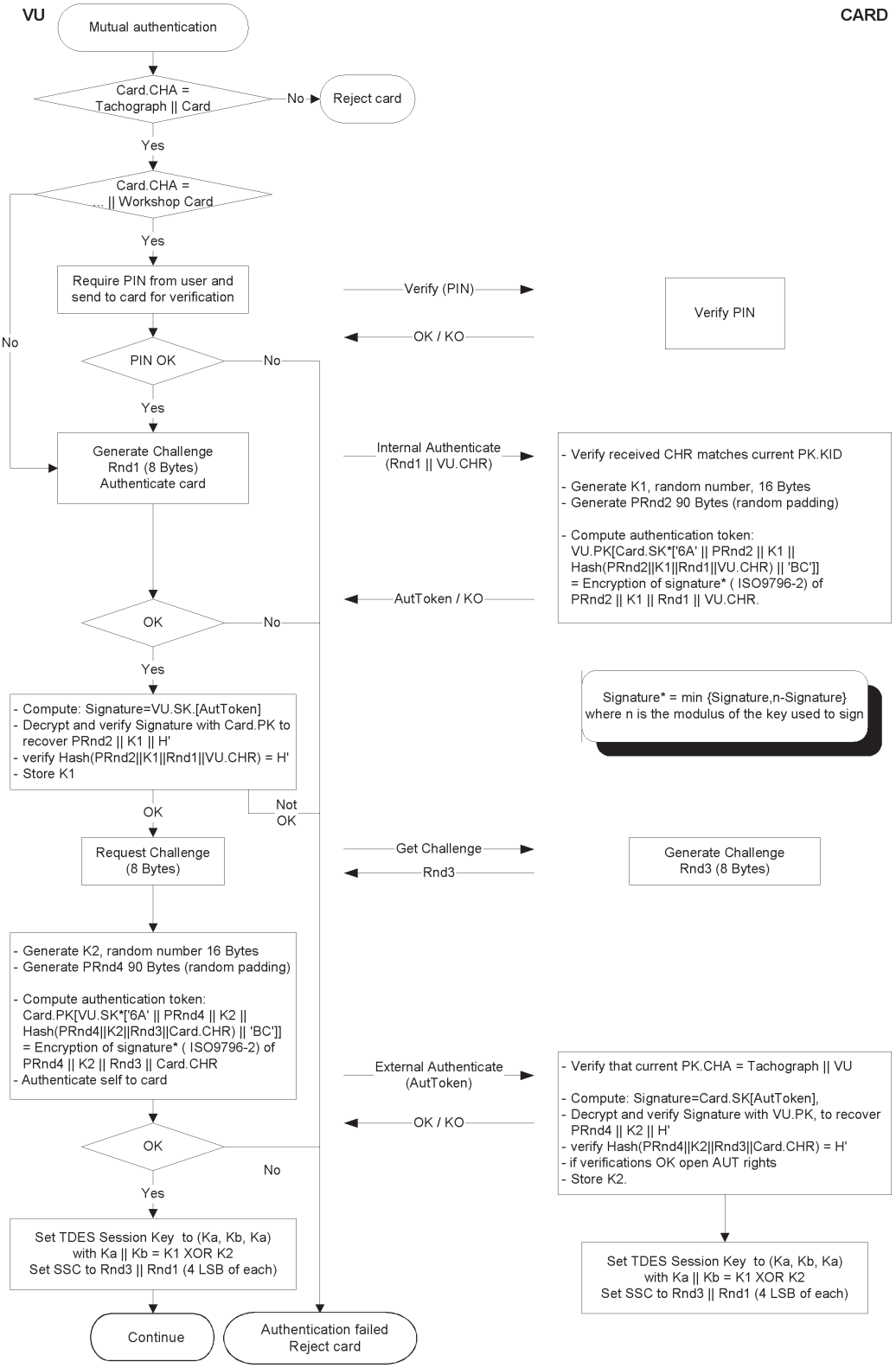
A mechanizmust a kártya járműegységbe való behelyezése váltja ki. Ez a tanúsítványok cseréjével és a nyilvános kulcsok kicsomagolásával kezdődik, és a munkamenetkulcs beállításával végződik.

▼B

CSM_020 A következő protokollt kell használni (a nyilak a parancsokat és a kicserélt adatokat jelzik ([lásd 2. függelék]):



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. A JÁRMŰEGYSÉGKÁRTYÁK ADATÁTVITELLEL KAPCSOLATOS TITKOSSÁGI, INTEGRITÁSI ÉS HITELESÍTÉSI MECHANIZMUSA

5.1. **Biztonságos üzenetküldés**

CSM_021 A járműegységkártyák adatátviteli integritását biztonságos üzenetküldés védi az ISO/IEC 7816-4. sz. és az ISO/IEC 7816-8. sz. hivatkozással összhangban.

CSM_022 Ha az adatokat védeni kell átvitel közben, „titkosítási ellenőrző összeg” adatobjektumot kell fűzni a parancson vagy a válaszon belül küldött adatobjektumokhoz. A fogadó fél ellenőrzi a titkosítási ellenőrző összeget.

CSM_023 A parancson belül küldött adatok titkosítási ellenőrző összege a parancsfejet és az összes elküldött adatobjektumot (= > CLA = 0C, és minden adatobjektumot címkék vesznek körül, amelyekben b1 = 1) tartalmazza.

CSM_024 A válasz állapotinformációs bájtjait titkosítási ellenőrző összeg védi, amennyiben a válasz nem tartalmaz adatmezőt.

CSM_025 A titkosítási ellenőrző összegek négy bájt hosszúságúak.

A parancsok és a válaszok biztonságos üzenetküldéskor ezért az alábbiak szerint épülnek fel:

A felhasznált DO-k az ISO/IEC 7816-4. sz. szabványban leírt biztonságos üzenetküldési DO-k részhalmazai:

Címke	Rövidítés	Jelentés
81	T_{PV}	Egyszerű értékű nem BER-TLV-ben kódolt adat (CC-vel védendő)
97	$\mathbf{T_{LE}}$	Az Le értéke a biztosítatlan parancsban (CC-vel védendő)
99	T_{SW}	Állapotinformáció (CC-vel védendő)
8E	T_{CC}	Titkosítási ellenőrző összeg
87	$T_{PI\ CG}$	Kitöltésjelző bájt || Kriptogram (Egyszerű értékű nem BER-TLV-ben kódolt adat)

▼B

Biztosítatlan parancsválasz-pár esetében:

Parancsfej				Parancstörzs		
CLA	INS	P1	P2	[L_c mező]	[Adatmező]	[L_e mező]
négy bájt				L bájt, jelzésük B_1–B_L		

Választörzs	A válasz vége	
[Adatmező]	SW1	SW2
L_r adatbájt	két bájt	

A megfelelő biztosított parancsválasz-pár:

Biztosított parancs:

Parancsfej (CH)				Parancstörzs										
CLA	INS	P1	P2	[Új L_c mező]	[Új adatmező]									[Új L_e mező]
OC				Az új adatmező hossza	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	00
					81	L_c	Adatmező	97	01	L_e	8E	04	CC	

Az ellenőrző összegbe integrálandó adatok = CH | PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = kitöltőbájtok (80 .. 00) az ISO-IEC 7816-4. sz. és az ISO 9797. sz. szabvány 2. módszerével összhangban.

A DO-k, a PV és az LE csak akkor vannak jelen, ha van bizonyos számú megfelelő adat a biztosítatlan parancsban.

Biztosított válasz:

1. Amennyiben a válasz adatmezője nem üres, és nem kell titkossági védelmet biztosítani a számára:

Választörzs						A válasz vége
[Új adatmező]						új SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
81	L_r	Adatmező	8E	04	CC	

Az ellenőrző összegbe integrálandó adatok = T_{PV} || L_{PV} || PV || PB

2. Amennyiben a válasz adatmezője nem üres, és titkossági védelmet kell biztosítani a számára:

▼B

Választörzs						A válasz vége
[Új adatmező]						új SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
87		PI || CG	8E	04	CC	

A CG által továbbítandó adatok: nem BER-TLV-ben kódolt adatok és kitöltőbájtok.

Az ellenőrző összegbe integrálandó adatok = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Amennyiben a válasz adatmezője üres:

Választörzs						A válasz vége
[Új adatmező]						új SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
99	02	Új SW1 SW2	8E	04	CC	

Az ellenőrző összegbe integrálandó adatok = T_{SW} || L_{SW} || SW || PB

5.2. **A biztonságos üzenetküldéssel kapcsolatos hibák kezelése**

CSM_026 Amennyiben a tachográfkártya SM-hibát észlel, miközben parancsot értelmez, az állapotbájtokat SM nélkül kell visszaküldeni. Az ISO/IEC 7816-4. sz. szabvánnyal összhangban, az alábbiak szerint definiált állapotbájtok jelzik az SM-hibákat:

66 88: a titkosítási ellenőrző összeg hitelesítése hibás,

69 87: a várt SM-adatobjektumok hiányoznak,

69 88: az SM-adatobjektumok helytelenek.

CSM_027 Ha a tachográfkártya SM DO-k nélküli vagy hibás SM DO-t tartalmazó állapotbájtokat küld vissza, a járműegységnek meg kell szakítania a munkamenetet.

5.3. **A titkosítási ellenőrző összeget kiszámító algoritmus**

CSM_028 A titkosítási ellenőrző összeg létrehozása egy szokásos MAC segítségével történik, DES-sel rendelkező ANSI X9.19-cel összhangban:

— kezdő állapot: az y0 kezdő ellenőrző tömb E(Ka, SSC);

— szekvenciális állapot: az y1, … yn ellenőrző tömbök kiszámítása a Ka segítségével történik;

— végső állapot: a titkosítási ellenőrző összeg kiszámítása az utolsó yn ellenőrző tömb alapján történik az alábbiak szerint: E(Ka, D(Kb, yn)).

ahol az E() rövidítés a DES segítségével történő titkosítást, a D() rövidítés pedig a DES segítségével történő visszafejtést jelenti.

A titkosítási ellenőrző összeg négy legjelentősebb bájtját továbbítani kell.

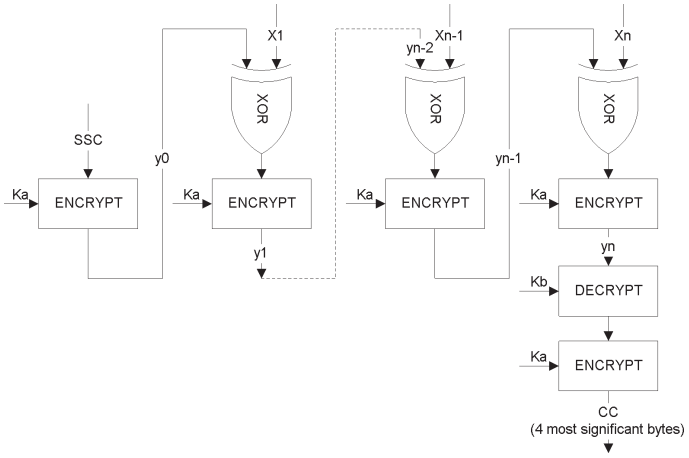
▼B

CSM_029 A küldési sorrendszámláló (SSC) indítását a kulcsegyeztetési eljárás során a következők szerint kell elvégezni:

Kezdő SSC: Rnd3 (4 legjelentéktelenebb bájt) || Rnd1 (4 legjelentéktelenebb bájt).

CSM_030 A küldési sorrendszámláló minden alkalommal 1-gyel növekszik a MAC kiszámítása előtt (azaz az első parancs SSC-je a kezdő SSC +1, az első válasz SSC-je pedig a kezdő SSC + 2).

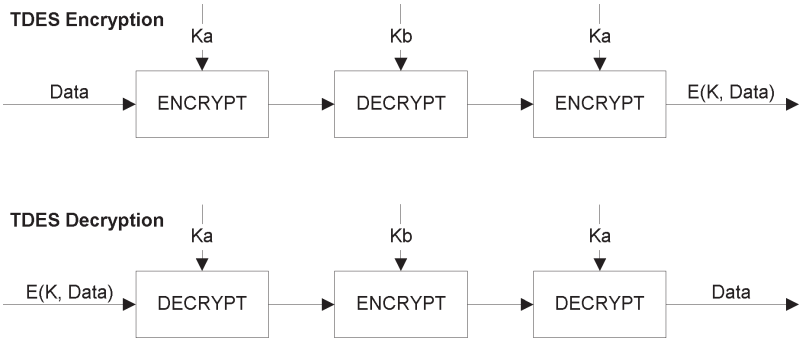
A MAC kiszámítását az alábbi ábra szemlélteti:



5.4. **A titkossági DO-utasítások kriptogramjait kiszámító algoritmus**

CSM_031 A kriptogramok kiszámítása a TCBC-üzemmódban használt TDEA segítségével, a (TDES) és (TDES-OP) hivatkozással összhangban és a nulla vektorral mint kezdő értéktömbbel történik.

A kulcsok alkalmazását a TDES-ben az alábbi táblázat szemlélteti:



▼B

6. AZ ADATLETÖLTÉS DIGITÁLIS ALÁÍRÁSI MECHANIZMUSAI

CSM_032 Az intelligens kijelölt berendezés (IDE) egyetlen fizikai adatállományon belül tárolja a berendezésektől (járműegység vagy kártya) a letöltési munkamenet során kapott adatokat. Ezen állománynak az MS_i.C és EQT.C tanúsítványokat kell tartalmaznia. Az állomány az adattömböknek a 7. függelékben (Adatletöltési protokollok) meghatározott digitális aláírásait tartalmazza.

CSM_033 A letöltött adatok digitális aláírásainak olyan digitális aláírási rendszert kell használniuk, amelynek függeléke adott esetben lehetővé teszi a letöltött adatok visszakódolás nélküli olvasását.

6.1. **Aláírások generálása**

CSM_034 Az adataláírások berendezés általi generálásának olyan aláírási rendszert kell követnie, amelynek függeléke a (PKCS1) hivatkozásban van meghatározva az SHA-1 hasító funkcióval:

Aláírás = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Kitöltőbájt-oktettek 128 hosszúságú ‘FF’ értékkel.

DER(SHA-1(*M*)) az ID algoritmus kódolása a hasító funkció esetében és a hasító érték DigestInfo típusú ASN.1 értékké való kódolása (megkülönböztetett kódolási szabályok):

30||21||30||09||06||05||2B||0E||03||02||1A||05||00||04||14|| Hasító érték.

6.2. **Aláírások ellenőrzése**

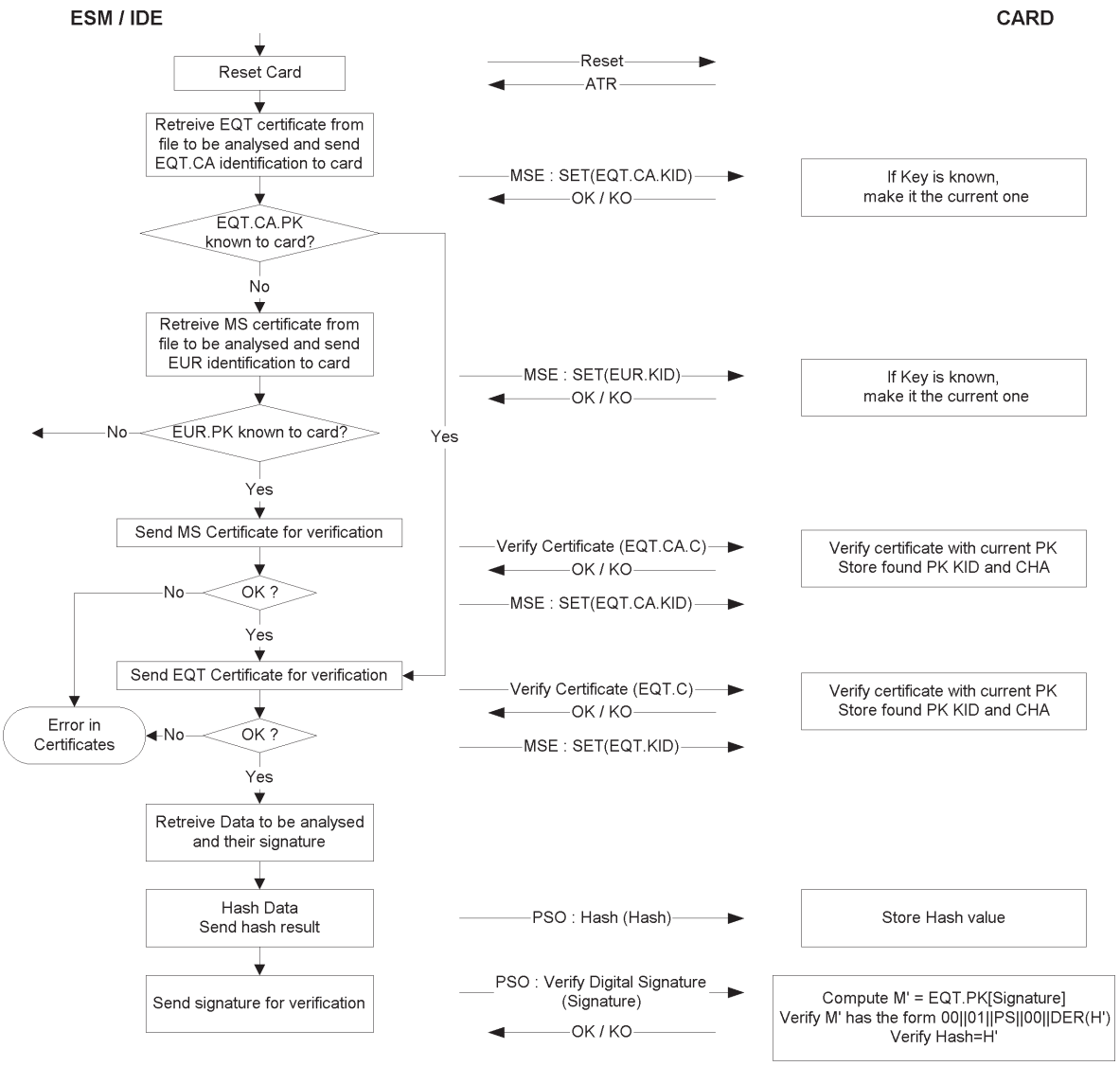
CSM_035 Az adataláírások letöltött adatokon való ellenőrzésének olyan aláírási rendszert kell követnie, amelynek függeléke a (PKCS1) hivatkozásban van meghatározva az SHA-1 hasító funkcióval.

A hitelesítőnek ismernie kell (és jóvá kell hagynia) az EUR.PK európai nyilvános kulcsot.

Az alábbi táblázat egy ellenőrzőkártyát hordozó IDE által követhető protokollt szemléltet, a letöltött és ESM-en (külső tárolóeszközön) tárolt adatok integritásának ellenőrzéséhez. Az ellenőrzőkártya segítségével kell elvégezni a digitális aláírások visszakódolását. Ebben az esetben e funkció nem hajtható végre az IDE-n belül.

Az EQT jelöli azt a berendezést, amely letöltötte és aláírta az elemzendő adatokat.

▼B



B. RÉSZ

MÁSODIK GENERÁCIÓS MENETÍRÓ RENDSZER

7. BEVEZETÉS

7.1. **Hivatkozások**

A függelék ezen része az alábbi hivatkozásokat használja.

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 2001. november 26.
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), 2013. július
ISO 7816-4	ISO/IEC 7816-4, Azonosító kártyák. Integrált áramkörös kártyák. 4. rész: Szervezet, biztonság és parancsok adatcseréhez. Harmadik kiadás: 2013. április 15.
ISO 7816-8	ISO/IEC 7816-8, Azonosító kártyák. Integrált áramkörös kártyák. 8. rész: Biztonsági műveletek parancsai. Második kiadás: 2004. június 1.

▼B

ISO 8825-1	ISO/IEC 8825-1, Információtechnológia. ASN.1. kódolási szabályok: Alapvető kódolási szabályok meghatározása (BER), kanonikus kódolási szabályok (CER) és megkülönböztetett kódolási szabályok (DER). Negyedik kiadás: 2008. december 15.
ISO 9797-1	ISO/IEC 9797-1, Információtechnológia. Biztonsági technikák. Üzenethitelesítési kódok (MAC-ek). 1. rész: Blokktitkosítást alkalmazó mechanizmusok. Második kiadás: 2011. március 1.
ISO 10116	ISO/IEC 10116, Információtechnológia. Biztonsági technikák. Az *n* bites blokktitkosítás üzemmódjai. Harmadik kiadás: 2006. február 1.
ISO 16844-3	ISO/IEC 16844-3, Közúti járművek. Tachográfrendszerek. 3. rész: Mozgásérzékelő-interfész. 2004-es első kiadás, a műszaki változtatásokat is ideértve (2006. 01.)
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, 2009. március
RFC 5639	Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), 2010. május
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, 2012. március
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012. június 28.

7.2. **Jelzések és rövidítések**

E függelék az alábbi jelzéseket és rövidítéseket használja:

AES	Advanced Encryption Standard – Fejlett titkosítási szabvány
CA	Certificate Authority – Tanúsító hatóság
CAR	Certificate Authority Reference – A tanúsító hatóság hivatkozása
CBC	Cipher Block Chaining (mode of operation) – Titkosított blokkok láncolata (üzemmód)
CH	Command Header – Parancsfej
CHA	Certificate Holder Authorisation – A tanúsítvány tulajdonosának engedélye
CHR	Certificate Holder Reference – A tanúsítvány tulajdonosának hivatkozása
CV	Constant Vector – Állandóvektor
DER	Distinguished Encoding Rules – Megkülönböztetett kódolási szabályok
DO	Data Object – Adatobjektum
DSRC	Dedicated Short Range Communication – Célorientált rövid távolságú adatkommunikáció
ECC	Elliptic Curve Cryptography – Elliptikus görbéken alapuló kriptográfia
ECDSA	Elliptic Curve Digital Signature Algorithm – Elliptikus görbéken alapuló digitális aláírási algoritmus
ECDH	Elliptic Curve Diffie-Hellman (key agreement algorithm) – Elliptikus görbéken alapuló Diffie-Hellman algoritmus (kulcsegyeztetési algoritmus)
EGF	External GNSS Facility – Külső GNSS-eszköz
EQT	Equipment – Berendezés

▼B

IDE	Intelligent Dedicated Equipment – Intelligens kijelölt berendezés
K_M	Motion Sensor Master Key, allowing the pairing of a Vehicle Unit to a Motion Sensor – Mozgásérzékelő mesterkulcsa, amely lehetővé teszi a járműegység és a mozgásérzékelő párosítását
$K_{M\text{-}VU}$	Key inserted in vehicle units, allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU – Járműegységekbe behelyezett kulcs, amelylyel a járműegység képes meghatározni a mozgásérzékelő mesterkulcsát, ha műhelykártyát helyeznek be a járműegységbe
$K_{M\text{-}WC}$	Key inserted in workshop cards, allowing a VU to derive the Motion Sensor Master Key if a workshop card is inserted into the VU – Műhelykártyákba behelyezett kulcs, amellyel a járműegység képes meghatározni a mozgásérzékelő mesterkulcsát, ha műhelykártyát helyeznek be a járműegységbe
MAC	Message Authentication Code – Üzenethitelesítési kód
MoS	Motion Sensor – Mozgásérzékelő
MSB	Most Significant Bit – Legjelentősebb bit
PKI	Public Key Infrastructure – Nyilvános kulcsú infrastruktúra
RCF	Remote Communication Facility – Távoli kommunikációs egység
SSC	Send Sequence Counter – Küldési sorrendszámláló
SM	Secure Messaging – Biztonságos üzenetküldés
TDES	Triple Data Encryption Standard – Háromszoros adattitkosítási szabvány
TLV	Tag Length Value – A címke hosszának értéke
VU	Vehicle Unit – Járműegység
X.C	The public key certificate of user X – X felhasználó nyilvánoskulcs-tanúsítványa
X.CA	The certificate authority that issued the certificate of user X – Az X felhasználó tanúsítványát kibocsátó tanúsító hatóság
X.CAR	The certificate authority reference mentioned in the certificate of user X – Az X felhasználó tanúsítványában feltüntetett tanúsítóhatóság-hivatkozás
X.CHR	The certificate holder reference mentioned in the certificate of user X – Az X felhasználó tanúsítványában feltüntetett tanúsítványtulajdonos-hivatkozás
X.PK	Public key of user X – X felhasználó nyilvános kulcsa
X.SK	Private key of user X – X felhasználó privát kulcsa
$X.PK_{eph}$	Ephemeral public key of user X – X felhasználó átmeneti nyilvános kulcsa
$X.SK_{eph}$	Ephemeral private key of user X – X felhasználó átmeneti privát kulcsa
xx	A hexadecimal value – hexadecimális érték
||	Concatenation operator – összefűzési operátor

7.3. **Fogalommeghatározások**

A függelékben használt kifejezések fogalommeghatározásai az 1C. melléklet I. szakaszában találhatók.

8. TITKOSÍTÁSI RENDSZEREK ÉS ALGORITMUSOK

8.1. **Titkosítási rendszerek**

CSM_38 A járműegységeknek és a tachográfkártyáknak elliptikus görbéken alapuló nyilvános kulcsú titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegységek és a kártyák közötti kölcsönös hitelesítés;

▼B

— AES-munkamenetkulcsok egyeztetése a járműegységek és a kártyák között;

— a járműegységekről vagy a tachográfkártyákról külső tárolóeszközre letöltött adatok hitelessége, integritása és letagadhatatlansága.

CSM_39 A járműegységeknek és a külső GNSS-eszközöknek elliptikus görbéken alapuló nyilvános kulcsú titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegységek külső GNSS-eszközzel történő összekapcsolása;

— kölcsönös hitelesítés a járműegységek és egy külső GNSS-eszköz között;

— AES-munkamenetkulcs egyeztetése a járműegységek és egy külső GNSS-eszköz között.

CSM_40 A járműegységeknek és a tachográfkártyáknak AES-alapú szimmetrikus titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegység és a tachográfkártya között kicserélt adatok hitelessége és integritása;

— szükség esetén a járműegység és a tachográfkártya között kicserélt adatok titkossága.

CSM_41 A járműegységeknek és a külső GNSS-eszközöknek AES-alapú szimmetrikus titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegység és a külső GNSS-eszköz között kicserélt adatok hitelessége és integritása.

CSM_42 A járműegységeknek és a mozgásérzékelőknek AES-alapú szimmetrikus titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegység párosítása mozgásérzékelővel;

— a járműegység és egy mozgásérzékelő közötti kölcsönös hitelesítés;

— szükség esetén a járműegység és a mozgásérzékelő között kicserélt adatok titkossága.

CSM_43 A járműegységeknek és az ellenőrzőkártyáknak AES-alapú szimmetrikus titkosítási rendszer segítségével az alábbi biztonsági szolgáltatásokat kell biztosítaniuk:

— a járműegység és az ellenőrzőkártya között kicserélt adatok titkossága, hitelessége és integritása.

Megjegyzések:

— Az adatok átvitelére tulajdonképpen egy ellenőrző tisztviselő felügyelete alatt kerül sor a járműegységről egy távoli lekérdezőegységre, a járműegységhez tartozó belső vagy külső távoli kommunikációs egység használatával (lásd a 14. függeléket). A távoli lekérdezőegység

▼B

azonban a fogadott adatokat egy ellenőrzőkártyára küldi visszafejtés és a hitelesség ellenőrzése céljából. Biztonsági szempontból a távoli kommunikációs egység és a távoli lekérdezőegység teljesen transzparens.

— A műhelykártya ugyanazokat a biztonsági szolgáltatásokat kínálja a DSRC-interfésznek, mint az ellenőrzőkártya. A műhely így ellenőrizheti a járműegység távoli kommunikációs interfészének működését, a biztonsági funkciókat is beleértve. További információkért lásd a 9.2.2. szakaszt.

8.2. **Titkosítási algoritmusok**

8.2.1 *Szimmetrikus algoritmusok*

CSM_44 A járműegységeknek, a tachográfkártyáknak, a mozgásérzékelőknek és a külső GNSS-eszközöknek 128, 192 és 256 bites kulcshosszokkal kell támogatniuk az [AES] által definiált AES algoritmust.

8.2.2 *Aszimmetrikus algoritmusok és szabványosított tartományparaméterek*

CSM_45 A járműegységeknek, a tachográfkártyáknak és a külső GNSS-eszközöknek 256, 384 és 512/521 bites kulcsméretekkel kell támogatniuk az elliptikus görbéken alapuló kriptográfiát.

CSM_46 A járműegységeknek, a tachográfkártyáknak és a külső GNSS-eszközöknek a [DSS] definíciója alapján támogatniuk kell az ECDSA aláírási algoritmust.

CSM_47 A járműegységeknek, a tachográfkártyáknak és a külső GNSS-eszközöknek a [TR 03111] definíciója alapján támogatniuk kell az ECKA-EG kulcsegyeztetési algoritmust.

CSM_48 A járműegységeknek, a tachográfkártyáknak és a külső GNSS-eszközöknek az 1. táblázat összes, az elliptikus görbéken alapuló kriptográfiához meghatározott szabványosított tartományparaméterét támogatniuk kell.

1. táblázat

Szabványosított tartományparaméterek

Név	Méret (bit)	Hivatkozás	Objektumazonosító
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

▼B

Megjegyzés: az 1. táblázat utolsó oszlopában szereplő objektumazonosítókat az [RFC 5639] határozza meg a Brainpool-görbékhez, az [RFC 5480] pedig a NIST-görbékhez.

1. példa: A BrainpoolP256r1 görbe objektumazonosítója {iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}.

Pontokkal tagolt jelöléssel: 1.3.36.3.3.2.8.1.1.7.

2. példa: A NIST P-384 görbe objektumazonosítója

{iso(1) identified-organization(3) certicom(132) curve(0) 34}.

Pontokkal tagolt jelöléssel: 1.3.132.0.34.

8.2.3 *Hasító algoritmusok*

CSM_49 A járműegységeknek és a tachográfkártyáknak támogatniuk kell az SHA-256, SHA-384 és SHA-512 algoritmusokat az [SHS] előírásai szerint.

8.2.4 *Titkosítási készletek*

CSM_50 Ha egy szimmetrikus algoritmust, egy aszimmetrikus algoritmust és/vagy egy hasító algoritmust együtt alkalmazva képeznek biztonsági protokollt, akkor ezek kulcshosszainak és hasítási méreteinek (közelítőleg) egyenlőnek kell lenniük. A 2. táblázat a megengedett titkosítási készleteket tartalmazza:

2. táblázat

Megengedett titkosítási készletek

Titkosítási készlet azonosítója	ECC-kulcsméret (bit)	AES-kulcshossz (bit)	Hasító algoritmus	MAC-hossz (bájt)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Megjegyzés: az 512 bites és 521 bites kulcsméretű ECC-kulcsokat ebben a függelékben azonos erősségűnek tekintjük.

9. KULCSOK ÉS TANÚSÍTVÁNYOK

9.1. **Aszimmetrikus kulcspárok és nyilvánoskulcs-tanúsítványok**

9.1.1 *Általános tudnivalók*

Megjegyzés: az ebben a szakaszban ismertetett kulcsokat a járműegységek és a tachográfkártyák, valamint a járműegységek és a GNSS-eszközök közötti kölcsönös hitelesítéshez és biztonságos üzenetküldéshez használják. Ezeknek a folyamatoknak a részletes leírása e függelék 10. és 11. fejezetében található.

CSM_51 Az európai intelligens menetírókészülék-rendszerben három funkcionális hierarchiaszinten kell létrehozni és kezelni az ECC-kulcspárokat és azoknak megfelelő tanúsítványokat:

— európai szint;

— tagállami szint;

— berendezési szint.

▼B

CSM_52 A teljes európai intelligens menetírókészülék-rendszerben szabványos és biztonságos módszerek használatával kell nyilvános és privát kulcsokat létrehozni, kezelni és kommunikálni.

9.1.2 *Európai szint*

CSM_53 Európai szinten egyetlen egyedi ECC-kulcspárt kell létrehozni, EUR megnevezéssel. Ennek egy privát kulcsból (EUR.SK) és egy nyilvános kulcsból kell állnia (EUR.PK). Ez a kulcspár az európai intelligens menetíró készülékek teljes nyilvános kulcsú infrastruktúrájának (PKI) gyökérkulcspárja. Ezt a feladatot egy európai gyökértanúsítványokat kezelő hatóság (az ERCA) látja el az Európai Bizottság felügyeletével.

CSM_54 Az ERCA-nak az európai nyilvános kulcs használatával kell aláírnia az európai nyilvános kulcs egy (önaláírt) gyökértanúsítványát, és ezt az európai gyökértanúsítványt minden tagállamnak át kell adnia.

CSM_55 Az ERCA-nak kérésre az európai privát kulcs használatával kell aláírnia a tagállamok nyilvános kulcsainak tanúsítványait. Az ERCA-nak a tagállamok minden aláírt nyilvánoskulcs-tanúsítványáról nyilvántartást kell vezetnie.

CSM_56 Ahogy az 1. ábra mutatja (9.1.7. szakasz), az ERCA-nak 17 évente kell új európai gyökérkulcspárt létrehoznia. Amikor az ERCA új európai gyökérkulcspárt készít, egyben új önaláírt gyökértanúsítványt is létrehoz az új európai nyilvános kulcshoz. Az európai gyökértanúsítvány érvényességi időszaka 34 év és 3 hónap.

Megjegyzés: az új gyökérkulcspár bevezetése azt is jelenti, hogy az ERCA új mozgásérzékelő mesterkulcsot és DSRC-mesterkulcsot hoz létre (lásd: 9.2.1.2. és 9.2.2.2. szakasz).

CSM_57 Az új európai gyökérkulcspár létrehozása előtt az ERCA-nak meg kell vizsgálnia és meg kell állapítania az új kulcspárhoz szükséges titkosítási erősséget, figyelembe véve, hogy a kulcspárnak az elkövetkező 34 éven keresztül biztonságosnak kell maradnia. Szükség esetén az ERCA-nak a jelenleginél erősebb titkosítási készletre kell átváltania (a következőben leírtak szerint: CSM_50).

CSM_58 Az új európai gyökérkulcspár elkészítésekor az ERCA-nak egy hivatkozási tanúsítványt kell létrehoznia az új európai nyilvános kulcshoz, és azt az előző európai privát kulcs használatával alá kell írnia. A hivatkozási tanúsítvány érvényességi időszaka 17 év. Ezt az 1. ábra illusztrálja a 9.1.7. szakaszban.

Megjegyzés: mivel tartalmazza az ERCA *X*. generációs nyilvános kulcsát, továbbá az ERCA *X-1*. generációs privát kulcsával van aláírva, a hivatkozási tanúsítvány alkalmas módszert kínál az *X-1*. generáció alatt kibocsátott berendezéseknek arra, hogy megbízhatónak tekintsék az *X*. generáció alatt kibocsátott berendezéseket.

CSM_59 Az ERCA semmilyen célra nem használhatja a gyökérkulcspár privát kulcsát azt követően, hogy új, gyökérkulccsal aláírt tanúsítvány lép érvénybe.

▼B

CSM_60 Az ERCA mindenkor rendelkezik a következő titkosítási kulcsokkal és tanúsítványokkal:

— A jelenlegi EUR-kulcspár és a megfelelő tanúsítvány.

— Minden korábbi EUR-tanúsítvány a még érvényben lévő MSCA-tanúsítványok ellenőrzéséhez.

— Hivatkozási tanúsítványok az EUR-tanúsítványok összes generációjához, az elsőt kivéve.

9.1.3 *Tagállami szint*

CSM_61 Tagállami szinten minden, tachográfkártya-tanúsítvány aláírására kötelezett tagállamnak egy vagy több egyedi ECC-kulcspárt kell létrehoznia, MSCA_Card megnevezéssel. A járműegységekhez vagy külső GNSS-eszközökhöz tartozó tanúsítványok aláírására kötelezett tagállamok ezenfelül egy vagy több MSCA_VU-EGF megnevezésű egyedi ECC-kulcspárt is létrehoznak.

CSM_62 A tagállami kulcspárok létrehozásának feladatát egy tagállami tanúsító hatóság (MSCA) végzi. Amikor egy MSCA tagállami kulcspárt hoz létre, a nyilvános kulcsot el kell küldenie az ERCA számára, hogy ily módon beszerezhesse az ERCA által aláírt megfelelő tagállami tanúsítványt.

CSM_63 Az MSCA-nak úgy kell megválasztania a tagállami kulcspár erősségét, hogy megegyezzen a megfelelő tagállami tanúsítvány aláírásához használt európai gyökérkulcspár erősségével.

CSM_64 Az MSCA_VU-EGF kulcspárnak (ha van ilyen) az MSCA_VU-EGF.SK privát kulcsból és az MSCA_VU-EGF.PK nyilvános kulcsból kell állnia. Az MSCA az MSCA_VU-EGF.SK privát kulcsot kizárólag a járműegységek és a külső GNSS-eszközök nyilvánoskulcs-tanúsítványainak aláírására használhatja.

CSM_65 Az MSCA_Card kulcspárnak az MSCA_Card.SK privát kulcsból és az MSCA_Card.PK nyilvános kulcsból kell állnia. Az MSCA az MSCA_Card.SK privát kulcsot kizárólag a tachográfkártyák nyilvánoskulcs-tanúsítványainak aláírására használhatja.

CSM_66 Az MSCA nyilvántartást vezet a járműegységek, a külső GNSS-eszközök és a kártyák összes aláírt tanúsítványáról, valamint azokról a készülékekről, amelyekhez az egyes tanúsítványokat létrehozták.

CSM_67 Az MSCA_VU-EGF tanúsítvány érvényességi időszaka 17 év és 3 hónap. Az MSCA_Card tanúsítvány érvényességi időszaka 7 év és 1 hónap.

CSM_68 Az MSCA_VU-EGF kulcspár privát kulcsának és az MSCA_Card kulcspár privát kulcsának használati időszaka két év (lásd a 9.1.7. szakasz 1. ábráját).

▼B

CSM_69 Az MSCA semmilyen célra nem használhatja az MSCA_VU-EGF kulcspár privát kulcsát a használati időszak lejártát követően. Az MSCA az MSCA_Card kulcspár privát kulcsát sem használhatja semmilyen célra a használati időszak lejártát követően.

CSM_70 Az MSCA mindenkor rendelkezik a következő titkosítási kulcsokkal és tanúsítványokkal:

— A jelenlegi MSCA_Card kulcspár és a megfelelő tanúsítvány.

— Minden korábbi MSCA_Card tanúsítvány a még érvényben lévő tachográfkártyák tanúsítványainak ellenőrzéséhez.

— Az aktuális MSCA-tanúsítvány ellenőrzéséhez szükséges jelenlegi EUR-tanúsítvány.

— A még érvényben lévő MSCA-tanúsítványok ellenőrzéséhez szükséges minden korábbi EUR-tanúsítvány.

CSM_71 Ha egy MSCA-nak járműegységek vagy külső GNSS-eszközök számára kell tanúsítványokat aláírnia, akkor a következő kulcsokkal és tanúsítványokkal is rendelkeznie kell:

— A jelenlegi MSCA_VU-EGF kulcspár és a megfelelő tanúsítvány.

— Minden korábbi MSCA_VU-EGF nyilvános kulcs a járműegységek vagy GNSS-eszközök még érvényben lévő tanúsítványainak ellenőrzéséhez.

9.1.4 *Berendezési szint: Járműegységek*

CSM_72 Minden egyes járműegységhez két egyedi ECC-kulcspárt kell létrehozni, VU_MA és VU_Sign megnevezéssel. Ezt a feladatot a járműegységek gyártói végzik. Egy járműegység-kulcspár létrehozásakor a kulcsot létrehozó félnek el kell küldenie a nyilvános kulcsot a székhelye szerinti ország MSCA-ja számára, hogy beszerezze az MSCA által aláírt megfelelő járműegység-tanúsítványt. A privát kulcsot csak a járműegység használhatja.

CSM_73 Egy adott járműegység VU_MA és VU_Sign tanúsítványainak hatálybalépési dátuma megegyezik.

CSM_74 A járműegység gyártójának úgy kell megválasztania a járműegység-kulcspár erősségét, hogy az megegyezzen a megfelelő járműegység-tanúsítvány aláírásához használt MSCA-kulcspár erősségével.

CSM_75 A járműegység a VU_MA kulcspárt – amely a VU_MA.SK privát kulcsból és a VU_MA.PK nyilvános kulcsból áll – kizárólag arra használhatja, hogy járműegység-hitelesítést végezzen a tachográfkártyák és külső GNSS-eszközök felé az e függelék 10.3. és 11.4. szakaszában leírtaknak megfelelően.

CSM_76 A járműegységnek képesnek kell lennie ideiglenes ECC-kulcspárok létrehozására, és az ideiglenes kulcspárt kizárólag arra a célra használhatja, hogy munkamenetkulcs-egyeztetést végezzen egy tachográfkártyával vagy külső GNSS-eszközzel az e függelék 10.4. és 11.4. szakaszában leírtaknak megfelelően.

▼B

CSM_77 A járműegység a VU_Sign kulcspárhoz tartozó VU_Sign.SK privát kulcsot kizárólag arra használhatja, hogy aláírja a letöltött adatfájlokat az e függelék 14. fejezetében leírtaknak megfelelően. A megfelelő VU_Sign.PK nyilvános kulcs kizárólag a járműegység által létrehozott aláírások ellenőrzésére használható.

CSM_78 A VU_MA tanúsítvány érvényességi időszaka 15 év és 3 hónap (lásd: a 9.1.7. szakasz 1. ábráját). A VU_Sign tanúsítvány érvényességi időszaka szintén 15 év és 3 hónap.

Megjegyzések:

— A VU_Sign tanúsítvány kibővített érvényességi időszaka lehetővé teszi a járműegység számára, hogy a lejáratot követően még három hónapig érvényes aláírásokat hozzon létre a letöltött adatokhoz, az 581/2010/EU rendelet előírásainak megfelelően.

— A VU_MA kibővített érvényességi időszakára azért van szükség, hogy a járműegység számára lehetővé tegye az ellenőrzőkártyák vagy vállalkozáskártyák hitelesítését a lejáratot követő első három hónapban, és ezáltal lehetőség legyen az adatletöltésre.

CSM_79 A járműegység a megfelelő tanúsítvány lejártát követően semmilyen célra nem használhatja a járműegység-kulcspár privát kulcsát.

CSM_80 A járműegység-kulcspárok (kivéve az ideiglenes kulcspárokat) és az adott járműegység megfelelő tanúsítványai nem cserélhetők vagy újíthatók meg, miután a járműegységet üzembe állították.

Megjegyzések:

— Az ideiglenes kulcspárokra ez a követelmény nem vonatkozik, mivel a járműegység minden chiphitelesítéskor és munkamenetkulcs-egyeztetéskor új ideiglenes kulcspárt hoz létre (lásd a 10.4. szakaszt). Az ideiglenes kulcspárokhoz nem tartozik tanúsítvány.

— Ez a követelmény nem tiltja a statikus járműegység-kulcspárok esetleges cseréjét a járműegység gyártója által ellenőrzött biztonságos környezetben végzett javítás vagy felújítás során.

CSM_81 Az üzembe állított járműegységek a következő titkosítási kulcsokkal és tanúsítványokkal rendelkeznek:

— A VU_MA privát kulcs és a megfelelő tanúsítvány.

— A VU_Sign privát kulcs és a megfelelő tanúsítvány.

— A VU_MA tanúsítvány és a VU_Sign tanúsítvány ellenőrzésére szolgáló MSCA_VU-EGF.PK nyilvános kulcsot tartalmazó MSCA_VU-EGF tanúsítvány.

▼B

— Az MSCA_VU-EGF tanúsítvány ellenőrzésére szolgáló EUR.PK nyilvános kulcsot tartalmazó EUR-tanúsítvány.

— Az az EUR-tanúsítvány, amelynek érvényességi időszaka közvetlenül megelőzi az MSCA_VU-EGF tanúsítvány ellenőrzésére szolgáló EUR-tanúsítvány (ha van) érvényességi időszakát.

— A fenti két EUR-tanúsítványt összekapcsoló hivatkozási tanúsítvány (ha van).

CSM_82 A CSM_81 szövegében felsorolt titkosítási kulcsokon és tanúsítványokon kívül a járműegységeknek rendelkezniük e függelék A. részében meghatározott kulcsokkal és tanúsítványokkal is rendelkezniük kell, amelyek lehetővé teszik a járműegység számára, hogy kommunikáljanak az első generációs tachográfkártyákkal.

9.1.5 *Berendezési szint: Tachográfkártyák*

CSM_83 Minden tachográfkártyához egy darab egyedi ECC-kulcspárt kell létrehozni, Card_MA megnevezéssel. Emellett egy második, Card_Sign megnevezésű ECC-kulcspárt is létre kell hozni minden egyes járművezetői kártyához és műhelykártyához. Ezt a feladatot a kártyák gyártói vagy a kártyák testreszabását végző felek végzik. Egy kártyakulcspár létrehozásakor a kulcsot létrehozó félnek el kell küldenie a nyilvános kulcsot a székhelye szerinti ország MSCA-ja számára, hogy beszerezze az MSCA által aláírt megfelelő kártyatanúsítványt. A privát kulcsot csak a tachográfkártya használja.

CSM_84 Egy adott járművezetői kártya vagy műhelykártya Card_MA és Card_Sign tanúsítványainak hatálybalépési dátuma megegyezik.

CSM_85 A kártya gyártójának vagy a kártya testreszabását végző félnek úgy kell megválasztania a kártyakulcspár erősségét, hogy az megegyezzen a megfelelő kártyatanúsítvány aláírásához használt MSCA-kulcspár erősségével.

CSM_86 A tachográfkártya a Card_MA kulcspárt – amely a Card_MA.SK privát kulcsból és a Card_MA.PK nyilvános kulcsból áll – kizárólag arra használhatja, hogy kölcsönös hitelesítést és munkamenetkulcs-egyeztetést végezzen a járműegységekkel az e függelék 10.3. és 10.4. szakaszában leírtaknak megfelelően.

CSM_87 A járművezetői kártya vagy műhelykártya a Card_Sign kulcspárhoz tartozó Card_Sign.SK privát kulcsot kizárólag arra használhatja, hogy aláírja a letöltött adatfájlokat az e függelék 14. fejezetében leírtaknak megfelelően. A megfelelő Card_Sign.PK nyilvános kulcs kizárólag a kártya által létrehozott aláírások ellenőrzésére használható.

CSM_88 A Card_MA tanúsítvány érvényességi időszaka a következők szerint alakul:

— Járművezetői kártyák: 5 év

— Vállalkozáskártyák: 2 év

— Ellenőrzőkártyák: 2 év

— Műhelykártyák: 1 év

▼B

CSM_89 A Card_Sign tanúsítvány érvényességi időszaka a következők szerint alakul:

— Járművezetői kártyák: 5 év és 1 hónap

— Műhelykártyák: 1 év és 1 hónap

Megjegyzés: a Card_Sign tanúsítvány kibővített érvényességi időszaka lehetővé teszi a járművezetői kártya számára, hogy a lejáratot követően még egy hónapig érvényes aláírásokat hozzon létre a letöltött adatokhoz. Erre az 581/2010/EU rendelet előírásai miatt van szükség, amely megköveteli, hogy a járművezetői kártyáról még a legutolsó adatrögzítést követő 28 napig lehetséges legyen az adatletöltés.

CSM_90 Egy adott tachográfkártya kulcspárjai és megfelelő tanúsítványai a kártya kibocsátását követően nem lesznek kicserélve vagy megújítva.

CSM_91 A kibocsátott tachográfkártyák a következő titkosítási kulcsokkal és tanúsítványokkal rendelkeznek:

— A Card_MA privát kulcs és a megfelelő tanúsítvány.

— Járművezetői kártyák és műhelykártyák esetében ezenfelül: a Card_Sign privát kulcs és a megfelelő tanúsítvány.

— A Card_MA tanúsítvány és a Card_Sign tanúsítvány ellenőrzésére szolgáló MSCA_Card.PK nyilvános kulcsot tartalmazó MSCA_Card tanúsítvány.

— Az MSCA_Card tanúsítvány ellenőrzésére szolgáló EUR.PK nyilvános kulcsot tartalmazó EUR-tanúsítvány.

— Az az EUR-tanúsítvány, amelynek érvényességi időszaka közvetlenül megelőzi az MSCA_Card tanúsítvány (ha van) ellenőrzésére szolgáló EUR-tanúsítvány érvényességi időszakát.

— A fenti két EUR-tanúsítványt összekapcsoló hivatkozási tanúsítvány (ha van).

CSM_92 A CSM_91 szövegében felsorolt titkosítási kulcsokon és tanúsítványokon kívül a tachográfkártyáknak e függelék A. részében meghatározott kulcsokkal és tanúsítványokkal is rendelkezniük kell, amelyek lehetővé teszik a tachográfkártyák számára, hogy kommunikáljanak az első generációs járműegységekkel.

9.1.6 *Berendezési szint: Külső GNSS-eszközök*

CSM_93 Minden külső GNSS-eszközhöz egy egyedi ECC-kulcspárt hoznak létre, EGF_MA megnevezéssel. Ezt a feladatot a GNSS-eszközök gyártói végzik. Egy EGF_MA kulcspár létrehozásakor a létrehozó félnek el kell küldenie a nyilvános kulcsot a székhelye szerinti ország MSCA-ja számára, hogy beszerezze az MSCA által aláírt megfelelő EGF_MA tanúsítványt. A privát kulcsot csak a GNSS-eszköz használja.

CSM_94 Az EGF gyártójának úgy kell megválasztania az EGF_MA kulcspár erősségét, hogy az megegyezzen a megfelelő EGF_MA tanúsítvány aláírásához használt MSCA-kulcspár erősségével.

▼B

CSM_95 A külső GNSS-eszköz az EGF_MA kulcspárt – amely az EGF_MA.SK privát kulcsból és az EGF_MA.PK nyilvános kulcsból áll – kizárólag arra használhatja, hogy kölcsönös hitelesítést és munkamenetkulcs-egyeztetést végezzen a járműegységekkel az e függelék 11.4. és 11.4. szakaszában leírtaknak megfelelően.

CSM_96 Az EGF_MA tanúsítvány érvényességi időszaka 15 év.

CSM_97 A külső GNSS-eszköz a megfelelő tanúsítvány lejártát követően nem használja az EGF_MA kulcspár privát kulcsát a járműegységekhez való kapcsolódásra.

Megjegyzés: a 11.3.3. szakaszban leírtaknak megfelelően az EGF potenciálisan használhatja a privát kulcsát olyan járműegységgel történő kölcsönös hitelesítésre, amelyhez már kapcsolódott, még a megfelelő tanúsítvány lejártát követően is.

CSM_98 Egy adott külső GNSS-eszköz EGF_MA kulcspárja és megfelelő tanúsítványa nem cserélhető vagy újítható meg, miután az EGF-egységet üzembe állították.

Megjegyzés: ez a követelmény nem tiltja az EGF-kulcspárok esetleges cseréjét az EGF gyártója által ellenőrzött biztonságos környezetben végzett javítás vagy felújítás során.

CSM_99 Az üzembe állított külső GNSS-eszközök a következő titkosítási kulcsokkal és tanúsítványokkal rendelkeznek:

— Az EGF_MA privát kulcs és a megfelelő tanúsítvány.

— Az EGF_MA tanúsítvány ellenőrzésére szolgáló MSCA_VU-EGF.PK nyilvános kulcsot tartalmazó MSCA_VU-EGF tanúsítvány.

— Az MSCA_VU-EGF tanúsítvány ellenőrzésére szolgáló EUR.PK nyilvános kulcsot tartalmazó EUR-tanúsítvány.

— Az az EUR-tanúsítvány, amelynek érvényességi időszaka közvetlenül megelőzi az MSCA_VU-EGF tanúsítvány ellenőrzésére szolgáló EUR-tanúsítvány (ha van) érvényességi időszakát.

— A fenti két EUR-tanúsítványt összekapcsoló hivatkozási tanúsítvány (ha van).

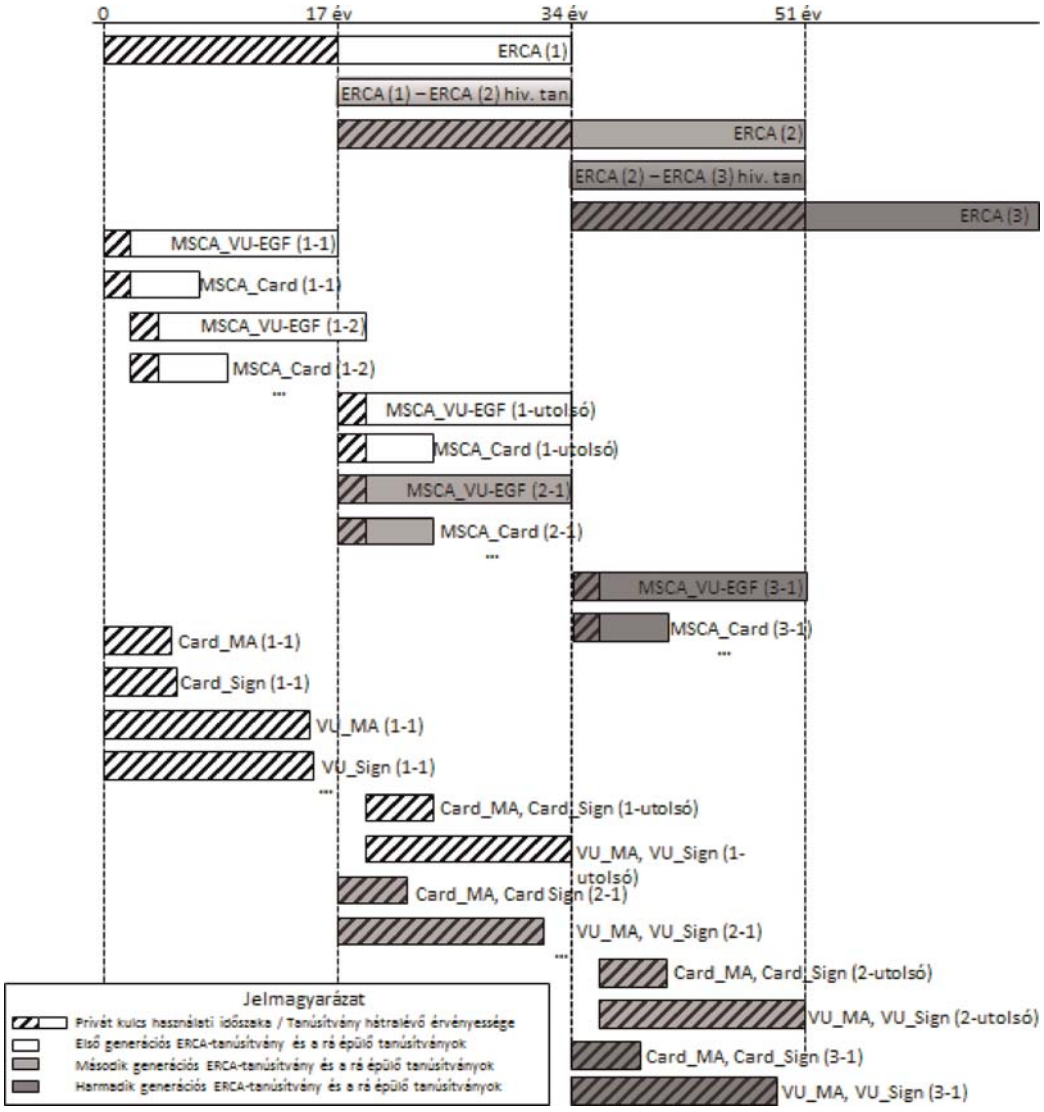
9.1.7 *Áttekintés: Tanúsítványok cseréje*

Az alábbi 1. ábra azt szemlélteti, hogyan történik az ERCA gyökértanúsítványok, az ERCA hivatkozási tanúsítványok, az MSCA tanúsítványok és a berendezéshez (járműegység és kártya) tartozó tanúsítványok különböző generációinak kibocsátása és felhasználása:

▼B

1. ábra

Az ERCA gyökértanúsítványok, az ERCA hivatkozási tanúsítványok, az MSCA-tanúsítványok és a berendezéshez (járműegység és kártya) tartozó tanúsítványok különböző generációinak kibocsátása és felhasználása



Megjegyzések az 1. ábra tartalmához:

1. A gyökértanúsítvány különböző generációit zárójelben lévő szám jelzi. Az „ERCA (1)” például az ERCA gyökértanúsítvány első generációját, az „ERCA (2)” pedig ugyanezen tanúsítvány második generációját jelenti, és így tovább.

2. Más tanúsítványok két zárójeles számmal vannak megjelölve: az első annak a gyökértanúsítványnak a generációját jelzi, amely alatt a kibocsátás történt, a második pedig magának a tanúsítványnak a generációját. Az MSCA_Card (1-1) például az első MSCA_Card tanúsítvány, amelyet az ERCA (1) alatt bocsátottak ki; az MSCA_Card (2-1) az első MSCA_Card tanúsítvány, amelyet az ERCA (2) alatt bocsátottak ki; az MSCA_Card (2-utolsó) az utolsó olyan MSCA_Card tanúsítvány, amelyet az ERCA (2) alatt bocsátottak ki; a Card_MA (2-1) az első kölcsönös hitelesítési kártyatanúsítvány, amelyet az ERCA (2) alatt bocsátottak ki; és így tovább.

▼B

3. Az MSCA_Card (2-1) és az MSCA_Card (1-utolsó) tanúsítvány kibocsátása majdnem (de nem pontosan) egy időben történik. Az MSCA_Card (2-1) az első olyan MSCA_Card tanúsítvány, amelyet az ERCA (2) alatt bocsátanak ki, és a kibocsátására valamivel az MSCA_Card (1-utolsó) – azaz az ERCA (1) alatt kibocsátott utolsó MSCA_Card tanúsítvány – után kerül sor.

4. Ahogy az ábrán is látható, az ERCA (2) alatt kibocsátott első járműegység- és kártyatanúsítványok majdnem két évvel az ERCA (1) alatt kibocsátott utolsó járműegység- és kártyatanúsítványok megjelenését követően jelennek meg. Ennek az az oka, hogy a járműegység- és kártyatanúsítványokat MSCA-tanúsítvány, és nem közvetlenül az ERCA-tanúsítvány részeként bocsátják ki. Az MSCA (2-1) tanúsítvány kibocsátására közvetlenül az ERCA (2) érvényessé válása után kerül sor, de az MSCA (1-utolsó) tanúsítványt nem sokkal ezelőtt bocsátják ki, az ERCA (1) tanúsítvány érvényességének utolsó pillanatában. Ezért ez a két MSCA-tanúsítvány közelítőleg azonos érvényességi időszakkal fog rendelkezni, annak ellenére, hogy két különböző generációhoz tartoznak.

5. A kártyák érvényességi időszakaként a járművezetői kártyák érvényességi időszaka van feltüntetve (5 év).

6. A helytakarékosság érdekében a Card_MA és Card_Sign tanúsítvány, valamint a VU_MA és VU_Sign tanúsítvány érvényességi időszakai közötti eltérés csak az első generációnál van feltüntetve.

9.2. **Szimmetrikus kulcsok**

9.2.1 *A járműegységek és mozgásérzékelők közötti kommunikáció biztonságossá tételét szolgáló kulcsok*

9.2.1.1 *Általános tudnivalók*

Megjegyzés: e rész olvasói feltételezhetően ismerik a járműegység és a mozgásérzékelő közötti interfészt leíró ISO 16844-3. sz. szabvány tartalmát. A járműegység és a mozgásérzékelő párosításának folyamatát e függelék 12. fejezete ismerteti részletesen.

CSM_100 A járműegységek és mozgásérzékelők párosításához, a járműegységek és mozgásérzékelők közötti kölcsönös hitelesítéshez, valamint a járműegységek és mozgásérzékelők közötti kommunikáció titkosításához több szimmetrikus kulcs szükséges (lásd: 3. táblázat). E kulcsok mindegyike a mozgásérzékelő mesterkulcsával azonos hosszúságú AES-kulcs. A mozgásérzékelő mesterkulcsa a (tervezett) európai gyökérkulcspár hosszához lesz kötve (lásd: CSM_50).

3. táblázat

A járműegység és a mozgásérzékelő közötti kommunikáció biztonságossá tételét szolgáló kulcsok

Kulcs	Szimbólum	Létrehozó	Létrehozási módszer	Tároló
Mozgás-érzékelő mesterkulcsa – járműegységhez tartozó rész	$K_{M\text{-}VU}$	ERCA	Véletlenszerű	ERCA, a járműegységek tanúsítványainak kibocsátásában részt vevő MSCA-k, járműegységek gyártói, járműegységek
Mozgás-érzékelő mesterkulcsa – műhelyhez tartozó rész	$K_{M\text{-}WC}$	ERCA	Véletlenszerű	ERCA, MSCA-k, kártyagyártók, műhelykártyák

▼B

Kulcs	Szimbólum	Létrehozó	Létrehozási módszer	Tároló
Mozgás-érzékelő mesterkulcsa	K_M	Nem függetlenül létrehozott	Kiszámítása a $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$ képlettel	ERCA, a mozgásérzékelők kulcsainak kibocsátásában részt vevő MSCA-k (opcionálisan) (*)
Azonosítási kulcs	K_{ID}	Nem függetlenül létrehozott	Kiszámítása a $K_{ID} = K_M$ XOR CV képlettel (a CV meghatározását lásd: CSM_106)	ERCA, a mozgásérzékelők kulcsainak kibocsátásában részt vevő MSCA-k (opcionálisan) (*)
Párosítási kulcs	K_P	Mozgásérzékelő gyártója	Véletlenszerű	Egy mozgásérzékelő
Munkamenet-kulcs	K_S	Járműegység (a járműegység és a mozgásérzékelő párosításakor)	Véletlenszerű	Egy járműegység és egy mozgásérzékelő

(*) A K_M és a K_{ID} tárolása opcionális, mivel ezek a kulcsok származtathatók a $K_{M\text{-}VU}$, a $K_{M\text{-}WC}$ és a CV értékeiből.

CSM_101 Az európai gyökértanúsítványokat kezelő hatóság létrehozza a $K_{M\text{-}VU}$ és $K_{M\text{-}WC}$ kulcsot, ezt a két véletlenszerű és egyedi AES-kulcsot, amelyekből a K_M mozgásérzékelő-mesterkulcs a $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$ képlettel számítható ki. Az ERCA-nak a K_M, $K_{M\text{-}VU}$ és $K_{M\text{-}WC}$ értékeit kérésre közölnie kell a tagállami tanúsító hatóságokkal.

CSM_102 Az ERCA-nak minden K_M mozgásérzékelő-mesterkulcshoz hozzá kell rendelnie egy egyedi verziószámot, amely a $K_{M\text{-}VU}$ és $K_{M\text{-}WC}$ kulcsok, valamint a kapcsolódó K_{ID} azonosítási kulcs létrehozására is vonatkozik. Az ERCA-nak tájékoztatnia kell az MSCA-kat a verziószámról, amikor elküldi számukra a $K_{M\text{-}VU}$ és $K_{M\text{-}WC}$ értékeit.

Megjegyzés: a verziószám arra szolgál, hogy megkülönböztessék a kulcsok különböző generációit (erről részletesen lásd a 9.2.1.2. szakaszt).

CSM_103 A tagállami tanúsító hatóságnak kérésre továbbítania kell a $K_{M\text{-}VU}$ kulcsot és annak verziószámát a járműegység-gyártók számára. A járműegység-gyártóknak a $K_{M\text{-}VU}$ kulcsot és verziószámát minden legyártott járműegységbe integrálniuk kell.

CSM_104 A tagállami tanúsító hatóságnak gondoskodnia kell arról, hogy a $K_{M\text{-}WC}$ és annak verziószáma minden, az adott hatóság felelősségi körében kibocsátott műhelykártyába integrálva legyen.

Megjegyzések:

— Lásd a `SensorInstallationSecData` adattípus leírását a 2. függelékben.

— A 9.2.1.2. szakaszban leírtaknak megfelelően előfordulhat, hogy a $K_{M\text{-}WC}$ több generációját is integrálni kell egy adott műhelykártyába.

▼B

CSM_105 A CSM_104 által meghatározott AES-kulcson felül az MSCA-nak gondoskodnia kell arról, hogy a Km_{WC} TDES-kulcsot (lásd e függelék A. részének CSM_037 követelményét) integrálják a saját felelősségi körében kibocsátott minden műhelykártyába.

Megjegyzések:

— Ez lehetővé teszi, hogy második generációs műhelykártyákat használjanak az első generációs járműegységekhez való kapcsolódáshoz.

— A második generációs műhelykártya két különböző alkalmazást fog tartalmazni: az egyik az e függelék B. részének, a másik pedig az A. részének felel meg. Az utóbbi tartalmazza a Km_{WC} TDES-kulcsot.

CSM_106 A mozgásérzékelők kibocsátásában részt vevő MSCA-nak az azonosítási kulcsot a mozgásérzékelő mesterkulcsából kell származtatnia úgy, hogy XOR-műveletet végez a mesterkulcs és a CV állandóvektor között. A CV értéke a következő:

— 128 bites mozgásérzékelő-mesterkulcsok esetében: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— 192 bites mozgásérzékelő-mesterkulcsok esetében: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

— 256 bites mozgásérzékelő-mesterkulcsok esetében: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Megjegyzés: az állandóvektorok létrehozása a következőképpen zajlott:

Pi_10 = a matematikai π állandó decimális részének első 10 bájtja = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = az SHA-256(Pi_10) első 16 bájtja

CV_192-bits = az SHA-384(Pi_10) első 24 bájtja

CV_256-bits = az SHA-512(Pi_10) első 32 bájtja

CSM_107 A mozgásérzékelő-gyártók minden mozgásérzékelőhöz létrehoznak egy véletlenszerű és egyedi K_P párosítási kulcsot, és az egyes párosítási kulcsokat elküldik egy tagállami tanúsító hatóság számára. Az MSCA az egyes párosítási kulcsokat a K_M mozgásérzékelő-mesterkulccsal titkosítja, és a titkosított kulcsot visszaküldi a mozgásérzékelő gyártója számára. Az MSCA-nak minden titkosított kulcs esetében tájékoztatnia kell a mozgásérzékelő gyártóját a társított K_M verziószámáról.

Megjegyzés: a 9.2.1.2. szakaszban leírtaknak megfelelően előfordulhat, hogy a mozgásérzékelő gyártójának több egyedi párosítási kulcsot is létre kell hoznia egyetlen mozgásérzékelőhöz.

▼B

CSM_108 A mozgásérzékelő-gyártóknak minden mozgásérzékelőhöz létre kell hozniuk egy egyedi sorozatszámot, és az összes sorozatszámot el kell küldeniük a tagállami tanúsító hatóság számára. Az MSCA-nak az egyes sorozatszámokat a K_{ID} azonosítási kulccsal külön-külön titkosítania kell, és a titkosított sorozatszámot vissza kell küldenie a mozgásérzékelő gyártója számára. Az MSCA-nak minden titkosított sorozatszám esetében tájékoztatnia kell a mozgásérzékelő gyártóját a társított K_{ID} verziószámáról.

CSM_109 A CSM_107 és CSM_108 követelményhez az MSCA-nak az AES algoritmust kell alkalmaznia titkosított blokkok láncolatán alapuló üzemmódban, az ISO 10116. sz. szabvány definíciója szerint, m = 1 kihagyási paraméterrel és SV = 00 {16} inicializálási vektorral (azaz 16 bájt, '0' bináris értékkel). Szükség esetén az MSCA-nak az ISO 9797-1. sz. szabvány szerinti 2. kitöltési módszert kell alkalmaznia.

CSM_110 A mozgásérzékelő gyártója a titkosított párosítási kulcsot és a titkosított sorozatszámot a titkosításhoz használt K_M és K_{ID} kulcs megfelelő egyszerű szöveges értékével és verziószámával együtt a mozgásérzékelőben tárolja.

Megjegyzés: a 9.2.1.2. szakaszban leírtaknak megfelelően előfordulhat, hogy a mozgásérzékelő gyártójának több titkosított párosítási kulcsot és sorozatszámot is tárolnia kell egyetlen mozgásérzékelőn.

CSM_111 A CSM_110 által meghatározott AES-alapú titkosítási tartalmon felül a mozgásérzékelő gyártója az egyes mozgásérzékelőkben a TDES-alapú titkosítási tartalmat is tárolhatja, amely e függelék A. részének CSM_037 követelményében van leírva.

Megjegyzés: mindez lehetővé teszi a második generációs mozgásérzékelő első generációs járműegységhez történő kapcsolódását.

CSM_112 A járműegység által a mozgásérzékelővel való párosítás során létrehozott K_S munkamenetkulcs hossza a $K_{M\text{-}VU,}$ hosszához igazodik, a CSM_50 követelményben leírtaknak megfelelően.

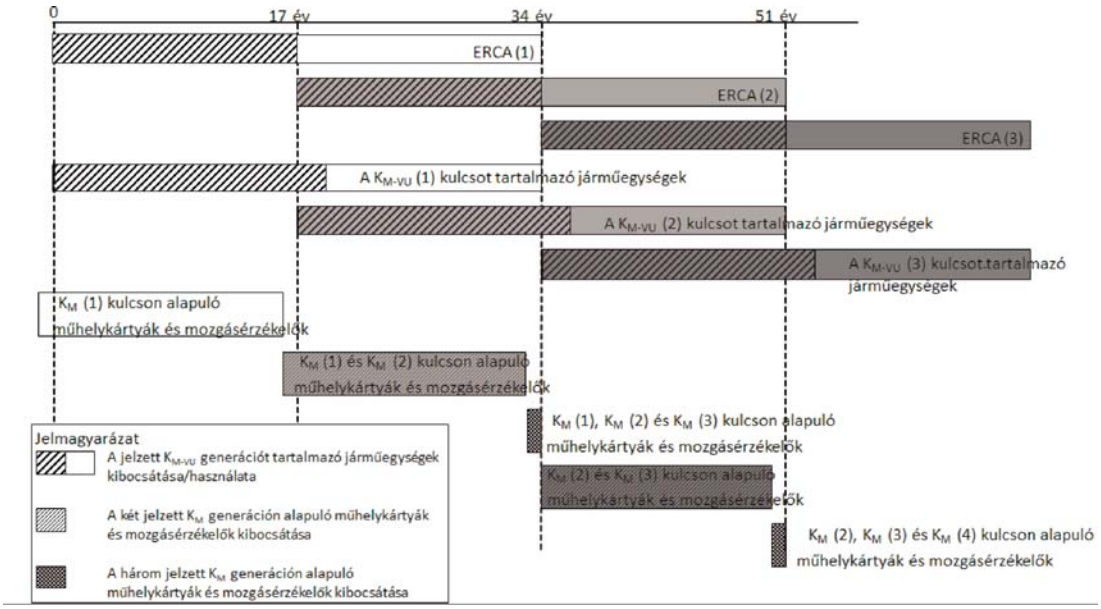
9.2.1.2 *Mozgásérzékelő mesterkulcsának cseréje második generációs készülékekben*

CSM_113 Minden egyes mozgásérzékelő-mesterkulcs és minden kapcsolódó kulcs (lásd: 3. táblázat) az ERCA gyökérkulcspár adott generációjához van társítva. Így ezeket a kulcsokat 17 évente kell cserélni. A mozgásérzékelő-mesterkulcsok minden generációjának érvényességi időszaka egy évvel a társított ERCA gyökérkulcspár érvényessé válása előtt kezdődik, és a társított ERCA gyökérkulcspár lejáratakor ér véget. A 2. ábra ezt ábrázolja.

▼B

2. ábra

A mozgásérzékelő-mesterkulcs különböző generációinak kibocsátása és használata a járműegységekben, mozgásérzékelőkben és műhelykártyákban



CSM_114 Legalább egy évvel az új európai gyökérkulcspár létrehozása előtt (lásd: CSM_56) az ERCA-nak a K_{M-VU} és a K_{M-WC} létrehozásával el kell készítenie az új K_M mozgásérzékelő-mesterkulcsot. A mozgásérzékelő-mesterkulcs hosszának az új európai gyökérkulcspár tervezett erősségéhez kell igazodnia (lásd: CSM_50). Az ERCA-nak az új K_M, K_{M-VU} és K_{M-WC} kulcsot és verziószámukat kérésre közölnie kell az MSCA-kkal.

CSM_115 Az MSCA-nak gondoskodnia kell arról, hogy a K_{M-WC} minden érvényes generációja és ezek verziószáma a saját felelősségi körében kibocsátott összes műhelykártyán tárolva legyen (lásd: 2. ábra).

Megjegyzés: ez azt is jelenti, hogy az ERCA-tanúsítványok érvényességi időszakának utolsó évében a műhelykártyákat a K_{M-WC} három különböző generációjával bocsátják ki (lásd: 2. ábra).

CSM_116 A fenti CSM_107 és CSM_108 követelményben leírt folyamattal kapcsolatos tudnivalók: az MSCA a mozgásérzékelő gyártójától kapott egyes K_P párosítási kulcsokat külön-külön titkosítja a K_M mozgásérzékelő-mesterkulcs minden egyes érvényes generációjával. Az MSCA emellett a mozgásérzékelő gyártójától kapott egyes sorozatszámokat is külön-külön titkosítja a K_{ID} azonosítási kulcs minden egyes érvényes generációjával. A mozgásérzékelő gyártója a párosítási kulcs és a sorozatszám minden titkosítását az adott mozgásérzékelőben tárolja, a titkosításhoz használt K_M és K_{ID} kulcs megfelelő egyszerű szöveges értékeivel és verziószámaival együtt.

▼B

Megjegyzés: ez azt is jelenti, hogy egy ERCA-tanúsítvány érvényességi időszakának utolsó évében a mozgásérzékelőket a K_M három különböző generációján alapuló titkosított adatokkal bocsátják ki (lásd: 2. ábra).

CSM_117 A fenti CSM_107 követelményekben leírt folyamattal kapcsolatos tudnivalók: mivel a K_P párosítási kulcs hossza a K_M hosszához igazodik (lásd: CSM_100), előfordulhat, hogy a mozgásérzékelő gyártójának akár három különböző (eltérő hosszúságú) párosítási kulcsot is létre kell hoznia egyetlen mozgásérzékelőhöz, amennyiben a K_M egymást követő generációinak hossza nem azonos. Ilyen esetben a gyártó minden egyes párosítási kulcsot elküld az MSCA számára. Az MSCA gondoskodik arról, hogy az egyes párosítási kulcsok a mozgásérzékelő-mesterkulcs megfelelő (vagyis a velük azonos hosszúságú) generációjával legyenek titkosítva.

Megjegyzés: ha a mozgásérzékelő gyártója TDES-alapú párosítási kulcsot használ egy második generációs mozgásérzékelőhöz (lásd: CSM_111), akkor a gyártó tájékoztatja az MSCA-t, hogy a TDES-alapú mozgásérzékelő-mesterkulcsot kell alkalmazni a párosítási kulcs titkosításához. Ez azért fontos, mert a TDES-kulcs hossza megegyezhet az AES-kulcs hosszával, így az MSCA pusztán a kulcshossz alapján nem képes dönteni.

CSM_118 A járműegységek gyártói csak egy generációjú $K_{M\text{-}VU}$ kulcsot integrálhatnak minden egyes járműegységbe, a kulcs verziószámával együtt. Ennek a $K_{M\text{-}VU}$-generációnak ahhoz az ERCA-tanúsítványhoz kell kapcsolódnia, amelyen a járműegység tanúsítványai alapulnak.

Megjegyzések:

— az *X*. generációs ERCA-tanúsítványon alapuló járműegységek csak az *X*. generációs $K_{M\text{-}VU}$ kulcsot tartalmazhatják, még akkor is, ha azt az *X+1*. generációs ERCA-tanúsítvány érvényességi időszakának kezdete után bocsátották ki. Ezt a 2. ábra szemlélteti.

— A *X*. generációhoz tartozó járműegységek nem párosíthatók össze *X-1*. generációs mozgásérzékelőkkel.

— Mivel a műhelykártyák érvényességi időszaka egy év, a CSM_113–CSM_118 eredményeképpen minden műhelykártya tartalmazni fogja az új $K_{M\text{-}WC}$ kulcsot az új $K_{M\text{-}VU}$ kulcsot tartalmazó első járműegység kibocsátásakor. Emellett ekkorra a legtöbb új mozgásérzékelő már tartalmazni fogja az új K_M kulcson alapuló titkosított adatokat is. Emellett ekkorra a legtöbb új mozgásérzékelő már tartalmazni fogja az új K_M kulcson alapuló titkosított adatokat is.

9.2.2 *Kulcsok a DSRC-kommunikáció biztonságossá tételéhez*

9.2.2.1 *Általános tudnivalók*

CSM_119 A járműegységek és az ellenőrző hatóságok közötti, DSRC távoli kommunikációs csatornán zajló adatforgalom hitelességét és titkosságát olyan járműegység-specifikus AES-kulcsokkal kell biztosítani, amelyeket egyetlen DSRC-mesterkulcsból, a KM_{DSRC} kulcsból származtatnak.

▼B

CSM_120 A KM_{DSRC} DSRC-mesterkulcs egy, az ERCA által biztonságosan létrehozott, tárolt és terjesztett AES-kulcs. Hossza 128, 192 vagy 256 bit lehet, az európai gyökérkulcspár hosszának megfelelően (lásd: CSM_50).

CSM_121 Az ERCA-nak kérésre biztonságos módon el kell juttatnia a DSRC-mesterkulcsot a tagállamok tanúsító hatóságai számára, hogy azok származtathassák belőle a járműegység-specifikus DSRC-kulcsokat, valamint biztosíthassák, hogy a DSRC-mesterkulcs integrálva legyen minden, a saját felelősségi körükben kibocsátott ellenőrzőkártyába és műhelykártyába.

CSM_122 Az ERCA-nak minden egyes DSRC-mesterkulcshoz egyedi verziószámot kell rendelnie. Az ERCA-nak tájékoztatnia kell az MSCA-kat a verziószámról, amikor elküldi számukra a DSRC-mesterkulcsot.

Megjegyzés: A verziószám arra szolgál, hogy megkülönböztessék a DSRC-mesterkulcs különböző generációit (erről részletesen lásd a 9.2.2.2. szakaszt).

CSM_123 A járműegység gyártójának minden járműegységhez létre kell hoznia egy egyedi járműegység-sorozatszámot, majd ezt a számot el kell küldenie a tagállami tanúsító hatóság számára, hogy beszerezze a két járműegység-specifikus DSRC-kulcsot. A járműegység sorozatszáma `VuSerialNumber` adattípusú, a kódoláshoz pedig az ISO 8825-1. sz. szabvány szerinti megkülönböztetett kódolási szabályokat (DER) kell használni.

CSM_124 A járműegység-specifikus DSRC-kulcsokra vonatkozó kérés beérkezésekor az MSCA-nak két AES-kulcsot kell származtatnia a járműegységhez: a K_VU_{DSRC}_ENC és a K_VU_{DSRC}_MAC kulcsot. Ezek a járműegység-specifikus kulcsoknak a DSRC-mesterkulccsal megegyező hosszúságúnak kell lenniük. Az MSCA-nak az [RFC 5869] szerinti kulcsszármaztatási funkciót kell alkalmaznia. A HMAC-Hash funkció példányosításához szükséges hasító funkció a DSRC-mesterkulcs hosszához igazodik (lásd: CSM_50). Az [RFC 5869] szerinti kulcsszármaztatási funkciót a következőképpen kell használni:

1. lépés (kiemelés):

— *PRK* = HMAC-Hash (*salt, IKM*), ahol a *salt* üres ‘’ karakterlánc, az *IKM* pedig a KM_{DSRC} értéke.

2. lépés (kibontás):

— *OKM* = *T(1)*, ahol

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || 01) és

▼B

— *T(0)* = üres karakterlánc (‘ ’)

— *info* = a járműegység sorozatszáma a CSM_123 szerint

— K_VU_{DSRC}_ENC = az első *L* oktett az *OKM* értékéből

K_VU_{DSRC}_MAC = az utolsó *L* oktett az *OKM* értékéből

ahol *L* a K_VU_{DSRC}_ENC és a K_VU_{DSRC}_MAC szükséges hossza oktettekben (nyolcbites egységekben) megadva.

CSM_125 Az MSCA-nak a K_VU_{DSRC}_ENC és K_VU_{DSRC}_MAC kulcsot biztonságos módon el kell juttatnia a járműegység gyártója számára a kérdéses járműegységbe történő integrálás céljából.

CSM_126 Kibocsátáskor a járműegységnek a biztonságos memóriájában kell tárolnia a K_VU_{DSRC}_ENC és K_VU_{DSRC}_MAC kulcsot, hogy biztosíthassa a távoli kommunikációs csatornán küldött adatok integritását, hitelességét és titkosságát. A járműegységnek emellett a járműegység-specifikus kulcsok származtatásához használt DSRC-mesterkulcsverzió számát is tárolnia kell.

CSM_127 Kibocsátáskor az ellenőrzőkártyáknak és a műhelykártyáknak a biztonságos memóriájukban kell tárolniuk a KM_{DSRC} kulcsot, hogy ellenőrizhessék a járműegység által a távoli kommunikációs csatornán keresztül küldött adatok integritását és hitelességét, valamint képesek legyenek ezen adatok visszafejtésére. Az ellenőrzőkártyáknak és a műhelykártyáknak emellett a DSRC-mesterkulcs verziószámát is tárolniuk kell.

Megjegyzés: a 9.2.2.2. szakaszban leírtaknak megfelelően előfordulhat, hogy a KM_{DSRC} több generációját is integrálni kell egy adott műhelykártyába vagy ellenőrzőkártyába.

CSM_128 Az MSCA-nak nyilvántartást kell vezetnie minden általa létrehozott járműegység-specifikus DSRC-kulcsról, azok verziószámáról, valamint azoknak a járműegységeknek az azonosítóiról, amelyekhez az egyes kulcskészletek tartoznak.

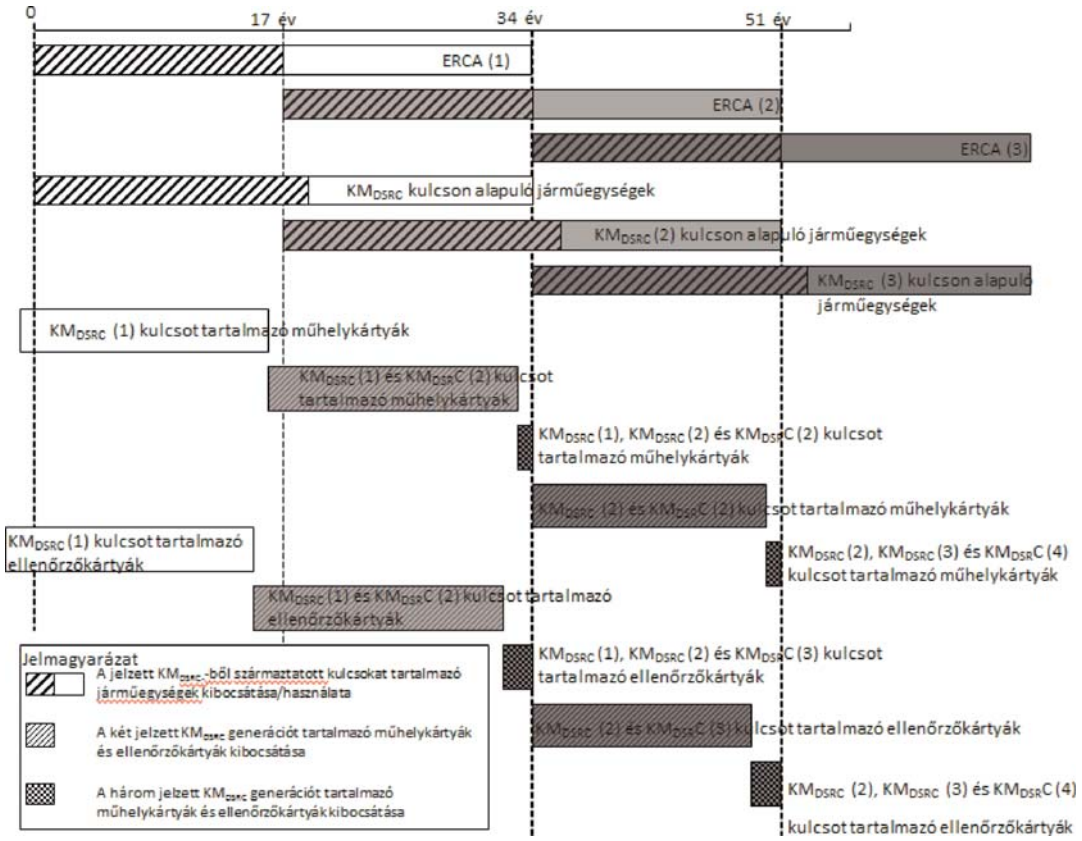
9.2.2.2 *A DSRC-mesterkulcs cseréje*

CSM_129 Minden egyes DSRC-mesterkulcs az ERCA gyökérkulcspár adott generációjához van társítva. Az ERCA-nak ezért 17 évente kell cserélnie a DSRC-mesterkulcsot. Az egyes DSRC-mesterkulcsok minden generációjának érvényességi időszaka két évvel a társított ERCA gyökérkulcspár érvényessé válása előtt kezdődik, és a társított ERCA gyökérkulcspár lejáratakor ér véget. A 3. ábra ezt ábrázolja.

▼B

3. ábra

A DSRC-mesterkulcs különböző generációinak kibocsátása és használata a járműegységekben, műhelykártyákban és ellenőrzőkártyákban



CSM_130 Legalább két évvel az új európai gyökérkulcspár létrehozása előtt (lásd: CSM_56) az ERCA új DSRC-mesterkulcsot hoz létre. A DSRC-mesterkulcs hossza az új európai gyökérkulcspár tervezett hosszához igazodik (lásd: CSM_50). Az ERCA-nak az új DSRC-mesterkulcsot és verziószámát kérésre közölnie kell az MSCA-kkal.

CSM_131 Az MSCA-nak gondoskodnia kell arról, hogy a KM_{DSRC} minden érvényes generációja és ezek verziószáma a saját felelősségi körében kibocsátott összes ellenőrzőkártyán tárolva legyen (lásd: 3. ábra).

Megjegyzés: ez azt is jelenti, hogy az ERCA-tanúsítványok érvényességi időszakának utolsó két évében az ellenőrzőkártyákat a KM_{DSRC} három különböző generációjával bocsátják ki (lásd: 3. ábra).

CSM_132 Az MSCA-nak gondoskodnia kell arról, hogy a KM_{DSRC} összes, legalább egy éve érvényes és még mindig érvényben lévő generációja, valamint ezek verziószáma a saját felelősségi körében kibocsátott összes műhelykártyán tárolva legyen (lásd: 3. ábra).

▼B

Megjegyzés: ez azt is jelenti, hogy az ERCA-tanúsítványok érvényességi időszakának utolsó évében a műhelykártyákat a KM_{DSRC} három különböző generációjával bocsátják ki (lásd: 3. ábra).

CSM_133 A járműegységek gyártói csak egy járműegység-specifikus DSRC-kulcskészletet integrálhatnak minden egyes járműegységbe, annak verziószámával együtt. Ezt a kulcskészletet a KM_{DSRC} azon generációjából kell származtatni, amely a járműegység tanúsítványainak alapjául szolgáló ERCA-tanúsítványhoz van kapcsolva.

Megjegyzések:

— ez azt jelenti, hogy az *X*. generációs ERCA-tanúsítványon alapuló járműegységek csak az *X*. generációs K_VU_{DSRC}_ENC és K_VU_{DSRC}_MAC kulcsot tartalmazhatják, még akkor is, ha a járműegységet az *X+1*. generációs ERCA-tanúsítvány érvényességének kezdete után bocsátották ki. Ezt a 3. ábra szemlélteti.

— Mivel a műhelykártyák érvényességi időszaka egy év, az ellenőrzőkártyáké pedig két év, a CSM_131–CSM_133 eredményeképpen minden műhelykártya és ellenőrzőkártya az új DSRC-mesterkulcsot fogja tartalmazni attól a pillanattól kezdve, hogy kibocsátják az első olyan járműegységet, amely a kérdéses mesterkulcsra épülő járműegység-specifikus kulcsokat tartalmazza.

9.3. **Tanúsítványok**

9.3.1 *Általános tudnivalók*

CSM_134 Az európai intelligens menetírókészülék-rendszer minden tanúsítványának önleíró (self-descriptive) és kártyával ellenőrizhető (card-verifiable – CV) tanúsítványnak kell lennie, az ISO 7816-4. sz. és ISO 7816-8. sz. szabvány előírásainak megfelelően.

CSM_135 A tanúsítványokon belül mind az ASN.1 adatstruktúrák, mind az (alkalmazásspecifikus) adatobjektumok kódolására az ISO 8825-1. sz. szabvány szerinti megkülönböztetett kódolási szabályok (DER) vonatkoznak.

Megjegyzés: ez a kódolás a következő címke-hossz-érték (TLV) struktúrát eredményezi:

Címke: a címke egy vagy két oktettben (nyolcbites egységben) van kódolva, és a tartalmat jelöli.

Hossz: a hossz kódolása előjel nélküli egész számként történik egy, két vagy három oktettben, így a maximális hossz 65 535 oktett. A minimális számú oktettet kell alkalmazni.

Érték: az érték kódolása nulla vagy több oktettben történik.

9.3.2 *A tanúsítvány tartalma*

CSM_136 Minden tanúsítványnak a 4. táblázat szerinti tanúsítványprofilnak megfelelő struktúrával kell rendelkeznie.

4. táblázat

Tanúsítványprofil, 1. verzió

Mező	Mezőazonosító	Címke	Hossz (bájt)	ASN.1 adattípus (lásd az 1. függeléket)
ECC-tanúsítvány	C	7F 21	változó	
ECC-tanúsító szerv	B	7F 4E	változó	

▼B

Mező	Mezőazonosító	Címke	Hossz (bájt)	ASN.1 adattípus (lásd az 1. függeléket)
Tanúsítványprofil-azonosító	CPI	5F 29	01	`INTEGER(0..255)`
A tanúsító hatóság hivatkozása	CAR	42	08	`KeyIdentifier`
A tanúsítvány tulajdonosának engedélye	CHA	5F 4C	07	`CertificateHolder Authorisation`
Nyilvános kulcs	PK	7F 49	változó	
Tartományparaméterek	DP	06	változó	`OBJECT IDENTIFIER`
Nyilvános pont	PP	86	változó	`OCTET STRING`
A tanúsítvány tulajdonosának hivatkozása	CHR	5F 20	08	`KeyIdentifier`
A tanúsítvány hatálybalépési dátuma	CEfD	5F 25	04	`TimeReal`
A tanúsítvány lejárati dátuma	CExD	5F 24	04	`TimeReal`
Az ECC-tanúsítvány aláírása	S	5F 37	változó	`OCTET STRING`

Megjegyzés: A mezőazonosítót e függelék későbbi részeiben a tanúsítványok egyes mezőinek jelölésére használjuk – az X.CAR például az X felhasználó tanúsítványában szereplő tanúsítóhatóság-hivatkozás.

9.3.2.1 Tanúsítványprofil-azonosító

CSM_137 A tanúsítványoknak a tanúsítványprofil-azonosítóval kell jelezniük az alkalmazott tanúsítványprofilt. Az 1. verzió (lásd: 4. táblázat) azonosítója a ‘00’ érték.

9.3.2.2 A tanúsító hatóság hivatkozása

CSM_138 A tanúsító hatóság hivatkozása a tanúsítvány aláírásának ellenőrzésére használt nyilvános kulcsot azonosítja. A tanúsító hatóság hivatkozása így megegyezik a tanúsítvány tulajdonosának hivatkozásával a megfelelő tanúsító hatóság tanúsítványában.

CSM_139 Az ERCA gyökértanúsítványok önaláírtak, vagyis a tanúsítványban megegyezik a tanúsító hatóság hivatkozása és a tanúsítvány tulajdonosának hivatkozása.

▼B

CSM_140 ERCA hivatkozási tanúsítványok esetében a tanúsítvány tulajdonosának hivatkozása megegyezik az új ERCA gyökértanúsítvány CHR-értékével. A hivatkozási tanúsítványokban szereplő tanúsítóhatóság-hivatkozás megegyezik az előző ERCA gyökértanúsítvány tanúsítványtulajdonos-hivatkozásával.

9.3.2.3 A tanúsítvány tulajdonosának engedélye

CSM_141 A tanúsítvány tulajdonosának engedélye arra szolgál, hogy azonosítsa a tanúsítvány típusát. Értéke a tachográfalkalmazás-azonosító hat legjelentősebb bájtjából áll, amelyhez hozzá van fűzve az a készüléktípus, amelyhez a tanúsítványt szánták.

9.3.2.4 Nyilvános kulcs

A nyilvános kulcs két adatelemet tartalmaz: a tanúsítványban a nyilvános kulccsal használandó szabványosított tartományparamétereket, valamint a nyilvános pont értékét.

CSM_142 A tartományparamétereket leíró adatelemnek egy vagy több objektumazonosítót (lásd: 1. táblázat) kell tartalmaznia a szabványosított tartományparaméterek adott készletének megadásához.

CSM_143 A nyilvános pontot leíró adatelemnek a nyilvános pontot kell tartalmaznia. Az elliptikus görbék nyilvános pontjait oktett-karakterlánccá kell konvertálni a [TR-03111] előírásainak megfelelően. Ehhez a tömörítetlen kódolási formátumot kell alkalmazni. Egy elliptikus görbe nyilvános pontjának kódolt formátumból való kinyerésekor mindig el kell végezni a [TR-03111] szerinti ellenőrzéseket.

9.3.2.5 A tanúsítvány tulajdonosának hivatkozása

CSM_144 A tanúsítvány tulajdonosának hivatkozása a tanúsítványban megadott nyilvános kulcs azonosítója. Más tanúsítványokban az adott nyilvános kulcsra való hivatkozásra szolgál.

CSM_145 A kártyák és a külső GNSS-eszközök tanúsítványai esetében a tanúsítvány tulajdonosának hivatkozása az 1. függelékben meghatározott `ExtendedSerialNumber` adattípusú.

CSM_146 Járműegységek esetében két eset lehetséges: a gyártó a tanúsítvány igénylésekor vagy ismeri, vagy nem ismeri a gyártóspecifikus sorozatszámot ahhoz a járműegységhez, amelyhez a tanúsítványt és a társított privát kulcsot szánja. Az első esetben a tanúsítvány tulajdonosának hivatkozása az 1. függelékben meghatározott `ExtendedSerialNumber` adattípusú. A második esetben a tanúsítvány tulajdonosának hivatkozása az 1. függelékben meghatározott `CertificateRequestID` adattípusú.

CSM_147 Az ERCA- és MSCA-tanúsítványok esetében a tanúsítvány tulajdonosának hivatkozása az 1. függelékben meghatározott `CertificationAuthorityKID` adattípusú.

▼B

9.3.2.6 A tanúsítvány hatálybalépési dátuma

CSM_148 A tanúsítvány hatálybalépési dátuma a tanúsítvány érvényességi időszakának kezdő dátumát és időpontját jelöli. A tanúsítvány hatálybalépési dátuma a tanúsítvány elkészítésének dátuma.

9.3.2.7 A tanúsítvány lejárati dátuma

CSM_149 A tanúsítvány lejárati dátuma a tanúsítvány érvényességének záró dátumát és időpontját jelzi.

9.3.2.8 A tanúsítvány aláírása

CSM_150 A tanúsítvány aláírását – a tanúsítványtörzs címkéjét és hosszát is figyelembe véve – a kódolt tanúsítványtörzs alapján kell létrehozni. Az aláíráshoz ECDSA algoritmust kell alkalmazni (meghatározás: [DSS]) az aláíró hatóság kulcsméretéhez kötött hasító algoritmussal (lásd: CSM_50). Az aláírás egyszerű formátumú (lásd: [TR-03111]).

9.3.3 *Tanúsítványok igénylése*

CSM_151 Tanúsítvány igénylésekor az igénylőnek a következő adatokat kell elküldenie a tanúsító hatóság számára:

— A kért tanúsítvány profilazonosítója.

— A tanúsítvány aláírásához várhatóan alkalmazott tanúsítóhatóság-hivatkozás.

— Az aláírandó nyilvános kulcs.

CSM_152 A CSM_151 szövegében szereplő adatokon kívül az MSCA-nak a következő adatokat kell elküldenie a tanúsítási kérelemben az ERCA részére, lehetővé téve az ERCA számára, hogy létrehozza az új MSCA-tanúsítvány tanúsítványtulajdonos-hivatkozását:

— A tanúsító hatóság numerikus nemzeti kódja (adattípus: az 1. függelékben definiált `NationNumeric`).

— A tanúsító hatóság alfanumerikus nemzeti kódja (adattípus: az 1. függelékben definiált `NationAlpha`).

— Az 1 bájtos sorozatszám a tanúsító hatóság különböző kulcsainak megkülönböztetésére, amennyiben bizonyos kulcsokat megváltoztatnak.

— A tanúsító hatóságra vonatkozó további adatokat tartalmazó kétbájtos mező.

CSM_153 A CSM_151 szövegében szereplő adatokon kívül a készülékgyártónak a következő adatokat kell elküldenie a tanúsítási kérelemben az MSCA részére, lehetővé téve az MSCA számára, hogy létrehozza az új készüléktanúsítvány tanúsítványtulajdonos-hivatkozását:

— A készüléktípus gyártóspecifikus azonosítója.

— Ha ismert (lásd: CSM_154), a készülék sorozatszáma, amely egyedi módon azonosítja a gyártót, a készüléktípust és a gyártási hónapot. Ellenkező esetben a tanúsítási kérelem egyedi azonosítója.

▼B

— A készülékgyártás vagy a tanúsítási kérelem hónapja és éve.

A gyártónak gondoskodnia kell az adatok helyességéről, valamint arról, hogy az MSCA által visszaküldött tanúsítványt integrálják a megfelelő készülékbe.

CSM_154 Járműegységek esetében két eset lehetséges: a gyártó a tanúsítvány igénylésekor vagy ismeri, vagy nem ismeri a gyártóspecifikus sorozatszámot ahhoz a járműegységhez, amelyhez a tanúsítványt és a társított privát kulcsot szánja. Ha ismeri, a járműegység gyártójának el kell küldenie a sorozatszámot az MSCA számára. Ha nem ismeri, a gyártónak egyedi módon azonosítania kell az egyes tanúsítási kérelmeket, és a tanúsítási kérelem sorozatszámát kell elküldenie az MSCA számára. Az ennek alapján elkészült tanúsítvány tartalmazza a tanúsítási kérelem sorozatszámát. Miután a tanúsítványt integrálták az adott járműegységbe, a gyártónak tájékoztatnia kell az MSCA-t a tanúsítási kérelem sorozatszáma és a járműegység-azonosító közötti kapcsolatról.

10. JÁRMŰEGYSÉG ÉS KÁRTYA KÖZÖTTI KÖLCSÖNÖS HITELESÍTÉS ÉS BIZTONSÁGOS ÜZENETKÜLDÉS

10.1. **Általános tudnivalók**

CSM_155 A járműegység és a tachográfkártya közötti biztonságos kommunikáció általános szinten a következő lépésekből áll:

— Elsőként mindkét félnek igazolnia kell a másik számára, hogy érvényes nyilvánoskulcs-tanúsítvánnyal rendelkezik, amelyet egy tagállami tanúsító hatóság írt alá, az MSCA nyilvánoskulcs-tanúsítványának pedig az európai gyökértanúsítványokat tanúsító hatóság aláírásával kell rendelkeznie. Ez a lépés az úgynevezett kulcsláncolat-ellenőrzés, amelyről a 10.2. szakaszban található részletes leírás.

— A második lépésben a járműegységnek igazolnia kell a kártya felé, hogy rendelkezik a bemutatott tanúsítvány nyilvános kulcsának megfelelő privát kulccsal. Ezt úgy végzi el, hogy aláírja a kártya által küldött véletlenszerű számot. A kártya ellenőrzi az aláírást a véletlenszerű szám alapján. Ha az ellenőrzés sikeres, megtörténik a járműegység hitelesítése. Ez a lépés a járműegység-hitelesítés, amelyről a 10.3. szakaszban található részletes leírás.

— Harmadik lépésként mindkét fél egymástól függetlenül kiszámít két AES-munkamenetkulcsot egy aszimmetrikus kulcsegyeztetési algoritmus segítségével. Az egyik munkamenetkulcs felhasználásával a kártya létrehoz egy üzenethitelesítési kódot (MAC) a járműegység által küldött egyes adatok alapján. A járműegység ellenőrzi az üzenethitelesítési kódot. Ha az ellenőrzés sikeres, megtörténik a kártya hitelesítése. Ez a lépés a kártyahitelesítés, amelyről a 10.4. szakaszban található részletes leírás.

— A negyedik lépésben a járműegységnek és a kártyának az egyeztetett munkamenetkulcs használatával kell biztosítania a kicserélt üzenetek titkosságát, integritását és hitelességét. Ezt hívják biztonságos üzenetküldésnek, amelyről a 10.5. szakaszban található részletes leírás.

CSM_156 A CSM_155-ben leírt mechanizmust a járműegységnek akkor kell aktiválnia, amikor az egyik kártyaolvasójába kártyát helyeznek be.

▼B

10.2. **Kölcsönös tanúsítványláncolat-ellenőrzés**

10.2.1 *A kártyatanúsítvány-láncolat járműegység által végzett ellenőrzése*

CSM_157 A járműegységeknek a 4. ábra szerinti protokollt kell használniuk a tachográfkártya tanúsítványláncolatának ellenőrzésére.

Megjegyzések a 4. ábra tartalmához:

— Az ábrán látható kártyatanúsítványok és nyilvános kulcsok azok, amelyeket a kölcsönös hitelesítéshez használnak. A 9.1.5. szakaszban ezek Card_MA néven szerepelnek.

— Az ábrán szereplő Card.CA tanúsítványok és nyilvános kulcsok azok, amelyeket a kártyatanúsítványokhoz használnak, amit a kártyatanúsítvány CAR-eleme jelöl. A 9.1.3. szakaszban ezek MSCA_Card néven szerepelnek.

— Az ábrán szereplő Card.CA.EUR tanúsítvány az az európai gyökértanúsítvány, amely a Card.CA tanúsítvány CAR-elemében van feltüntetve.

— Az ábrán szereplő Card.Link tanúsítvány a kártya hivatkozási tanúsítványa, ha van ilyen. A 9.1.2. szakaszban foglaltaknak megfelelően ez az ERCA által létrehozott és az előző európai privát kulccsal aláírt új európai gyökérkulcspár hivatkozási tanúsítványa.

— A Card.Link.EUR tanúsítvány az az európai gyökértanúsítvány, amely a Card.Link tanúsítvány CAR-elemében van feltüntetve.

CSM_158 Ahogy a 4. ábra szemlélteti, a kártya tanúsítványláncolatának ellenőrzése a kártya behelyezésekor kezdődik meg. A járműegységnek be kell olvasnia a kártyatulajdonos hivatkozását (`cardExtendedSerialNumber`) az EF ICC-ről. A járműegységnek ellenőriznie kell, hogy ismeri-e a kártyát, azaz hogy a múltban sikeresen ellenőrizte-e a kártya tanúsítványláncolatát és tárolta-e jövőbeli használatra. Ha igen, és a kártya tanúsítványa még érvényes, akkor a folyamat a járműegység tanúsítványláncolatának ellenőrzésével folytatódik. Ellenkező esetben a járműegységnek egymás után be kell olvasnia a kártyáról a kártyatanúsítvány ellenőrzésére szolgáló MSCA_Card tanúsítványt, az MSCA_Card tanúsítvány ellenőrzésére szolgáló Card.CA.EUR tanúsítványt, valamint adott esetben a hivatkozási tanúsítványt, amíg nem talál olyan tanúsítványt, amelyet ismer vagy ellenőrizni tud. Ha ilyen tanúsítványt talál, a járműegységnek ezzel kell ellenőriznie a kártyáról beolvasott kártyatanúsítványokat. Ha az ellenőrzés sikeres, a folyamat a járműegység tanúsítványláncolatának ellenőrzésével folytatódik. Ellenkező esetben a járműegységnek figyelmen kívül kell hagynia a kártyát.

▼B

Megjegyzés: a járműegység három különböző módon ismerheti a Card.CA.EUR tanúsítványt:

— A Card.CA.EUR tanúsítvány megegyezik a járműegység saját EUR-tanúsítványával.

— A Card.CA.EUR tanúsítvány a járműegység saját EUR-tanúsítványának az előzménye, és a járműegység már a kibocsátásakor tartalmazta ezt a tanúsítványt (lásd: CSM_81).

— A Card.CA.EUR tanúsítvány a járműegység saját EUR-tanúsítványának az utódja, és a járműegység a múltban hivatkozási tanúsítványt kapott egy másik tachográfkártyáról, majd az ellenőrzést követően tárolta jövőbeli felhasználás céljából.

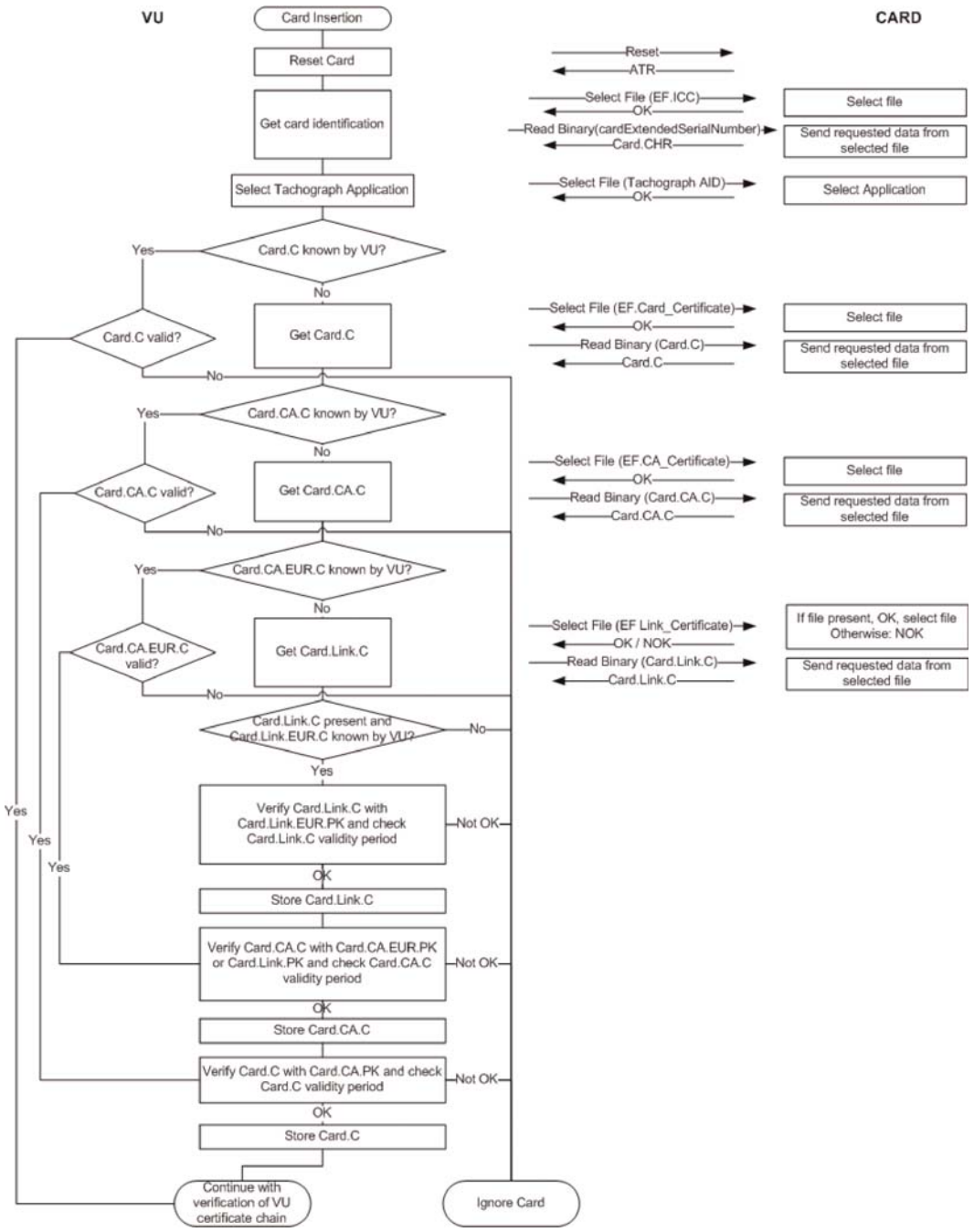
CSM_159 Ahogy a 4. ábra mutatja, miután a járműegység ellenőrizte egy korábban ismeretlen tanúsítvány hitelességét és érvényességét, tárolhatja a tanúsítványt jövőbeli felhasználás céljából, hogy a későbbiekben ne legyen szükség a tanúsítvány hitelességének ismételt ellenőrzésére. A teljes tanúsítvány tárolása helyett előfordulhat, hogy a járműegység csak a tanúsítványtörzs tartalmát tárolja (lásd a 9.3.2. szakaszt).

CSM_160 A járműegységnek ellenőriznie kell a kártyáról beolvasott vagy a memóriájában tárolt tanúsítványok időbeli érvényességét, és a lejárt tanúsítványokat el kell utasítania. A kártya által bemutatott tanúsítvány időbeli érvényességének ellenőrzéséhez a járműegységnek a saját belső óráját kell használnia.

▼B

4. ábra

A kártyatanúsítvány-láncolat járműegység általi ellenőrzésének protokollja



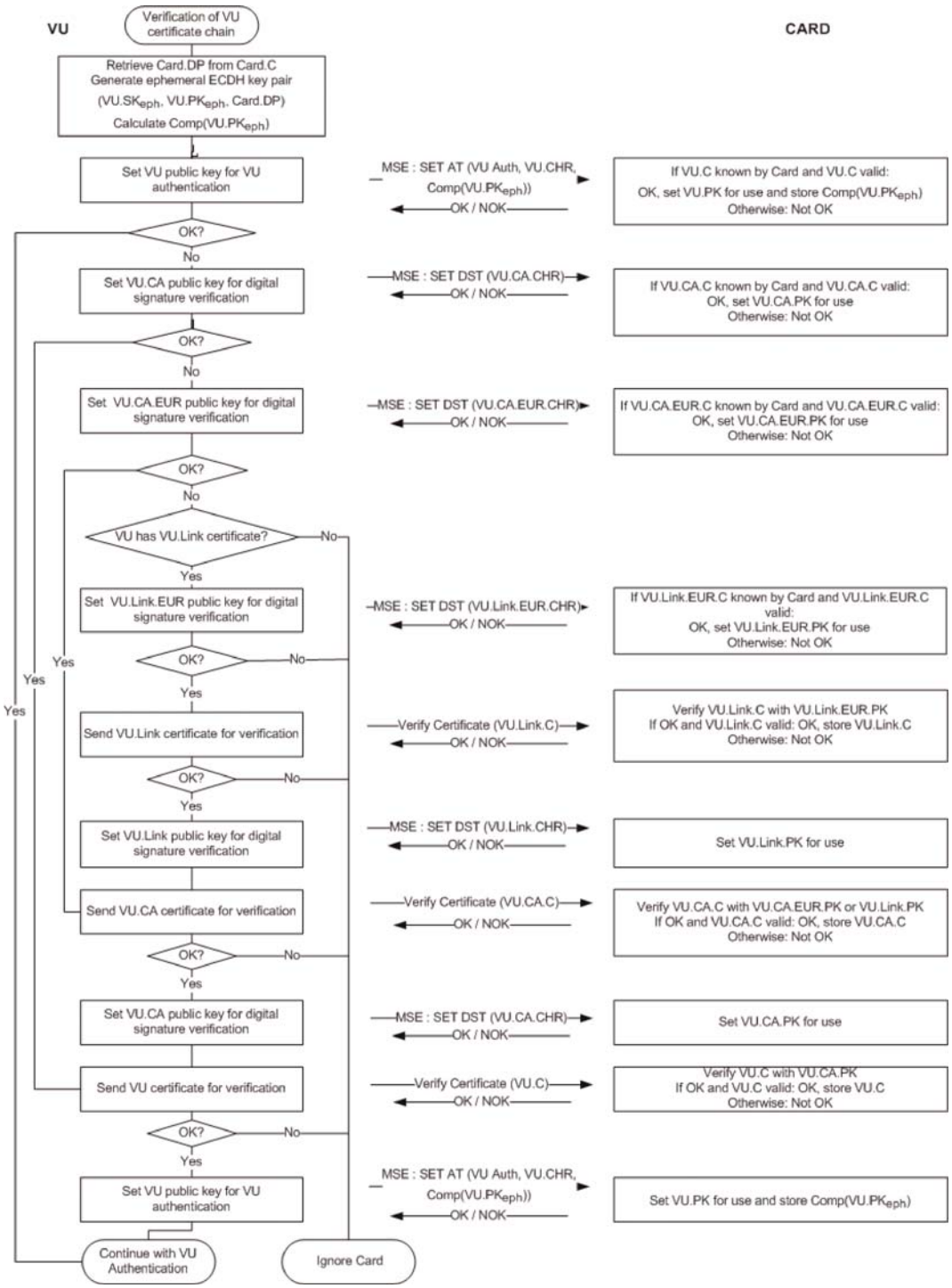
10.2.2 *A járműegység tanúsítványláncolatának kártya általi ellenőrzése*

CSM_161 A tachográfkártyáknak az 5. ábra szerinti protokollt kell használniuk a járműegység tanúsítványláncolatának ellenőrzésére.

▼B

5. ábra

A járműegység tanúsítványláncolatának kártya általi ellenőrzéséhez használt protokoll



Megjegyzések az 5. ábra tartalmához:

— Az ábrán látható járműegység-tanúsítványok és nyilvános kulcsok azok, amelyeket a kölcsönös hitelesítéshez használnak. A 9.1.4. szakaszban ezek VU_MA néven szerepelnek.

▼B

— Az ábrán szereplő VU.CA tanúsítványok és nyilvános kulcsok azok, amelyeket a járműegységek és a külső GNSS-eszközök tanúsítványainak aláírásához használnak. A 9.1.3. szakaszban ezek MSCA_VU-EGF néven szerepelnek.

— Az ábrán szereplő VU.CA.EUR tanúsítvány az az európai gyökértanúsítvány, amely a VU.CA tanúsítvány CAR-elemében van feltüntetve.

— Az ábrán szereplő VU.Link tanúsítvány a járműegység hivatkozási tanúsítványa, ha van ilyen. A 9.1.2. szakaszban foglaltaknak megfelelően ez az ERCA által létrehozott és az előző európai privát kulccsal aláírt új európai gyökérkulcspár hivatkozási tanúsítványa.

— A VU.Link.EUR tanúsítvány az az európai gyökértanúsítvány, amely a VU.Link tanúsítvány CAR-elemében van feltüntetve.

CSM_162 Ahogy az 5. ábra mutatja, a járműegység tanúsítványláncolatának ellenőrzése azzal kezdődik, hogy a járműegység megkísérli saját nyilvános kulcsát beállítani a tachográfkártyán történő használatra. Ha ez sikeres, az azt jelenti, hogy a kártya a múltban már sikeresen ellenőrizte a járműegység tanúsítványát és tárolta jövőbeli használatra. Ilyen esetben megtörténik a járműegység tanúsítványának használatra történő beállítása, és a folyamat a járműegység hitelesítésével folytatódik. Ha a kártya nem ismeri a járműegység tanúsítványát, akkor a járműegységnek egymás után be kell mutatnia a járműegység-tanúsítvány ellenőrzésére szolgáló VU.CA tanúsítványt, a VU.CA tanúsítvány ellenőrzésére szolgáló VU.CA.EUR tanúsítványt és adott esetben a hivatkozási tanúsítványt, hogy találjon egy, a kártya által ismert vagy ellenőrizhető tanúsítványt. Ha ilyen tanúsítványt talál, a kártyának ezzel kell ellenőriznie a járműegységről beolvasott járműegység-tanúsítványokat. Sikeres ellenőrzés esetén a járműegység végül beállítja saját nyilvános kulcsát a tachográfkártyán történő használatra. Ellenkező esetben a járműegységnek figyelmen kívül kell hagynia a kártyát.

Megjegyzés: a kártya három különböző módon ismerheti a VU.CA.EUR tanúsítványt:

— A VU.CA.EUR tanúsítvány megegyezik a kártya saját EUR-tanúsítványával.

— A VU.CA.EUR tanúsítvány a kártya saját EUR-tanúsítványának az előzménye, és a kártya már a kibocsátásakor tartalmazta ezt a tanúsítványt (lásd: CSM_91).

— A VU.CA.EUR tanúsítvány a kártya saját EUR-tanúsítványának az utódja, és a kártya a múltban hivatkozási tanúsítványt kapott egy másik járműegységtől, majd az ellenőrzést követően tárolta jövőbeli felhasználás céljából.

CSM_163 A járműegységnek az MSE: Set AT paranccsal be kell állítania saját nyilvános kulcsát a tachográfkártyán történő használatra. Ez a parancs (lásd a 2. függeléket) tartalmazza a beállított kulcshoz használt titkosítási mechanizmus meghatározását. Ez a mechanizmus az ECDSA algoritmus használatával történő járműegység-hitelesítés, a járműegység VU_MA kulcspárjának kulcsméretéhez illeszkedő hasító algoritmussal együtt (lásd: CSM_50).

▼B

CSM_164 Az MSE: Set AT parancsban emellett szerepel annak az ideiglenes kulcspárnak a meghatározása is, amelyet a járműegység a munkamenetkulcs-egyeztetéshez használ (lásd a 10.4. szakaszt). Ezért az MSE: Set AT parancs elküldése előtt a járműegységnek egy ideiglenes ECC-kulcspárt kell létrehoznia. Az ideiglenes kulcspár létrehozásához a járműegységnek a kártyatanúsítványban szereplő szabványosított tartományparamétereket kell használnia. Az ideiglenes kulcspár megnevezése: ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). A járműegységnek az ECDH ideiglenes nyilvános pont x koordinátáját kell használnia kulcsazonosítóként; ez a nyilvános kulcs tömörített ábrázolása, jelölése pedig $Comp(VU.PK_{eph})$.

CSM_165 Ha az MSE: Set AT parancs sikeres, a kártyának be kell állítania az adott VU.PK értékét a további járműegység-hitelesítéshez, és ideiglenesen tárolnia kell a $Comp(VU.PK_{eph})$ értéket. Ha a munkamenetkulcs-egyeztetés végrehajtása előtt két vagy több sikeres MSE: Set AT parancs küldésére is sor kerül, a kártyának csak a legutolsó fogadott $Comp(VU.PK_{eph})$ értéket kell tárolnia.

CSM_166 A kártyának ellenőriznie kell a járműegység által bemutatott vagy a járműegység által a kártyamemóriában történő tárolás során hivatkozott tanúsítványok időbeli érvényességét, és a lejárt tanúsítványokat el kell utasítania.

CSM_167 A járműegység által bemutatott tanúsítványok időbeli érvényességének ellenőrzéséhez minden egyes tachográfkártyának tárolnia kell olyan adatokat, amelyek az aktuális időpontot jelzik. Ezeket az adatokat a járműegységek nem módosíthatják közvetlenül. A kibocsátáskor a kártyán tárolt aktuális időpontot úgy kell beállítani, hogy megegyezzen a kártya Card_MA tanúsítványának hatálybalépési dátumával. A kártyának akkor kell frissítenie a rajta tárolt aktuális időpontot, ha egy járműegység által bemutatott hiteles „érvényes időforrás” típusú tanúsítvány hatálybalépési dátuma újabb, mint a kártyán tárolt aktuális időpont. Ilyen esetben a kártyának az adott tanúsítvány hatálybalépési dátumára kell állítania a rajta tárolt aktuális időpontot. A kártya csak a következő tanúsítványokat fogadhatja el érvényes időforrásként:

— Második generációs ERCA hivatkozási tanúsítványok.

— Második generációs MSCA-tanúsítványok.

— Olyan második generációs járműegység-tanúsítványok, amelyeket ugyanaz az ország bocsátott ki, mint a kártya saját kártyatanúsítványát vagy -tanúsítványait.

Megjegyzés: az utolsó követelmény azt is jelenti, hogy a kártyának képesnek kell lennie felismerni a járműegység-tanúsítvány (MSCA_VU-EGF tanúsítvány) CAR-elemét. Ez nem egyezik meg a saját tanúsítványa CAR-elemével, amely az MSCA_Card tanúsítvány.

CSM_168 Ahogy az 5. ábra mutatja, miután a kártya ellenőrizte egy korábban ismeretlen tanúsítvány hitelességét és érvényességét, tárolhatja a tanúsítványt jövőbeli felhasználás céljából, hogy a későbbiekben ne legyen szükség a tanúsítvány

▼B

hitelességének ismételt ellenőrzésére. A teljes tanúsítvány tárolása helyett előfordulhat, hogy a kártya csak a tanúsítványtörzs tartalmát tárolja (lásd a 9.3.2. szakaszt).

10.3. **Járműegység-hitelesítés**

CSM_169 A járműegységeknek és a kártyáknak a 6. ábra szerinti járműegység-hitelesítési protokoll használatával kell elvégezniük a járműegység kártyával történő hitelesítését. A járműegység-hitelesítés lehetővé teszi a tachográfkártya számára, hogy explicit módon ellenőrizze a járműegység hitelességét. Ehhez a járműegységnek a saját privát kulcsát kell használnia a kártya által létrehozott véletlenszerű szám aláírásához.

CSM_170 A kártya által létrehozott véletlenszerű szám mellett a járműegységnek a kártyatanúsítványból származó kártyatulajdonos-hivatkozást is szerepeltetnie kell az aláírásban.

Megjegyzés: így biztosítható, hogy az a kártya, amelynek a járműegység hitelesíti magát, ugyanaz a kártya, amelynek tanúsítványláncolatát a jármű korábban már ellenőrizte.

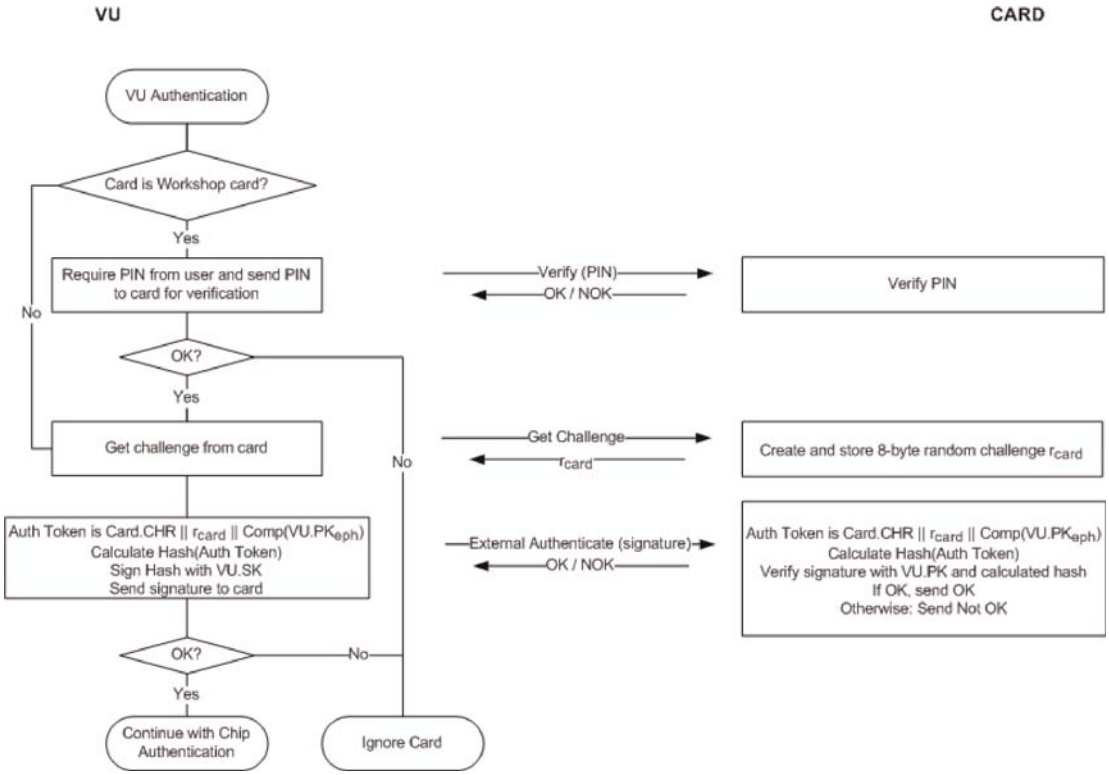
CSM_171 A járműegységnek az aláírásban szerepeltetnie kell még a Comp(VU.PK_{eph}) ideiglenes nyilvános kulcsot is, amelyet a járműegység a 10.4. szakaszban ismertetett chiphitelesítési eljárás során a biztonságos üzenetküldés konfigurálásához használ.

Megjegyzés: így biztosítható, hogy az a járműegység, amellyel a kártya a biztonságos üzenetküldés során kommunikál, ugyanaz a járműegység, amelyet a kártya hitelesített.

▼B

6. ábra

Járműegység-hitelesítési protokoll



CSM_172 Ha a járműegység-hitelesítés során a járműegység több GET CHALLENGE parancsot is elküld, akkor a kártyának minden alkalommal új 8 bájtos véletlenszerű számot kell létrehoznia, de csak a legutolsót tárolja.

CSM_173 A járműegység az ECDSA (a meghatározást lásd: [DSS]) aláírási algoritmust használja a járműegység-hitelesítéshez, a járműegység VU_MA kulcspárjának kulcsméretéhez kötött hasító algoritmus (lásd: CSM_50) alkalmazásával. Az aláírás egyszerű formátumú (lásd: [TR-03111]). A járműegységnek az elkészült aláírást el kell küldenie a kártya számára.

CSM_174 Amikor egy EXTERNAL AUTHENTICATE parancsban megkapja a járműegység aláírását, a kártyának a következő műveleteket kell elvégeznie:

— Ki kell számítania a hitelesítési tokent a Card.CHR, a kártya által létrehozott r_{card} véletlenszerű szám, valamint a járműegységhez tartozó Comp(VU.PK_{eph}) ideiglenes nyilvános kulcs azonosítójának összefűzésével.

— Ki kell számítania a hitelesítési token hasítását a járműegység VU_MA kulcspárjának kulcsméretéhez kötött hasító algoritmus használatával (lásd: CSM_50).

— Ellenőriznie kell a járműegység aláírását az ECDSA algoritmus, a VU.PK és a kiszámított hasítás használatával.

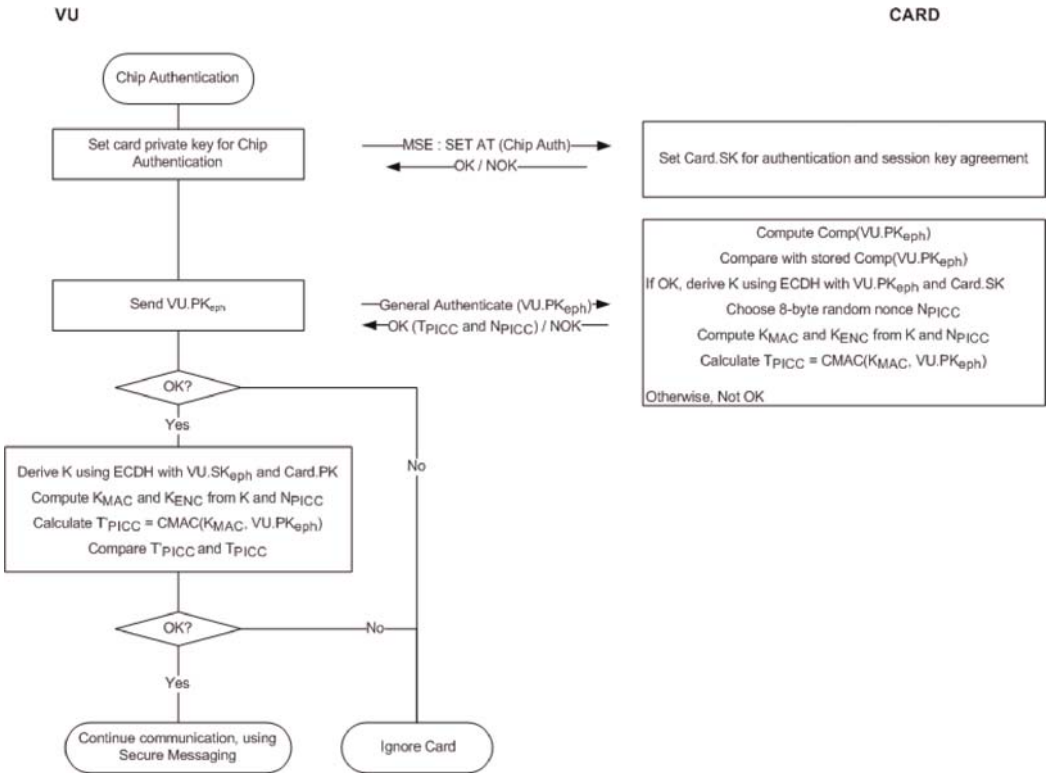
▼B

10.4. **Chiphitelesítés és munkamenetkulcs-egyeztetés**

CSM_175 A járműegységeknek és a kártyáknak a 7. ábra szerinti chiphitelesítési protokoll használatával kell elvégezniük a kártya járműegységgel történő hitelesítését. A chiphitelesítés lehetővé teszi a járműegység számára, hogy explicit módon ellenőrizze a kártya hitelességét.

7. ábra

Chiphitelesítés és munkamenetkulcs-egyeztetés



CSM_176 A járműegységnek és a kártyának a következő lépéseket kell elvégeznie:

1. A járműegység kezdeményezi a chiphitelesítési eljárást az MSE: Set AT parancs elküldésével, azaz chiphitelesítést indít az ECDH algoritmus használatával, amelynek eredményeképpen megkapja az AES-munkamenetkulcsnak a Card_MA kulcspár kulcsméretéhez kötött hosszát (lásd: CSM_50). A járműegységnek a kártyatanúsítvány alapján meg kell határoznia a kártya kulcspárjának kulcsméretét.

2. A járműegység elküldi a kártya számára saját ideiglenes $VU.PK_{eph}$ kulcspárjának nyilvános pontját. A járműegység ezt a kulcspárt a járműegység tanúsítványláncolatának ellenőrzése előtt hozta létre (lásd: CSM_164). A járműegység elküldte a $Comp(VU.PK_{eph})$ ideiglenes nyilvános kulcs azonosítóját a kártyának, amit a kártya eltárolt.

▼B

3. A kártya kiszámítja a Comp($VU.PK_{eph}$) értékét a $VU.PK_{eph}$ alapján, majd összehasonlítja a Comp($VU.PK_{eph}$) tárolt értékével.

4. Az ECDH algoritmus, valamint a kártya statikus privát kulcsának és a járműegység ideiglenes nyilvános kulcsának használatával a kártya kiszámít egy titkos K értéket.

5. A kártya kiválaszt egy véletlenszerű 8 bájtos N_{PICC} egyszer használatos számot, és ebből két AES-munkamenetkulcsot származtat (K_{MAC} és K_{ENC}) a K alapján. Lásd: CSM_179.

6. A K_{MAC} használatával a kártya hitelesítési tokent számít ki a járműegység ideiglenes nyilvános kulcsának azonosítójához: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). A kártya elküldi az N_{PICC} és a T_{PICC} értékét a járműegység számára.

7. Az ECDH algoritmus, valamint a kártya statikus privát kulcsának és a járműegység ideiglenes privát kulcsának használatával a járműegység kiszámítja ugyanazt a titkos K értéket, amelyet a kártya a 4. lépésben számított ki.

8. A járműegység K_{MAC} és K_{ENC} munkamenetkulcsot származtat a K és N_{PICC} értékeiből (lásd: CSM_179).

9. A járműegység ellenőrzi a T_{PICC} hitelesítési tokent.

CSM_177 A fenti 3. lépésben a kártyának ki kell számítania a Comp(VU.PKeph) értékét a VU.PKeph nyilvános pontjának x koordinátájaként.

CSM_178 A fenti 4. és 7. lépésben a kártyának és a járműegységnek a [TR-03111] szerinti ECKA-EG algoritmust kell használnia.

CSM_179 A fenti 5. és 8. lépésben a kártyának és a járműegységnek az AES-munkamenetkulcsokhoz tartozó kulcsszármaztatási funkciót kell használnia (lásd: [TR-03111]), a következő pontosságokkal és változtatásokkal:

— A számláló értéke ‘00 00 00 01’ a K_{ENC} esetében, és ‘00 00 00 02’ a K_{MAC} esetében.

— A folyamatban az opcionális *r* egyszer használatos számot kell használni, amelynek értéke N_{PICC}.

— A 128 bites AES-kulcsok származtatásához használt hasító algoritmus az SHA-256.

— A 192 bites AES-kulcsok származtatásához használt hasító algoritmus az SHA-384.

— A 256 bites AES-kulcsok származtatásához használt hasító algoritmus az SHA-512.

A munkamenetkulcsok hossza (vagyis az a hossz, amelyre a hasítást csonkolják) a Card_MA kulcspár méretéhez van kötve, a CSM_50 követelménynek megfelelően.

▼B

CSM_180 A fenti 6. és 9. lépésben a kártyának és a járműegységnek az [SP 800-38B] szerinti AES algoritmust kell használnia CMAC-üzemmódban. A T_{PICC} hossza az AES-munkamenetkulcsok hosszához van kötve, a CSM_50 követelménynek megfelelően.

10.5. **Biztonságos üzenetküldés**

10.5.1 *Általános tudnivalók*

CSM_181 A sikeres chiphitelesítést követően és a munkamenet végéig a járműegység és a tachográfkártya között kicserélt minden parancs és válasz kiadására biztonságos üzenetküldéssel kerül sor.

CSM_182 A biztonságos üzenetküldést a csak hitelesítésre szolgáló üzemmódban kell használni, kivéve az SM-R-ENC-MAC-G2 (lásd a 2. függelék 4. szakaszát) hozzáférési feltétellel történő fájlolvasáskor. Ebben az üzemmódban titkosítási ellenőrző összeget (más néven MAC) adnak a parancsokhoz és válaszokhoz, hogy biztosítva legyen az üzenetek hitelessége és integritása.

CSM_183 Ha egy fájlból SM-R-ENC-MAC-G2 hozzáférési feltétellel olvassák ki az adatokat, akkor a biztonságos üzenetküldést „titkosítás, majd hitelesítés” üzemmódban kell használni, azaz a válasz adatait előbb titkosítani kell, hogy biztosítva legyen az üzenet titkossága, majd a hitelesség és integritás érdekében ki kell számítani a formázott titkosított adatok MAC-értékét.

CSM_184 A biztonságos üzenetküldésnek az AES algoritmust kell használnia (lásd: [AES]) a chiphitelesítés során egyeztetett K_{MAC} és K_{ENC} munkamenetkulccsal.

CSM_185 Küldési sorrendszámlálóként (SSC) előjel nélküli egész számot kell használni az ismétléses támadások megakadályozására. Az SSC méretének egyenlőnek kell lennie az AES blokkméretével (128 bit). Az SSC-nek olyan formátumúnak kell lennie, amelyben a legjelentősebb bit kerül előre. A küldési sorrendszámlálót a biztonságos üzenetküldés megkezdésekor nullázni kell (‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’ értékre kell inicializálni). Az SSC értékének minden alkalommal növekednie kell, amikor egy parancs vagy válasz APDU jön létre, azaz mivel az SSC kezdőértéke a biztonságos üzenetküldési munkamenetben 0, az értéke az első parancsban 1 lesz. Az SSC értéke az első válasznál 2 lesz.

CSM_186 Az üzenetek titkosításához a K_{ENC} értékét használják az AES algoritmus titkosított blokkok láncolatán alapuló (CBC) üzemmódjában (lásd: ISO 10116. sz. szabvány), m = 1 kihagyási paraméterrel és SV = E(K_{ENC}, SSC) inicializálási vektorral, azaz a küldési sorrendszámláló K_{ENC} kulccsal titkosított aktuális értékével.

CSM_187 Az üzenethitelesítéshez a K_{MAC} értéket kell alkalmazni az AES algoritmus CMAC-üzemmódjában (lásd: [SP 800-38B]). A MAC hossza az AES-munkamenetkulcsok hosszához igazodik (lásd: CSM_50). A küldési sorrendszámlálót bele kell foglalni a MAC értékébe úgy, hogy a hitelesítendő adatcsomag elé illesztik.

▼B

10.5.2 *Biztonságos üzenetstruktúra*

CSM_188 A biztonságos üzenetküldés csak az 5. táblázat tartalmában szereplő biztonságos üzenetküldési adatobjektumokat használhatja (lásd: ISO 7816-4. sz. szabvány). Az üzeneteknek a táblázatban látható sorrendben kell használniuk az adatobjektumokat.

5. táblázat

A biztonságos üzenetküldés adatobjektumai

Adatobjektum neve	Címke	Szerepeltetése (K)ötelező, (F)eltételes vagy (T)ilos a	
		parancsokban	válaszokban
Egyszerű értékű, nem BER-TLV-ben kódolt adat	81	F	F
Egyszerű értékű, BER-TLV-ben kódolt, de SM DO-kat nem tartalmazó adat	B3	F	F
Kitöltésjelző és kriptogram; egyszerű értékű, nem BER-TLV-ben kódolt adat	87	F	F
Védett Le	97	F	T
Feldolgozási állapot	99	T	K
Titkosítási ellenőrző összeg	8E	K	K

Megjegyzés: ahogy a 2. függelékben le van írva, a tachográfkártyák támogathatják a READ BINARY és UPDATE BINARY parancsot páratlan INS bájttal (‘B1’, ill. ‘D7’). Ezek a parancsváltozatok a 32 768 bájtnál nagyobb fájlok olvasásához és frissítéséhez szükségesek. Ilyen parancsváltozat használatakor ‘B3’ címkével rendelkező adatobjektumot kell alkalmazni a ‘81’ címkével rendelkező helyett. További információkért lásd a 2. függeléket.

CSM_189 Minden SM-adatobjektumot DER TLV-ben kell kódolni (lásd: ISO 8825-1. sz. szabvány). Ez a kódolás a következő címke-hossz-érték (TLV) struktúrát eredményezi:

Címke: a címke egy vagy két oktettben (nyolcbites egységben) van kódolva, és a tartalmat jelöli.

Hossz: a hossz kódolása előjel nélküli egész számként történik egy, két vagy három oktettben, így a maximális hossz 65 535 oktett. A minimális számú oktettet kell alkalmazni.

Érték: az érték kódolása nulla vagy több oktettben történik.

CSM_190 A biztonságos üzenetküldéssel védett APDU-kat a következőképpen kell létrehozni:

— A parancsfejnek a MAC-számítás részét kell képeznie, ezért a ‘0C’ értéket kell használni a CLA besorolási bájthoz.

▼B

— A 2. függelékben foglaltaknak megfelelően minden INS bájtnak párosnak kell lennie; ez alól csak a READ BINARY és UPDATE BINARY parancsok páratlan INS bájtjai jelenthetnek kivételt.

— Az Lc tényleges értéke Lc'-re módosul a biztonságos üzenetküldés alkalmazása után.

— Az adatmezőnek SM-adatobjektumokból kell állnia.

— Az APDU védett parancsban az új Le bájt értéke ‘00’. Szükség esetén egy ‘97’ adatobjektumot kell belefoglalni az adatmezőbe az Le eredeti értékének átadásához.

CSM_191 Minden titkosítandó adatobjektumot az ISO 7816-4. sz. szabvány által meghatározott módon töltenek ki a ‘01’ kitöltés–tartalom jelző használatával. A MAC kiszámításához az APDU minden egyes adatobjektumát külön is ki kell tölteni az ISO 7816-4. sz. szabvány előírásainak megfelelően.

Megjegyzés: a biztonságos üzenetküldés kitöltését mindig a biztonságos üzenetküldési réteg végzi, nem a CMAC vagy a CBC algoritmus.

Összegzés és példák

Egy biztonságos üzenetküldéssel kiadott, parancsot tartalmazó APDU struktúrája a következő, a megfelelő biztosítatlan parancstól függően (a DO az adatobjektumot jelzi):

1. eset:	CLA INS P1 P2 || Lc' || DO ‘8E’ || Le
2. eset:	CLA INS P1 P2 || Lc' || DO ‘97’ || DO‘8E’ || Le
3. eset (páros INS bájt):	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘8E’ || Le
3. eset (páratlan INS bájt):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘8E’ || Le
4. eset (páros INS bájt):	CLA INS P1 P2 || Lc' || DO ‘81’ || DO‘97’ || DO‘8E’ || Le
4. eset (páratlan INS bájt):	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO‘97’ || DO‘8E’ || Le

ahol Le = ‘00’ vagy ‘00 00’ attól függően, hogy rövid vagy kiterjesztett hosszúságú mezőket használnak; lásd: ISO 7816-4. sz. szabvány.

Egy biztonságos üzenetküldéssel kiadott, választ tartalmazó APDU struktúrája a következő, a megfelelő biztosítatlan parancstól függően:

1. vagy 3. eset:	DO 99 || DO 8E || SW1SW2
2. vagy 4. eset (páros INS bájt) titkosítással:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
2. vagy 4. eset (páros INS bájt) titkosítás nélkül:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
2. vagy 4. eset (páratlan INS bájt) titkosítás nélkül:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

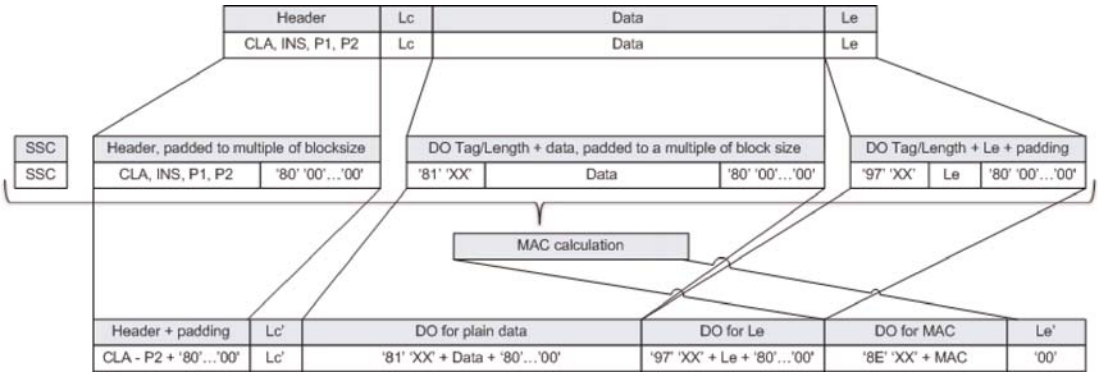
Megjegyzés: A 2. vagy 4. esetet (páratlan INS bájt) titkosítással soha nem használják a járműegység és kártya közötti kommunikációban.

▼B

Alább három példa látható az APDU-átalakításokra a páros INS-kóddal rendelkező parancsokhoz. A 8. ábra egy hitelesített 4. esetbeli, parancsot tartalmazó APDU-t, a 9. ábra pedig egy hitelesített 2./4. esetbeli, választ tartalmazó APDU-t mutat be, míg a 10. ábra egy titkosított és hitelesített 2./4. esetbeli, választ tartalmazó APDU-t ábrázol.

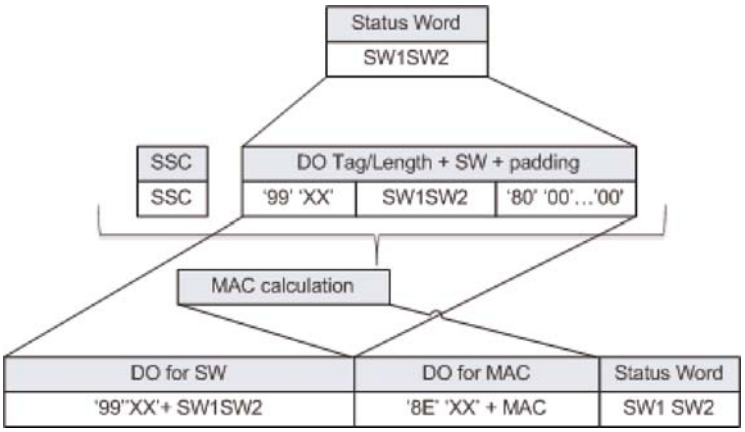
8. ábra

Átalakítás hitelesített 4. esetbeli, parancsot tartalmazó APDU-hoz



9. ábra

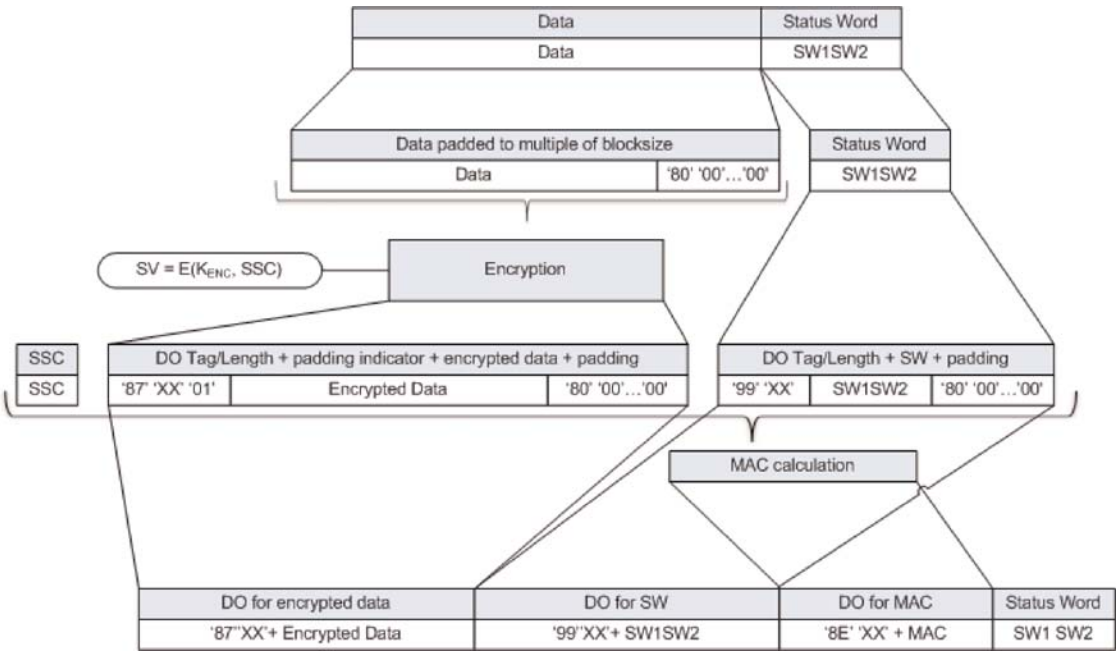
Átalakítás hitelesített 1./3. esetbeli, választ tartalmazó APDU-hoz



▼B

10. ábra

Átalakítás titkosított és hitelesített 2./4. esetbeli, választ tartalmazó APDU-hoz



10.5.3 *Biztonságos üzenetküldési munkamenet megszakítása*

CSM_192 A jármű akkor és csakis akkor szakíthatja meg a folyamatban lévő biztonságos üzenetküldési munkamenetet, ha a következők egyikére kerül sor:

— egyszerű, választ tartalmazó APDU-t kap;

— biztonságos üzenetküldési hibát észlel egy választ tartalmazó APDU-ban:

  — Egy várt biztonságos üzenetküldési objektum hiányzik, nem megfelelő az adatobjektumok sorrendje, vagy ismeretlen adatobjektum szerepel a válaszban.

  — Egy biztonságos üzenetküldési adatobjektum hibás, például nem megfelelő a MAC-érték, hibás a TLV-struktúra vagy a '87' címkében lévő kitöltésjelző nem '01'.

— a kártya állapotbájtot küld, amely azt jelzi, hogy SM-hibát észlelt (lásd: CSM_194);

— a jelenlegi munkamenet eléri a parancsok és a kapcsolódó válaszok határértékét. Egy adott járműegységhez ezt a határértéket a gyártó definiálja, figyelembe véve az alkalmazott hardver biztonsági követelményeit – maximális értéke 240 SM-parancs és -válasz munkamenetenként.

▼B

CSM_193 A tachográfkártya akkor és csakis akkor szakítja meg a folyamatban lévő biztonságos üzenetküldési munkamenetet, ha a következők egyikére kerül sor:

— egyszerű, parancsot tartalmazó APDU-t kap;

— biztonságos üzenetküldési hibát észlel egy parancsot tartalmazó APDU-ban:

— Egy várt biztonságos üzenetküldési objektum hiányzik, nem megfelelő az adatobjektumok sorrendje, vagy ismeretlen adatobjektum szerepel a válaszban.

— Egy biztonságos üzenetküldési adatobjektum hibás, például hibás a MAC-érték vagy a TLV-struktúra.

— az eszközt áramtalanítják vagy alaphelyzetbe állítják;

— a járműegység kiválaszt egy alkalmazást a kártyán;

— a járműegység elindítja a járműegység-hitelesítési eljárást;

— a jelenlegi munkamenet eléri a parancsok és a kapcsolódó válaszok határértékét. Egy adott kártyához ezt a határértéket a gyártó definiálja, figyelembe véve az alkalmazott hardver biztonsági követelményeit – maximális értéke 240 SM-parancs és -válasz munkamenetenként.

CSM_194 Biztonságos üzenetküldés hibakezelése a tachográfkártyán:

— Ha egy parancsot tartalmazó APDU-ban nem találhatók bizonyos várt biztonságos üzenetküldési adatobjektumok, nem megfelelő az adatobjektumok sorrendje vagy ismeretlen adatobjektumok szerepelnek, a tachográfkártya a ‘69 87’ állapotbájtokkal válaszol.

— Ha egy parancsot tartalmazó APDU-ban egy biztonságos üzenetküldési adatobjektum hibás, a tachográfkártya a ‘69 88’ állapotbájtokkal válaszol.

Ilyen esetben az állapotbájtokat nem a biztonságos üzenetküldés használatával kell visszaküldeni.

CSM_195 Ha megszakítanak egy biztonságos üzenetküldési munkamenetet egy járműegység és egy tachográfkártya között, a járműegység és a tachográfkártya:

— biztonságosan megsemmisíti a tárolt munkamenetkulcsokat;

— és azonnal új biztonságos üzenetküldési munkamenetet indít (lásd a 10.2–10.5. szakaszt).

CSM_196 Ha a járműegység bármilyen okból úgy dönt, hogy újraindítja a kölcsönös hitelesítést egy behelyezett kártyához, a folyamatnak a kártya tanúsítványláncolatának ellenőrzésével kell kezdődnie (lásd a 10.2. szakaszt) és a 10.2–10.5. szakaszban leírtak szerint kell folytatódnia.

▼B

11. JÁRMŰEGYSÉG ÉS KÜLSŐ GNSS-ESZKÖZ ÖSSZEKAPCSOLÁSA, KÖLCSÖNÖS HITELESÍTÉSE ÉS BIZTONSÁGOS ÜZENETKÜLDÉSE

11.1. **Általános tudnivalók**

CSM_197 A járműegység által a helyzetmeghatározáshoz használt GNSS-eszköz lehet belső (azaz a járműegység burkolatába épített, nem leválasztható) vagy külső modul is. Az előbbi esetben nem szükséges szabványosítani a GNSS-eszköz és a járműegység közötti belső kommunikációt, és ilyenkor az e fejezetben leírt követelmények nincsenek érvényben. Az utóbbi esetben a járműegység és a külső GNSS-eszköz közötti kommunikációt az e fejezetben leírtak szerint szabványosítani és védeni kell.

CSM_198 A járműegység és a külső GNSS-eszköz közötti biztonságos kommunikáció ugyanúgy zajlik, mint a járműegység és a tachográfkártya közötti biztonságos kommunikáció: a kártya szerepét ilyenkor a külső GNSS-eszköz(EGF) tölti be. Az EGF-nek a 10. fejezetben említett, tachográfkártyákra vonatkozó összes követelményt teljesítenie kell, figyelembe véve az ebben a fejezetben leírt eltéréseket, magyarázatokat és kiegészítéseket. Ez azt jelenti, hogy a kölcsönös tanúsítványláncolat-hitelesítést, a járműegység-hitelesítést és chip-hitelesítést is el kell végezni a 11.3. és 11.4. szakaszban leírtak szerint.

CSM_199 A járműegység és az EGF közötti kommunikáció abban különbözik a járműegység és a kártya közötti kommunikációtól, hogy a járműegységet és az EGF-et a műhelyben egy alkalommal párosítani kell, mielőtt a járműegység és az EGF között normál üzemben megkezdődhetne a GNSS-alapú adatok cseréje. Ezt az összekapcsolási eljárást a 11.2. szakasz ismerteti részletesen.

CSM_200 A járműegység és az EGF közötti kommunikációhoz az ISO 7816-4. sz. és az ISO 7816-8. sz. szabvány szerinti APDU-parancsokat kell használni. A kérdéses APDU-k pontos struktúráját ennek a mellékletnek a 2. függeléke ismerteti.

11.2. **A járműegység és a külső GNSS-eszköz összekapcsolása**

CSM_201 A járműegységet és a járműben található EGF-et a műhelynek kell összekapcsolnia. A járműegység és az EGF csak összekapcsolva lehet képes normál üzemben kommunikálni.

CSM_202 A járműegység és az EGF összekapcsolása csak akkor lehetséges, ha a járműegység kalibrálási üzemmódban van. Az összekapcsolást a járműegységnek kell kezdeményeznie.

CSM_203 A műhely a járműegységet bármikor újra összekapcsolhatja egy másik EGF-fel vagy ugyanazzal az EGF-fel. Az újbóli összekapcsolás során a járműegységnek biztonságosan meg kell semmisítenie a memóriájában tárolt EGF_MA tanúsítványt, és az újonnan hozzákapcsolt EGF egység EGF_MA tanúsítványát kell tárolnia.

CSM_204 A műhely a külső GNSS-eszközt bármikor újra összekapcsolhatja egy másik járműegységgel vagy ugyanazzal a járműegységgel. Az újbóli összekapcsolás során az EGF-nek biztonságosan meg kell semmisítenie a memóriájában tárolt VU_MA tanúsítványt, és az újonnan hozzákapcsolt járműegység VU_MA tanúsítványát kell tárolnia.

▼B

11.3. **Kölcsönös tanúsítványláncolat-ellenőrzés**

11.3.1 *Általános tudnivalók*

CSM_205 A járműegység és az EGF közötti kölcsönös tanúsítványlánc-colat-ellenőrzésre csak akkor kerülhet sor, amikor egy műhelyben összekapcsolják a járműegységet és az EGF-et. Az összekapcsolt járműegység és EGF normál üzeme során nem történik tanúsítvány-ellenőrzés. Ehelyett a járműegységnek és az EGF-nek megbízhatónak kell tekintenie az összekapcsoláskor tárolt tanúsítványokat, miután ellenőrzik ezen tanúsítványok időbeli érvényességét. A járműegység és az EGF a normál üzem során más tanúsítványokat nem tekinthet megbízhatónak, így garantálva a járműegység és az EGF közötti kommunikáció biztonságát.

11.3.2 *A járműegység és az EGF összekapcsolásakor*

CSM_206 Egy EGF járműegységgel való összekapcsolásakor a járműegységnek a 4. ábra szerinti protokollt kell használnia (10.2.1. szakasz) a külső GNSS-eszköz tanúsítványláncolatának ellenőrzéséhez.

Megjegyzések a 4. ábra tartalmához e függelék vonatkozásában:

— A kommunikáció vezérlését ez a függelék nem tárgyalja. Ugyanakkor tudni kell, hogy az EGF nem intelligens kártya, ezért a járműegység valószínűleg nem küld alaphelyzetbe állítási parancsot a kommunikáció kezdeményezéséhez, és nem fogad ATR-t.

— Az ábrán szereplő kártyatanúsítványok és nyilvános kulcsok úgy értelmezendők, mint az EGF kölcsönös hitelesítéshez használt tanúsítványai és nyilvános kulcsai. A 9.1.6. szakaszban ezek EGF_MA néven szerepelnek.

— Az ábrán szereplő Card.CA tanúsítványok és nyilvános kulcsok úgy értelmezendők, mint az MSCA tanúsítványai és nyilvános kulcsai, amelyeket az EGF-tanúsítványok aláírására használ. A 9.1.3. szakaszban ezek MSCA_VU-EGF néven szerepelnek.

— Az ábrán szereplő Card.CA.EUR tanúsítvány az az európai gyökértanúsítvány, amely az MSCA_VU-EGF tanúsítvány CAR-elemében van feltüntetve.

— Az ábrán szereplő Card.Link tanúsítvány az EGF hivatkozási tanúsítványa, ha van ilyen. A 9.1.2. szakaszban foglaltaknak megfelelően ez az ERCA által létrehozott és az előző európai privát kulccsal aláírt új európai gyökérkulcspár hivatkozási tanúsítványa.

— A Card.Link.EUR tanúsítvány az az európai gyökértanúsítvány, amely a Card.Link tanúsítvány CAR-elemében van feltüntetve.

— A `cardExtendedSerialNumber` helyett a járműegységnek a `sensorGNSSserialNumber` értéket kell használnia az EF ICC-ről.

— A menetíró készülék AID eleme helyett a járműegységnek az EGF AID elemét kell kiválasztania.

— Az „Ignore Card” parancsot „Ignore EGF” parancsként kell értelmezni.

▼B

CSM_207 Miután ellenőrizte az EGF_MA tanúsítványt, a járműegységnek tárolnia kell azt a normál üzemben történő használathoz; lásd a 11.3.3. szakaszt.

CSM_208 Járműegységgel való összekapcsolásakor a külső GNSS-eszköznek az 5. ábra szerinti protokollt kell használnia (10.2.2. szakasz) a járműegység tanúsítványláncolatának ellenőrzéséhez.

Megjegyzések a 5. ábra tartalmához e függelék vonatkozásában:

— A járműegységnek új ideiglenes kulcspárt kell létrehoznia az EGF-tanúsítványban lévő tartományparaméterek használatával.

— Az ábrán látható járműegység-tanúsítványok és nyilvános kulcsok azok, amelyeket a kölcsönös hitelesítéshez használnak. A 9.1.4. szakaszban ezek VU_MA néven szerepelnek.

— Az ábrán szereplő VU.CA tanúsítványok és nyilvános kulcsok azok, amelyeket a járműegységek és a külső GNSS-eszközök tanúsítványainak aláírásához használnak. A 9.1.3. szakaszban ezek MSCA_VU-EGF néven szerepelnek.

— Az ábrán szereplő VU.CA.EUR tanúsítvány az az európai gyökértanúsítvány, amely a VU.CA tanúsítvány CAR-elemében van feltüntetve.

— Az ábrán szereplő VU.Link tanúsítvány a járműegység hivatkozási tanúsítványa, ha van ilyen. A 9.1.2. szakaszban foglaltaknak megfelelően ez az ERCA által létrehozott és az előző európai privát kulccsal aláírt új európai gyökérkulcspár hivatkozási tanúsítványa.

— A VU.Link.EUR tanúsítvány az az európai gyökértanúsítvány, amely a VU.Link tanúsítvány CAR-elemében van feltüntetve.

CSM_209 A CSM_167 követelménytől eltérően az EGF-nek a GNSS időértékét kell használnia bármely bemutatott tanúsítvány időbeli érvényességének ellenőrzéséhez.

CSM_210 Miután ellenőrizte a VU_MA tanúsítványt, a külső GNSS-eszköz tárolja azt a normál üzemben történő használathoz; lásd a 11.3.3. szakaszt.

11.3.3 *Működés normál üzemben*

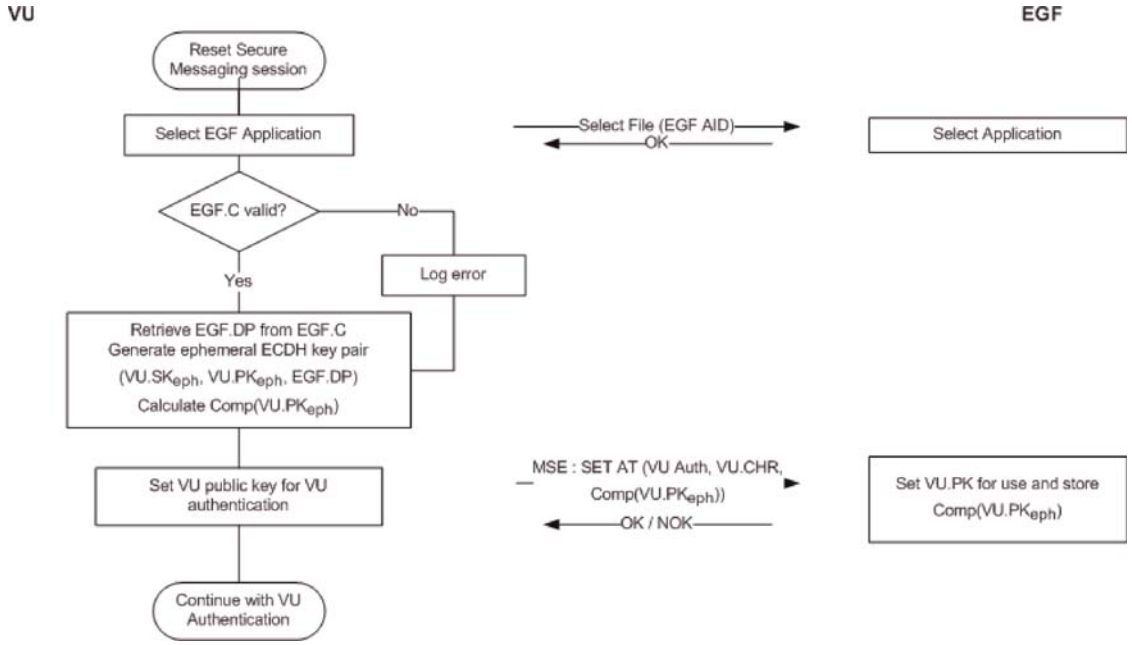
CSM_211 Normál üzem során a járműegységnek és az EGF-nek a 11. ábra szerinti protokollt kell használnia a tárolt EGF_MA és VU_MA tanúsítványok időbeli érvényességének ellenőrzéséhez és a VU_MA nyilvános kulcs későbbi járműegység-hitelesítéshez történő beállításához. Normál üzemben nem kerül sor a tanúsítványláncolatok további kölcsönös ellenőrzésére.

Fontos megjegyezni, hogy a 11. ábra lényegében a 4. ábra és az 5. ábra szerinti első lépésekből áll. Ugyanakkor mivel az EGF nem intelligens kártya, a járműegység valószínűleg nem küld alaphelyzetbe állítási parancsot a kommunikáció kezdeményezéséhez, és nem fogad ATR-t. Ennek részleteit azonban ez a függelék nem tárgyalja.

▼B

11. ábra

A tanúsítvány időbeli érvényességének kölcsönös ellenőrzése a járműegység és az EGF normál üzeme során



CSM_212 Ahogy a 11. ábra mutatja, a járműegységnek hibát kell naplóznia, ha az EGF_MA tanúsítvány nem érvényes. Ugyanakkor a kölcsönös hitelesítésnek, a kulcsegyeztetésnek és az ezt követő, biztonságos üzenetküldéssel végzett kommunikációnak normál módon folytatódnia kell.

11.4. **Járműegység-hitelesítés, chiphitelesítés és munkamenetkulcs-egyeztetés**

CSM_213 A járműegység és az EGF között végzett járműegység-hitelesítésre, chiphitelesítésre és munkamenetkulcs-egyeztetésre az összekapcsoláskor kerül sor, valamint minden esetben, amikor normál üzemben újra létrehoznak egy biztonságos üzenetküldési munkamenetet. A járműegységnek és az EGF-nek a 10.3. és 10.4. szakaszban leírt folyamatokat kell elvégeznie. Az említett szakaszokban található minden követelményt be kell tartani.

11.5. **Biztonságos üzenetküldés**

CSM_214 A sikeres chiphitelesítést követően és a munkamenet végéig a járműegység és a külső GNSS-eszköz között kicserélt minden parancsot és választ a csak hitelesítésre szolgáló üzemmódú biztonságos üzenetküldéssel kell védeni. A 10.5. szakaszban szereplő minden követelményt be kell tartani.

CSM_215 Ha egy járműegység és egy EGF közötti biztonságos üzenetküldési munkamenetet megszakítanak, a járműegységnek azonnal létre kell hoznia egy új biztonságos üzenetküldési munkamenetet, a 11.3.3. és 11.4. szakaszban leírtak szerint.

12. JÁRMŰEGYSÉG ÉS MOZGÁSÉRZÉKELŐ KÖZÖTTI PÁROSÍTÁS ÉS KOMMUNIKÁCIÓ

12.1. **Általános tudnivalók**

CSM_216 A járműegység és a mozgásérzékelő közötti kommunikáció a párosítás során és normál üzemben az ISO 16844-3. sz. szabványban meghatározott interfészprotokoll használatával történik, az e fejezetben és a 9.2.1. szakaszban leírt eltérésekkel.

▼B

Megjegyzés: e fejezet olvasói feltételezhetően ismerik az ISO 16844-3. sz. szabvány tartalmát.

12.2. **Járműegység és mozgásérzékelő párosítása különböző kulcsgenerációk használatával**

Ahogy a 9.2.1. szakaszban le van írva, a mozgásérzékelő mesterkulcsát és minden társított kulcsát rendszeresen cserélik. Emiatt egyszerre akár három, mozgásérzékelőhöz kapcsolódó $K_{M\text{-}WC}$ AES-kulcs is megtalálható lehet (egymást követő generációkból) a műhelykártyákon. Ennek megfelelően a mozgásérzékelőkben akár három különböző AES-alapú (a mozgásérzékelő K_M mesterkulcsának egymást követő generációin alapuló) adattitkosítás is jelen lehet. Egy adott járműegység csak egyetlen, mozgásérzékelőhöz kapcsolódó kulcsot tartalmaz, a $K_{M\text{-}VU}$ kulcsot.

CSM_217 Egy második generációs járműegység és egy második generációs mozgásérzékelő párosítása a következőképpen zajlik (lásd az ISO 16844-3. sz. szabvány 6. táblázatát):

1. A járműegységbe behelyeznek egy második generációs kártyát, és a járműegységet csatlakoztatják a mozgásérzékelőhöz.

2. A járműegység beolvassa az összes elérhető $K_{M\text{-}WC}$ kulcsot a műhelykártyáról, megvizsgálja a kulcsverzió-számukat, majd kiválasztja azt, amelyiknek a verzió-száma egyezik a $K_{M\text{-}VU}$ kulcs verziószámával. Ha a megfelelő $K_{M\text{-}WC}$ kulcs nem található meg a műhelykártyán, a járműegység megszakítja a párosítási folyamatot, és a hibának megfelelő hibaüzenetet jelenít meg a műhelykártya tulajdonosa számára.

3. A járműegység a mozgásérzékelő K_M mesterkulcsát a $K_{M\text{-}VU}$ és $K_{M\text{-}WC}$ értékéből, a K_{ID} azonosítási kulcsot pedig a K_M értékéből számítja ki (lásd a 9.2.1. szakaszt).

4. A járműegység az ISO 16844-3. sz. szabvány szerint elküldi a párosítási folyamatot kezdeményező utasítást, és a mozgásérzékelőtől kapott sorozatszámot titkosítja a K_{ID} azonosítási kulccsal. A járműegység visszaküldi a titkosított sorozatszámot a mozgásérzékelőnek.

5. A mozgásérzékelő a titkosított sorozatszámot egymás után összehasonlítja a sorozatszám általa tárolt egyes titkosításaival. Ha egyezést talál, hitelesíti a járműegységet. A mozgásérzékelő észleli a jármű által használt K_{ID} generációját, és a párosítási kulcs megfelelő titkosított verzióját küldi vissza, vagyis azt a titkosított változatot, amelyet a K_M ugyanazon generációjával készítettek.

6. A járműegység visszafejti a párosítási kulcsot a K_M használatával, majd létrehoz egy K_S munkamenetkulcsot, titkosítja a párosítási kulccsal, és visszaküldi az eredményt a mozgásérzékelőnek. A mozgásérzékelő visszafejti a K_S kulcsot.

7. A jármű az ISO 16844-3. sz. szabvány előírásainak megfelelően összeállítja a párosítási adatokat, titkosítja az információkat a párosítási kulccsal, majd elküldi az eredményt a mozgásérzékelőnek. A mozgásérzékelő visszafejti a párosítási adatokat.

8. A mozgásérzékelő titkosítja a megkapott párosítási adatokat a megkapott K_S kulccsal, és visszaküldi a járműegység számára. A járműegység ellenőrzi, hogy a párosítási adatok megegyeznek-e a járműegység által az előző lépésben a mozgásérzékelő számára elküldött

▼B

adatokkal. Ha igen, akkor ez igazolja, hogy a mozgásérzékelő ugyanazt a K_S kulcsot használta, mint a járműegység, így az 5. lépésben a párosítási kulcsot a K_M megfelelő generációjával titkosítva küldte el. Ezzel megtörténik a mozgásérzékelő hitelesítése.

Látható, hogy a 2. és 5. lépés eltér az ISO 16844-3 szabványos eljárásától, míg a többi lépés szabványos.

Példa: Tegyük fel, hogy a párosítás az ERCA (3) tanúsítvány érvényességének első évében történik; lásd: a 9.2.1.2. szakasz 2. ábráját. Továbbá:

— Tegyük fel, hogy a mozgásérzékelőt az ERCA (1) tanúsítvány érvényességének utolsó évében bocsátották ki. Ezért a következő kulcsokat és adatokat tartalmazza:

  — $N_s[1]$: a mozgásérzékelő sorozatszáma a K_{ID} 1. generációjával titkosítva;

  — $N_s[2]$: a mozgásérzékelő sorozatszáma a K_{ID} 2. generációjával titkosítva;

  — $N_s[3]$: a mozgásérzékelő sorozatszáma a K_{ID} 3. generációjával titkosítva;

  — $K_P[1]$: a mozgásérzékelő generációját eggyel megelőző generációjú párosítási kulcs ([1]), a K_M 1. generációjával titkosítva;

  — $K_P[2]$: a mozgásérzékelő generációját kettővel megelőző generációjú párosítási kulcs, a K_M 2. generációjával titkosítva;

  — $K_P[3]$: a mozgásérzékelő generációját hárommal megelőző generációjú párosítási kulcs, a K_M 3. generációjával titkosítva.

— Tegyük fel, hogy a műhelykártyát az ERCA (3) tanúsítvány érvényességének első évében bocsátották ki. Ezért a $K_{M\text{-}WC}$ kulcs 2. és 3. generációját tartalmazza.

— Tegyük fel, hogy a járműegység a jelenlegit kettővel megelőző generációhoz tartozik, és a $K_{M\text{-}VU}$ 2. generációját tartalmazza.

Ebben az esetben a 2–5. lépésben a következő történik:

— 2. lépés: A járműegység beolvassa a $K_{M\text{-}WC}$ 2. és 3. generációját a műhelykártyáról, és megvizsgálja ezek verziószámát.

— 3. lépés: A járműegység kombinálja a kettővel ezelőtti generációjú $K_{M\text{-}WC}$ kulcsot a saját $K_{M\text{-}VU}$ kulcsával, hogy kiszámítsa a K_M és a K_{ID} értékét.

— 4. lépés: A járműegység a K_{ID} használatával titkosítja a mozgásérzékelőtől kapott sorozatszámot.

— 5. lépés: A mozgásérzékelő a megkapott adatokat összehasonlítja az $N_s[1]$ értékkel, és nem talál egyezést. Ezután az $N_s[2]$ értékkel hasonlítja össze, és egyezést talál. Ebből azt a következtetést vonja le, hogy a járműegység a kettővel ezelőtti generációhoz tartozik, ezért a $K_P[2]$ kulcsot küldi vissza.

([1]) Az adott generációt eggyel, kettővel és hárommal megelőző generációjú kulcsok teljesen meg is egyezhetnek, de három különböző hosszúságú, eltérő kulcsról is lehet szó (lásd: CSM_117).

▼B

12.3. **Járműegység és mozgásérzékelő közötti párosítás és kommunikáció AES használatával**

CSM_218 Ahogy a 3. táblázat tartalmából látható (9.2.1. szakasz), a (második generációs) járműegység és a mozgásérzékelő párosításában és az ezt követő kommunikációs műveletekben szereplő összes kulcs AES-kulcs, nem pedig az ISO 16844-3. sz. szabvány által előírt dupla hosszúságú TDES-kulcs. Ezen AES-kulcsok hosszúsága 128, 192 vagy 256 bit lehet. Mivel az AES blokkmérete 16 bájt, a titkosított üzenetek hossza a 16 bájt többszöröse, szemben a TDES-nél alkalmazott 8 bájttal. Emellett ezek az üzenetek adott esetben AES-kulcsok átadását is végzik, amelyeknek hossza 128, 192 vagy 256 bit lehet. Ezért az ISO 16844-3. sz. szabvány 5. táblázatában szereplő utasításonkénti adatbájtok számát a 6. táblázat értékeinek megfelelően módosítani kell:

6. táblázat

Egyszerű szöveges és titkosított adatbájtok száma utasításonként az ISO 16844-3. sz. szabvány meghatározása szerint

Utasítás	Kérés / válasz	Adatok leírása	Egyszerű szöveges adatbájtok száma az ISO 16844-3. sz. szabvány szerint	Egyszerű szöveges adatbájtok száma AES-kulcsok használatával	Egyszerű szöveges adatbájtok száma az alábbi hosszúságú (bitszámú) AES-kulcsok használatakor		
					128	192	256
10	kérés	Hitelesítési adatok + fájlszám	8	8	16	16	16
11	válasz	Hitelesítési adatok + fájltartalom	16 vagy 32, fájltól függ	16 vagy 32, fájltól függ	16 / 32	16 / 32	16 / 32
41	kérés	MoS sorozatszám	8	8	16	16	16
41	válasz	Párosítási kulcs	16	16 / 24 / 32	16	32	32
42	kérés	Munkamenetkulcs	16	16 / 24 / 32	16	32	32
43	kérés	Párosítási adatok	24	24	32	32	32
50	válasz	Párosítási adatok	24	24	32	32	32
70	kérés	Hitelesítési adatok	8	8	16	16	16
80	válasz	MoS számlálóérték + hitelesítési adatok	8	8	16	16	16

CSM_219 A ‘43’ (járműegység kérése) és ‘50’ (MoS válasza) utasításokban küldött párosítási információk összeállítása az ISO 16844-3. sz. szabvány 7.6.10. szakasza szerint zajlik, azzal az eltéréssel, hogy a TDES helyett az AES algoritmust alkalmazzák a párosítási adatok titkosításához, ami két AES-titkosítást eredményez, valamint a CSM_220 szerinti kitöltést használják az AES-blokkmérethez való igazodás érdekében. A titkosításhoz használt K'_P kulcs létrehozása a következőképpen zajlik:

— Ha a K_P párosítási kulcs 16 bájt hosszúságú: $K'_P = K_P \text{ XOR } (N_s||N_s)$

▼B

— Ha a K_P párosítási kulcs 24 bájt hosszúságú: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$

— Ha a K_P párosítási kulcs 32 bájt hosszúságú: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$

ahol az N_s a mozgásérzékelő 8 bájtos sorozatszáma.

CSM_220 Ha az egyszerű szöveges adatok hossza (AES-kulcsok használatával) nem 16 bájt többszöröse, akkor az ISO 9797-1. sz. szabványban meghatározott 2. kitöltési módszert kell alkalmazni.

Megjegyzés: az ISO 16844-3. sz. szabványban az egyszerű szöveges adatbájtok száma mindig a 8 többszöröse, így a TDES használatakor nincs szükség kitöltésre. Az ISO 16844-3. sz. szabványban szereplő adat- és üzenetdefiníciókat a függelék e része nem módosítja, ezért kitöltés alkalmazására van szükség.

CSM_221 A ‘11’ utasításnál és akkor, ha egynél több adatblokk titkosítására van szükség, az ISO 10116. sz. szabványban előírt, titkosított blokkok láncolatán alapuló üzemmódot kell használni, *m* = 1 kihagyási paraméterrel. Az alkalmazandó IV:

— A ‘11’ utasításhoz: az ISO 16844-3. sz. szabvány 7.6.3.3. szakaszában meghatározott 8 bájtos hitelesítési blokk, az ISO 9797-1. sz. szabvány szerinti 2. kitöltési módszerrel kitöltve; lásd még az ISO 16844-3. sz. szabvány 7.6.5. és 7.6.6. szakaszát.

— Minden más utasításhoz, amelyben 16 bájtnál több adat átvitelére kerül sor, a 6. táblázat szerint: ‘00’ {16}, azaz tizenhat bájt 0 bináris értékkel.

Megjegyzés: az ISO 16844-3. sz. szabvány 7.6.5. és 7.6.6. szakaszának megfelelően, ha az MoS titkosítja az adatfájlokat a ‘11’ utasításba való befoglaláshoz, a hitelesítési blokk:

— egyrészt az adatfájlok CBC-üzemmódú titkosításának inicializálási vektoraként szolgál;

— másrészt titkosítva szerepel a járműegységnek küldött adatok első blokkjában.

12.4. **Járműegység és mozgásérzékelő párosítása különböző készülékgenerációk esetében**

CSM_222 A 9.2.1. szakaszban leírtaknak megfelelően a második generációs mozgásérzékelő tartalmazhatja a párosítási adatok TDES-alapú titkosítását (lásd e függelék A. részét), amely lehetővé teszi a mozgásérzékelő első generációs járműegységgel történő párosítását. Ilyen esetben az első generációs járműegységet és a mozgásérzékelőt az e függelék A. részében és az ISO 16844-3. sz. szabványban leírtak szerint kell párosítani. A párosításhoz első vagy második generációs műhelykártya is használható.

Megjegyzések:

— második generációs járműegységet nem lehet párosítani első generációs mozgásérzékelővel.

▼B

— Első generációs műhelykártyával nem lehet második generációs járműegységet mozgásérzékelőhöz kapcsolni.

13. A DSRC-n KERESZTÜLI TÁVOLI KOMMUNIKÁCIÓ BIZTONSÁGA

13.1. **Általános tudnivalók**

A 14. függelékben leírtaknak megfelelően a járműegység rendszeresen létrehozza a távoli tachográf-megfigyelési (RTM) adatokat, és elküldi ezeket a (belső vagy külső) távoli kommunikációs egység (RCF) számára. A távoli kommunikációs egység feladata, hogy ezeket az adatokat a 14. függelékben leírt DSRC-interfészen keresztül továbbküldje a távoli lekérdezőegység számára. Az 1. függelékben leírtaknak megfelelően az RTM-adatoknak a következők konkatenációjából kell állniuk:

Titkosított tachográfterhelés az egyszerű szöveges tachográf-terhelési érték titkosítva

DSRC biztonsági adatok leírásukat lásd lent

Az egyszerű szöveges tachográf-terhelési adatok formátumát az 1. és a 14. függelék ismerteti. Ebben a szakaszban a DSRC biztonsági adatok struktúráját mutatjuk be; a formális definíció az 1. függelékben található.

CSM_223 Az egyszerű szöveges `tachographPayload` adatokat – amelyeket a járműegység a távoli kommunikációs egységnek (külső RCF esetében), illetve a DSRC interfészen keresztül a távoli lekérdezőegységnek (belső RCF esetében) küld el – „titkosítás, majd hitelesítés” üzemmóddal kell védeni, azaz a tachográf-terhelési adatokat először titkosítani kell az üzenet titkosságának biztosítása érdekében, majd ezt követően ki kell számítani az adatok hitelességét és integritását garantáló MAC értékét.

CSM_224 A DSRC biztonsági adatoknak a következő adatelemek alábbi sorrendben való konkatenációjából kell állniuk(lásd még: 12. ábra):

Aktuális dátum és idő	a járműegység aktuális dátuma és ideje (`TimeReal` adattípus)
Számláló	3 bájtos számláló, lásd: CSM_225
Járműegység sorozatszáma	a járműegység sorozatszáma (`VuSerialNumber` adattípus)
DSRC-mesterkulcs verziószáma	annak a DSRC-mesterkulcsnak az 1 bájtos verziószáma, amelyből a járműegység-specifikus DSRC-kulcsokat származtatták; lásd a 9.2.2. szakaszt.
MAC	Az RTM-adatok összes megelőző bájtjából kiszámított MAC értéke.

CSM_225 A DSRC biztonsági adatok 3 bájtos számlálója olyan formátumú, amelyben a legjelentősebb bit kerül előre. Amikor egy járműegység az üzembe állítását követően első alkalommal számít ki RTM-adatokat, a számláló értékét 0-ra kell állítania. A járműegységnek minden alkalommal, amikor új RTM-adatkészletet számít ki, eggyel növelnie kell a számláló értékét.

▼B

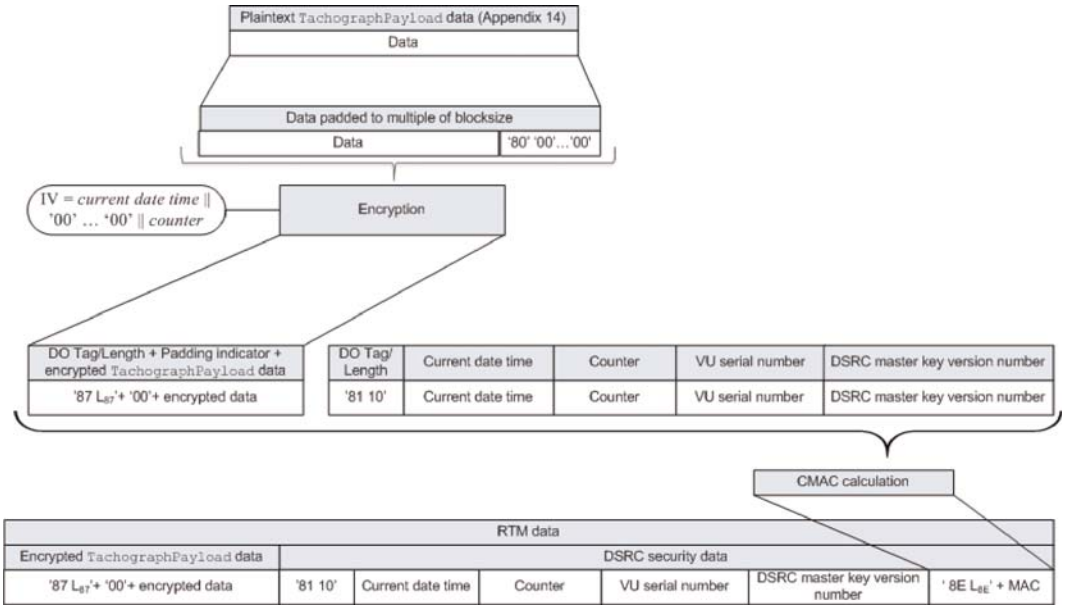
13.2. **A tachográfterhelés titkosítása és a MAC létrehozása**

CSM_226 A 14. függelékben leírt egyszerű szöveges `TachographPayload` adatelem esetében a járműegység a 12. ábra szerint végzi az adatok titkosítását: a járműegység $K_VU_{DSRC}_ENC$ titkosítási DSRC-kulcsát (lásd: 9.2.2. szakasz) titkosított blokkok láncolatán (CBC) alapuló üzemmódú AES algoritmussal együtt alkalmazza, az ISO 10116 sz. szabványban leírtaknak megfelelően, m = 1 kihagyási paraméterrel. Az inicializációs vektor *IV = aktuális dátum és időpont || 00 00 00 00 00 00 00 00 || számláló*, ahol az *aktuális dátum és időpont* és a *számláló* értékei a CSM_224 szerint alakul. A titkosítandó adatok esetében az ISO 9797-1. sz. szabvány 2. módszere szerinti kitöltést alkalmazzák.

CSM_227 A járműegységnek a DSRC biztonsági adatok MAC-értékét a 12. ábra szerint kell kiszámítania: a MAC értékének kiszámításához az RTM-adatok összes megelőző bájtját fel kell használni, egészen a DSRC-mesterkulcs verziószámáig (ezt az adatot is beleértve), valamint a címkéket és az adatobjektumok hosszát is felhasználva a számítás során. A járműegységnek a saját DSRC-kulcsát, azaz a $K_VU_{DSRC}_MAC$ kulcsot kell használnia a hitelesség biztosításához (lásd: 9.2.2. szakasz), CMAC üzemmódú AES algoritmus alkalmazásával (lásd: [SP 800-38B]). A MAC hossza a járműegység-specifikus DSRC-kulcsok hosszához van kötve, a CSM_50 előírásainak megfelelően.

12. ábra

A tachográfterhelés titkosítása és a MAC létrehozása



13.3. **A tachográfterhelés ellenőrzése és visszafejtése**

CSM_228 Amikor egy távoli lekérdezőegység RTM-adatokat fogad egy járműegységtől, az összes RTM-adatot el kell küldenie egy ellenőrzőkártya számára a PROCESS DSRC MESSAGE parancs adatmezőjében, a 2. függelékben leírtaknak megfelelően. Ezután:

▼B

1. Az ellenőrzőkártyának meg kell vizsgálnia a DSRC-mesterkulcs verziószámát a DSRC biztonsági adatokban. Ha az ellenőrzőkártya nem ismeri a feltüntetett DSRC-mesterkulcsot, a 2. függelékben meghatározott hibát kell visszaküldenie, és meg kell szakítania a folyamatot.

2. Az ellenőrzőkártyának a feltüntetett DSRC-mesterkulcsot a DSRC biztonsági adatokban szereplő járműegység-sorozatszámmal együtt kell használnia a járműegység-specifikus $K_VU_{DSRC}_ENC$ és $K_VU_{DSRC}_MAC$ DSRC-kulcsok származtatásához, a CSM_124 szerint.

3. Az ellenőrzőkártyának a $K_VU_{DSRC}_MAC$ kulcs használatával kell ellenőriznie a MAC értékét a DSRC biztonsági adatokban, a CSM_227 szerint. Ha a MAC nem megfelelő, az ellenőrzőkártyának a 2. függelékben meghatározott hibát kell visszaküldenie és meg kell szakítania a folyamatot.

4. Az ellenőrzőkártyának a $K_VU_{DSRC}_ENC$ kulcs használatával kell visszafejtenie a titkosított tachográfterhelést, a CSM_226 szerint. Az ellenőrzőkártyának el kell távolítania a kitöltést, és vissza kell küldenie a visszafejtett tachográf-terhelési adatokat a távoli lekérdezőegységnek.

CSM_229 Az ismétléses támadások megelőzése érdekében a távoli lekérdezőegységnek meg kell vizsgálnia az RTM-adatok aktualitását: ellenőriznie kell, hogy a DSRC biztonsági adatokban szereplő *aktuális dátum és időpont* nem tér-e el túlzottan a távoli lekérdezőegység aktuális időpontjától.

Megjegyzések:

— Ehhez az szükséges, hogy a távoli lekérdezőegység pontos és megbízható időforrással rendelkezzen.

— Mivel a 14. függelék értelmében a járműegységnek 60 másodpercenként új RTM-adatkészletet kell kiszámítania, és a járműegység órája 1 perccel eltérhet a valós időtől, az RTM-adatok aktualitásának alsó határa 2 perc. A ténylegesen előírt aktualitás a távoli lekérdezőegység órájának pontosságától is függ.

CSM_230 Amikor egy műhely ellenőrzi a járműegység DSRC-funkcióinak megfelelő működését, a járműegységtől kapott összes RTM-adatot el kell küldenie egy műhelykártya számára a PROCESS DSRC MESSAGE parancs adatmezőjében, a 2. függelékben leírtaknak megfelelően. A műhelykártyának el kell végeznie a CSM_228 szerinti összes ellenőrzést és műveletet.

14. AZ ADATLETÖLTÉSEK ALÁÍRÁSA ÉS AZ ALÁÍRÁSOK ELLENŐRZÉSE

14.1. **Általános tudnivalók**

CSM_231 Az intelligens kijelölt berendezésnek (IDE) egyetlen fizikai adatállományon belül kell tárolnia a járműegységről vagy kártyáról egy letöltési munkamenetben letöltött adatokat. Az adatok tárolása külső tárolóeszközön (ESM) történhet. Ez a fájl tartalmazza az adattömböknek a 7. függelékben meghatározott digitális aláírásait. A fájlnak a következő tanúsítványokat is tartalmaznia kell (lásd a 9.1. szakaszt):

▼B

— Járműegységről történő letöltés esetén:

— A VU_Sign tanúsítványt.

— A VU_Sign tanúsítvány ellenőrzésére szolgáló nyilvános kulcsot tartalmazó MSCA_VU-EGF tanúsítványt.

— Kártyáról történő letöltés esetén:

— A Card_Sign tanúsítványt.

— A Card_Sign tanúsítvány ellenőrzésére szolgáló nyilvános kulcsot tartalmazó MSCA_Card tanúsítványt.

CSM_232 Az IDE-nek az alábbiakkal is rendelkeznie kell:

— Amennyiben ellenőrzőkártyát használ az aláírás ellenőrzéséhez, a 13. ábra szerint: Azt a hivatkozási tanúsítványt, amely a legújabb EUR-tanúsítványt az azt közvetlenül megelőző érvényességi időszakkal rendelkező EUR-tanúsítványhoz kapcsolja.

— Amennyiben az aláírást maga ellenőrzi: az összes érvényes európai gyökértanúsítványt.

Megjegyzés: az IDE által a tanúsítványok beolvasásához használt módszer ebben a függelékben nincs meghatározva.

14.2. **Aláírások generálása**

CSM_233 A digitális aláírások létrehozásához az ECDSA aláírási algoritmust alkalmazzák (a meghatározást lásd: [DSS]), a járműegység vagy a kártya kulcsméretéhez kötött hasító algoritmussal (lásd: CSM_50). Az aláírás egyszerű formátumú (lásd: [TR-03111]).

14.3. **Aláírások ellenőrzése**

CSM_234 Az IDE a letöltött adatokon maga is elvégezheti az aláírás ellenőrzését, vagy ellenőrzőkártyát is használhat erre a célra. Amennyiben ellenőrzőkártyát használ, az aláírás ellenőrzésének a 13. ábra szerint kell történnie: Ha saját maga végzi az aláírás ellenőrzését, az IDE-nek meg kell vizsgálnia az adatfájlban lévő tanúsítványláncolat összes tanúsítványának hitelességét és érvényességét, az aláírás adatoknak való megfelelését pedig a [DSS] szerinti aláírási rendszer használatával kell ellenőriznie.

Megjegyzések a 13. ábra tartalmához:

— EQT jelöli azt a készüléket, amely aláírta az elemzendő adatokat.

— Az ábrán szereplő EQT-tanúsítványok és nyilvános kulcsok azok, amelyeket az aláíráshoz használnak (VU_Sign vagy Card_Sign).

— Az ábrán szereplő EQT.CA tanúsítványok és nyilvános kulcsok azok, amelyeket a járműegységek, illetve a kártyák tanúsítványainak aláírásához használnak.

— Az ábrán szereplő EQT.CA.EUR tanúsítvány az az európai gyökértanúsítvány, amely az EQT.CA tanúsítvány CAR-elemében van feltüntetve.

▼B

— Az ábrán szereplő EQT.Link tanúsítvány az EQT hivatkozási tanúsítványa, ha van ilyen. A 9.1.2. szakaszban foglaltaknak megfelelően ez az ERCA által létrehozott és az előző európai privát kulccsal aláírt új európai gyökérkulcspár hivatkozási tanúsítványa.

— Az EQT.Link.EUR tanúsítvány az az európai gyökértanúsítvány, amely az EQT.Link tanúsítvány CAR-elemében van feltüntetve.

CSM_235 A PSO:Hash parancsban az ellenőrzőkártyának küldött M hasítás kiszámításához az IDE-nek az adatletöltés forrásául szolgáló járműegység vagy kártya kulcsméretének megfelelő hasító algoritmust kell használnia (lásd: CSM_50).

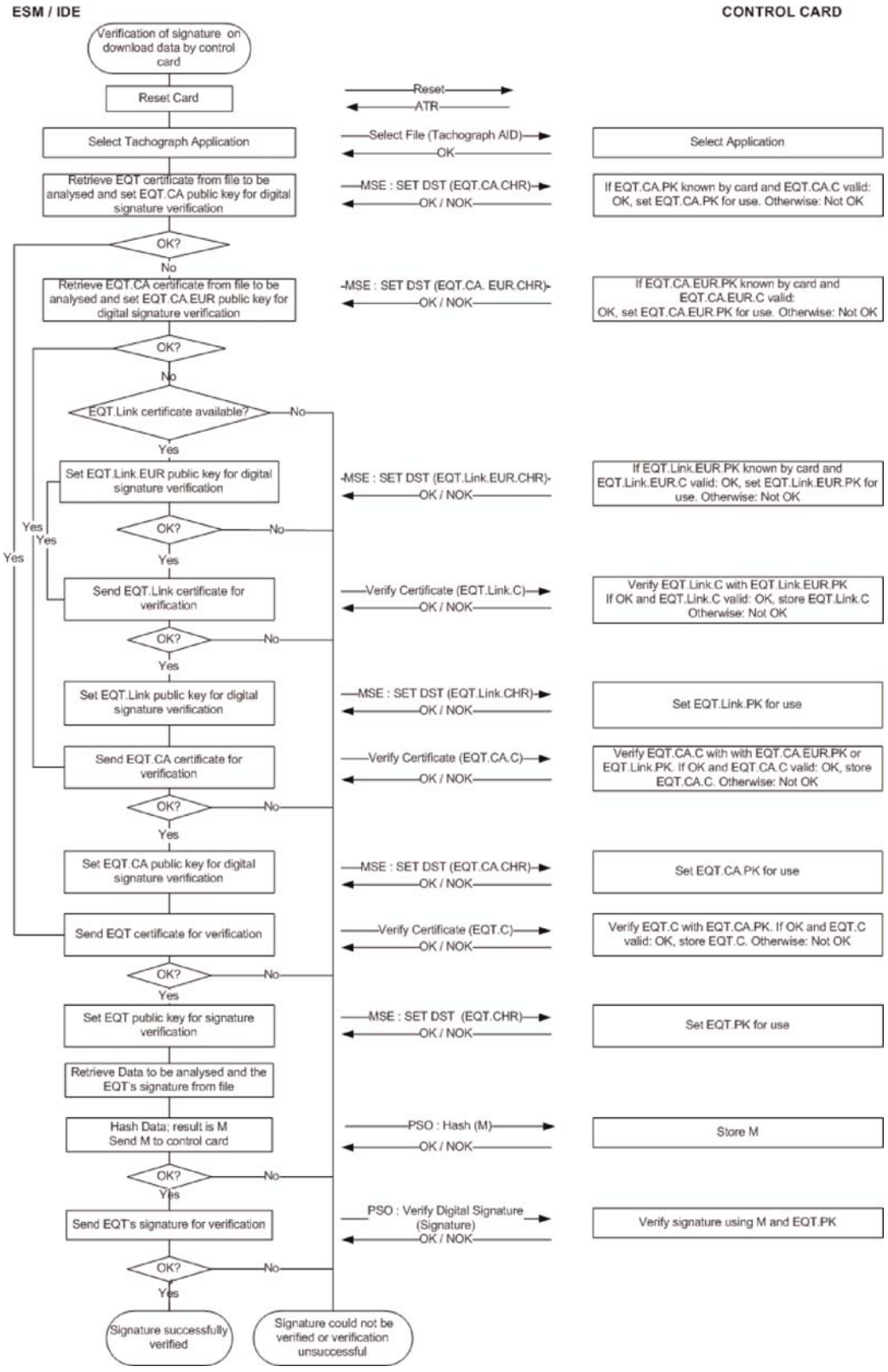
CSM_236 Az EQT aláírásának ellenőrzéséhez az ellenőrzőkártyának a [DSS] szerinti aláírási rendszert kell használnia.

Megjegyzés: ez a dokumentum nem ír elő semmilyen műveletet arra az esetre, ha a letöltött adatfájl aláírása nem ellenőrizhető vagy az ellenőrzés sikertelen.

▼B

13. ábra

Letöltött adatfájl aláírásának ellenőrzési protokollja



▼B

12. függelék

A GLOBÁLIS NAVIGÁCIÓS MŰHOLDRENDSZEREN (GNSS-RENDSZEREN) ALAPULÓ HELYZETMEGHATÁROZÁS

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. Hatály

1.2. Rövidítések és jelentésük

2. A GNSS-VEVŐRE VONATKOZÓ ELŐÍRÁSOK

3. NMEA-ADATMONDATOK

4. KÜLSŐ GNSS-ESZKÖZZEL RENDELKEZŐ JÁRMŰEGYSÉG

4.1. Konfiguráció

4.1.1 Fő alkotóelemek és interfészek

4.1.2 A külső GNSS-eszköz jellemzői a gyártási folyamat végén

4.2. Kommunikáció a külső GNSS-eszköz és a járműegység között

4.2.1 Kommunikációs protokoll

4.2.2 A GNSS-adatok biztonságos továbbítása

4.2.3 A Read Record parancs szerkezete

4.3. A külső GNSS-eszköz és a járműegység összekapcsolása, kölcsönös hitelesítése és műveletkulcs-egyeztetése

4.4. Hibakezelés

4.4.1 Kommunikációs hiba a külső GNSS-eszközzel

4.4.2 A külső GNSS-eszköz fizikai épségének megsértése

4.4.3 A GNSS-vevőből származó helyzetmeghatározási információk hiánya

4.4.4 A külső GNSS-eszköz tanúsítványa lejárt

5. KÜLSŐ GNSS-ESZKÖZ NÉLKÜLI JÁRMŰEGYSÉG

5.1. Konfiguráció

5.2. Hibakezelés

5.2.1 A GNSS-vevőből származó helyzetmeghatározási információk hiánya

6. A GNSS IDŐÜTKÖZÉSE

7. A JÁRMŰ MOZGÁSÁVAL KAPCSOLATOS ELLENTMONDÁS

1. BEVEZETÉS

Ez a függelék a járműegység által használt GNSS-adatokra vonatkozó műszaki követelményeket határozza meg, beleértve a helyzetmeghatározási információk biztonságos és megfelelő adatátviteléhez szükséges protokollokat is.

E követelmények alapját a 165/2014/EU rendelet következő cikkei képezik: 8. cikk: A jármű helyzetének rögzítése bizonyos pontokon a napi munkaidő során, 10. cikk: A menetíró készülékeket és az intelligens közlekedési rendszereket összekapcsoló interfész, 11. cikk: Az intelligens menetíró készülékre vonatkozó részletes rendelkezések.

▼B

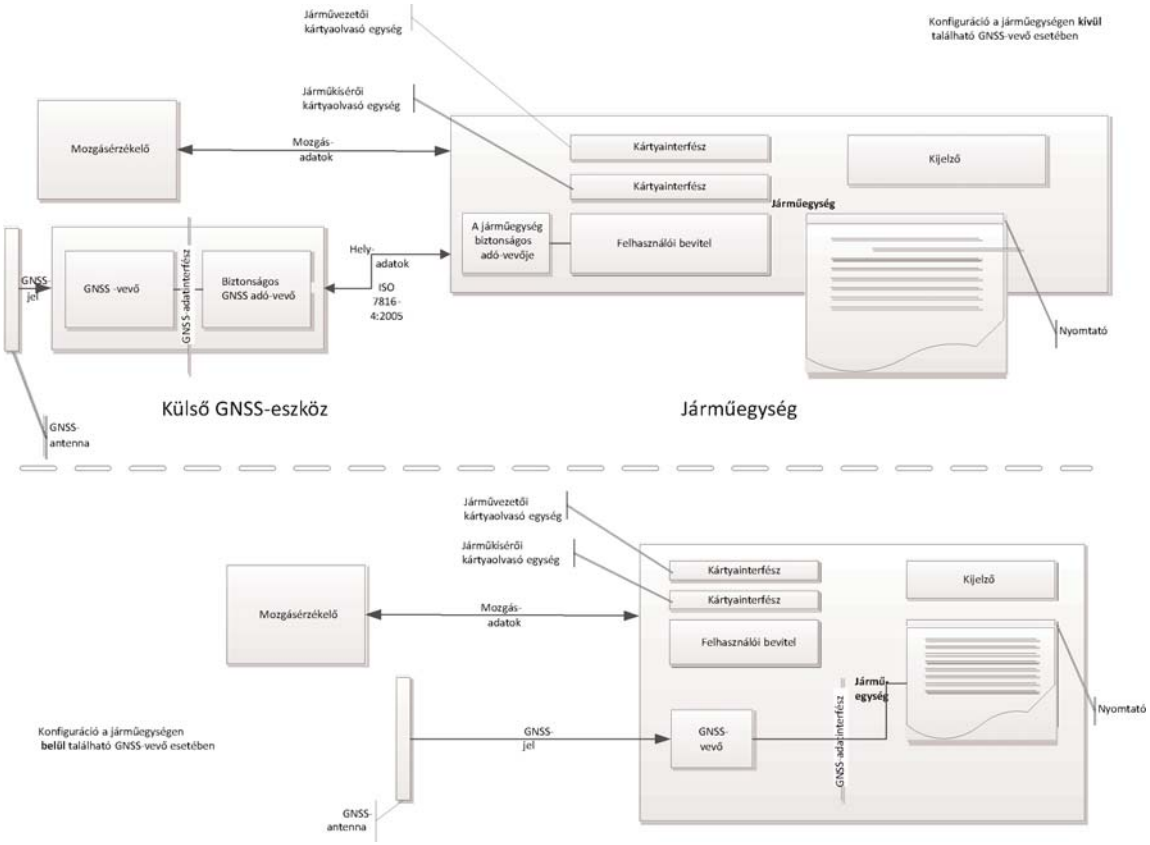
1.1. **Hatály**

GNS_1 A 8. cikk végrehajtásának elősegítése érdekében a járműegységnek legalább egy GNSS-rendszerből helymeghatározási adatokat kell gyűjtenie.

A járműegységek lehetnek GNSS-eszközzel felszereltek vagy GNSS-eszköz nélküliek, mint az az 1. ábrán látható:

1. ábra

A GNSS-vevő különféle konfigurációi



1.2. **Rövidítések és jelentésük**

E függelék a következő rövidítéseket használja:

DOP	Dilution of Precision – Pontossághígulás
EGF	Elementary file GNSS Facility – A GNSS-eszköz elemi fájlja
EGNOS	European Geostationary Navigation Overlay Service – Európai geostacionárius navigációs lefedési szolgáltatás
GNSS	Global Navigation Satellite System – Globális navigációs műholdrendszer
GSA	GPS DOP and active satellites – GPS DOP és aktív műholdak
HDOP	Horizontal Dilution of Precision – Vízszintes pontossághígulás
ICD	Interface Control Document – Interfészvezérlési dokumentáció
NMEA	National Marine Electronics Association – Az USA nemzeti tengerészeti elektronikai szervezete

▼B

PDOP Position Dilution of Precision – Helyzeti pontossághígulás

RMC Recommended Minimum Specific – Ajánlott minimális jellemző

SIS Signal in Space – Űrjel

VDOP Vertical Dilution of Precision – Függőleges pontossághígulás

VU Vehicle Unit – Járműegység

2. A GNSS-VEVŐRE VONATKOZÓ ELŐÍRÁSOK

Függetlenül attól, hogy az intelligens menetíró készülék a konfigurációja szerint rendelkezik-e külső GNSS-eszközzel, az intelligens menetíró készülékek hatékony működésének elengedhetetlen eleme a helyzetmeghatározási információk pontos és megbízható szolgáltatása. Ezért helyénvaló előírni, hogy a készülék kompatibilis legyen az 1285/2013/EU európai parlamenti és tanácsi rendeletben [1] meghatározott Galileo-program és az európai geostacionárius navigációs lefedési szolgáltatás (EGNOS) elnevezésű program keretében nyújtott szolgáltatásokkal. A Galileo program alapján létrehozott rendszer egy független globális műholdas navigációs rendszer, az EGNOS program alapján létrehozott rendszer pedig egy regionális műholdas navigációs rendszer, amely javítja a globális helyzetmeghatározó rendszer jeleinek minőségét.

GNS_2 A gyártóknak gondoskodniuk kell arról, hogy az intelligens menetíró készülékekben található GNSS-vevők kompatibilisek legyenek a Galileo és az EGNOS rendszer nyújtotta helyzetmeghatározási szolgáltatásokkal. A gyártók emellett dönthetnek az egyéb műholdas navigációs rendszerekkel való kompatibilitásról is.

GNS_3 A GNSS-vevőnek alkalmasnak kell lennie arra, hogy támogassa a Galileo nyílt szolgáltatásán történő hitelesítést, ha a Galileo ilyen szolgáltatást fog nyújtani és a GNSS-vevők gyártói támogatni fogják ezt a szolgáltatást. A korábbi feltételek teljesülése előtt piacra kerülő és a Galileo nyílt szolgáltatásán történő hitelesítést nem támogató intelligens menetíró készülékek esetében azonban nem lesz kötelező az utólagos átalakítás.

3. NMEA-ADATMONDATOK

Ez a rész az intelligens menetíró készülékek működéséhez szükséges NMEA-adatmondatokat ismerteti. A leírás a külső GNSS-eszközzel rendelkező és az anélküli intelligens menetíró készülékekre is érvényes.

GNS_4 A helymeghatározási adatok alapja az Ajánlott minimális specifikusság (RMC) NMEA-adatmondat, amely tartalmazza a helyzetre vonatkozó (szélességi, hosszúsági) adatokat, az UTC formátumú időt (hhmmss.ss), a csomóban megadott, földhöz viszonyított sebességet és egyéb kiegészítő értékeket.

Az RMC adatmondat formátuma a következő (az NMEA V4.1 szabvány alapján):

[1] Az Európai Parlament és a Tanács 2013. december 11-i 1285/2013/EU rendelete az európai műholdas navigációs rendszerek létrehozásáról és üzemeltetéséről, valamint a 876/2002/EK tanácsi rendelet és a 683/2008/EK európai parlamenti és tanácsi rendelet hatályon kívül helyezéséről (HL L 347., 2013.12.20., 1. o.).

▼B

2. ábra

Az RMC adatmondat formátuma



1) Idő (UTC)
2) Állapot, A = Érvényes helyzet, V = Figyelmeztetés
3) Szélesség
4) É vagy D
5) Hosszúság
6) K vagy Ny
7) Földhöz viszonyított sebesség csomóban
8) Valódi útirány
9) Dátum (nnhhéé)
10) Mágneses eltérés fokban
11) K vagy Ny
12) Ellenőrző összeg

Az állapot azt adja meg, hogy rendelkezésre áll-e a GNSS-jel. Amíg az állapot értéke A-ra nem változik, a fogadott adatok (pl. az idő vagy a szélesség/hosszúság) nem használhatók a jármű helyzetének a járműegységben való rögzítésére.

A helyzet felbontása a fent bemutatott RMC adatmondat szerkezetén alapszik. A 3. és 5. mező első része (első két számjegye) jelöli a fokokat. A mezők többi része a perceket adja meg három tizedesjegy pontossággal. Így a felbontás a következő: a perc 1/1000-ed része vagy a fok 1/60000-ed része (mivel egy perc egy foknak az 1/60-ad része).

GNS_5 A járműegységnek a szélességre és a hosszúságra vonatkozó helyzetmeghatározási adatokat a perc 1/10-ed részének vagy a fok 1/600-ad részének megfelelő felbontással kell eltárolnia a járműegység adatbázisában, az 1. függelékben a földrajzi koordinátákra vonatkozóan meghatározott előírásoknak megfelelően.

A GPS DOP és aktív műholdak (GSA) parancsot a jel rendelkezésre állásának és pontosságának meghatározására és rögzítésére használhatja a járműegység. A HDOP konkrétan a rögzített helymeghatározási adatok pontossági szintjének jelzésére szolgál (lásd a 4.2.2. pontot). A járműegységnek el kell tárolnia a vízszintes pontossághígulás (HDOP) értékét, amelyet a rendelkezésre álló GNSS-rendszer által begyűjtött HDOP-értékek minimumaként számítanak ki.

A GNSS-rendszer azonosítója jelzi, hogy a GPS, a Glonass, a Galileo, a Beidou vagy a műholdas pontosító rendszerről (SBAS) van-e szó.

3. ábra

A GSA adatmondat formátuma



1) Kiválasztási mód
2) Mód
3) A meghatározáshoz használt 1. műhold azonosítója
4) A meghatározáshoz használt 2. műhold azonosítója
...
14) A meghatározáshoz használt 12. műhold azonosítója
15) A PDOP méterben
16) A HDOP méterben
17) A VDOP méterben
18) A GNSS-rendszer azonosítója
19) Ellenőrző összeg

▼B

A mód (2) jelentheti azt, hogy nem áll rendelkezésre meghatározás (Mód=1), vagy azt, hogy kétdimenziós (Mód=2), illetve háromdimenziós (Mód=3) meghatározás áll rendelkezésre.

GNS_6 A GSA adatmondatot ‘06’ rekordszámmal kell eltárolni.

GNS_7 A rekord olvasása parancs méretezéséhez használt NMEA-adatmondatok (pl. RMS, GSA vagy egyéb) maximális mérete 85 bájt lehet (lásd: 1. táblázat).

4. KÜLSŐ GNSS-ESZKÖZZEL RENDELKEZŐ JÁRMŰEGYSÉG

4.1. **Konfiguráció**

4.1.1 *Fő alkotóelemek és interfészek*

Ebben a konfigurációban a GNSS-vevő a külső GNSS-eszköz részét képezi.

GNS_8 A külső GNSS-eszköznek specifikus járműinterfésszel kell rendelkeznie.

GNS_9 A külső GNSS-eszköznek a következő alkotóelemekből kell állnia (lásd: 4. ábra):

a) Egy kereskedelmi forgalomban kapható GNSS-vevő a helyzetmeghatározási adatoknak a GNSS-adatinterfészen keresztül történő szolgáltatásához. A GNSS-adatinterfész lehet például az NMEA V4.10 szabvány szerinti, ebben az esetben a GNSS-vevő adóként funkcionál, és 1 Hz-es frekvenciával továbbítja az NMEA-adatmondatokat a biztonságos GNSS adó-vevőnek az előre meghatározott NMEA-adatmondatok vonatkozásában, amelyeknek legalább az RMC és a GSA adatmondatokat magukban kell foglalniuk. A GNSS-adatinterfész megvalósításának mikéntjéről a külső GNSS-eszköz gyártója dönthet.

b) Az ISO/IEC 7816-4:2013 szabványt (lásd: 4.2.1) támogató adó-vevő egység (biztonságos GNSS adó-vevő), amely a járműegységgel való kommunikációra szolgál, és amely támogatja a GNSS-vevőhöz tartozó GNSS-adatinterfészt. Az egységnek rendelkeznie kell memóriával, hogy el tudja tárolni a GNSS-vevő és a külső GNSS-eszköz azonosítási adatait.

c) Manipulálásészlelő funkcióval ellátott burkolatrendszer, amely magában foglalja a GNSS-vevőt és a biztonságos GNSS adó-vevőt. A manipulálásészlelésnek az intelligens menetíró készülék védelmi profiljában előírt biztonsági és védelmi funkciókat kell ellátnia.

d) A járműre szerelt és a burkolatrendszeren keresztül a GNSS-vevőhöz kapcsolódó GNSS-antenna.

GNS_10 A külső GNSS-eszköznek legalább a következő külső interfészekkel kell rendelkeznie:

a) külső antenna használata esetén a járműre szerelt GNSS-antennához tartozó interfész;

b) a járműegységhez kapcsolódó interfész.

GNS_11 A járműegységben a biztonságos GNSS adó-vevővel zajló biztonságos kommunikáció másik végpontját a járműegység biztonságos adó-vevője alkotja, melynek támogatnia kell az ISO/IEC 7816-4:2013 szabványt a külső GNSS-eszközhöz való kapcsolódás tekintetében.

▼B

GNS_12 A külső GNSS-eszközzel való kommunikáció fizikai rétege tekintetében a járműegységnek támogatnia kell az ISO/IEC 7816-12:2005 szabványt vagy az ISO/IEC 7816-4:2013 szabvány támogatására alkalmas egyéb szabványt (lásd: 4.2.1).

4.1.2 *A külső GNSS-eszköz jellemzői a gyártási folyamat végén*

GNS_13 A gyárból kikerülő külső GNSS-eszköznek a következő értékeket kell tárolnia a biztonságos GNSS adó-vevő nem felejtő memóriájában:

— az EGF_MA kulcspár és a megfelelő tanúsítvány;

— az EGF_MA tanúsítvány hitelesítéséhez használandó MSCA_VU-EGF.PK nyilvános kulcsot tartalmazó MSCA_VU-EGF tanúsítvány;

— az MSCA_VU-EGF tanúsítvány hitelesítéséhez használandó EUR.PK nyilvános kulcsot tartalmazó EUR tanúsítvány;

— az EUR tanúsítvány, ha van ilyen, amelynek érvényességi ideje közvetlenül megelőzi az MSCA_VU-EGF tanúsítvány hitelesítéséhez használt EUR tanúsítvány érvényességi idejét;

— a két EUR tanúsítvány, ha vannak ilyenek, összekapcsolásához szükséges kapcsolattanúsítvány;

— a külső GNSS-eszköz bővített sorozatszáma;

— a GNSS-eszköz operációs rendszerének azonosítója;

— a külső GNSS-eszköz típus-jóváhagyási száma;

— a külső GNSS-eszköz biztonsági alkatrészének azonosítója.

4.2. **Kommunikáció a külső GNSS-eszköz és a járműegység között**

4.2.1 *Kommunikációs protokoll*

GNS_14 A külső GNSS-eszköz és a járműegység közötti kommunikációs protokollnak a következő három funkciót kell támogatnia:

1. a GNSS-adatok (pl. helyzet, idő, sebesség) összegyűjtése és szétosztása;

2. a külső GNSS-eszköz konfigurációs adatainak összegyűjtése;

3. a külső GNSS-eszköz és a járműegység összekapcsolásának, kölcsönös hitelesítésének és műveletkulcs-egyeztetésének támogatására szolgáló kezelési protokoll.

GNS_15 A kommunikációs protokollnak az ISO/IEC 7816-4:2013 szabványon kell alapulnia, és a járműegység biztonságos adó-vevőjének kell betöltenie a mester, a biztonságos GNSS adó-vevőnek pedig a szolga szerepet. A külső GNSS-eszköz és a járműegység közötti fizikai kapcsolatnak az ISO/IEC 7816-12:2005 szabványon vagy az ISO/IEC 7816-4:2013 szabvány támogatására alkalmas egyéb szabványon kell alapulnia.

▼B

GNS_16 A kommunikációs protokollon belül a kiterjesztett hosszúságú mezők nem támogathatók.

GNS_17 A külső GNSS-eszköz és a járműegység közötti, ISO 7816 (*-4:2013 és *-12:2005) szabvány szerinti kommunikációs protokollt beállításának T=1-nek lennie.

GNS_18 A GNSS-adatok összegyűjtése és szétosztása (1.), a külső GNSS-eszköz konfigurációs adatainak összegyűjtése (2.) és a kezelési protokoll (3.) funkciók tekintetében a biztonságos GNSS adó-vevőnek olyan fájlrendszer-architektúrával rendelkező intelligens kártyát kell szimulálnia, amely egy törzsállományból (MF), egy, az 1. függelék 6.2. fejezetében meghatározott alkalmazásazonosítóval (‘FF 44 54 45 47 4D’) és 3, tanúsítványokat tartalmazó EF-fel rendelkező könyvtárfájlból (DF) és egyetlen, az 1. táblázatnak megfelelően ‘2F2F’ fájlazonosítóval rendelkező elemi fájlból (EF.EGF) áll.

GNS_19 A biztonságos GNSS adó-vevőnek a GNSS-vevőből érkező adatokat és a konfigurációt az EF.EGF fájlban kell tárolnia. Ez egy lineáris, változó hosszúságú rekordokat tartalmazó fájl, melynek azonosítója egyenlő a hexadecimális formátumú ‘2F2F’-vel.

GNS_20 A biztonságos GNSS adó-vevőnek az adatok tárolásához olyan memóriával kell rendelkeznie, amely képes legalább 20 millió írási/olvasási ciklus elvégzésére. E követelményen kívül a gyártók szabhatják meg a biztonságos GNSS adó-vevő belső kialakítását és működését.

A rekordszámok és az adatok megfeleltetése az 1. táblázatban található. Megjegyzendő, hogy a négy műholdas rendszerhez és a műholdas pontosító rendszerhez (SBAS) négy GSA adatmondat áll rendelkezésre.

GNS_21 A fájlszerkezet az 1. táblázatban van megadva. A hozzáférési feltételeket (ALW, NEV, SM-MAC) lásd a 2. függelék 3.5. fejezetében.

1. táblázat

Fájlszerkezet

		Hozzáférési feltételek		
Fájl	Fájlazonosító	Olvasás	Frissítés	Titkosított
MF	3F00			
EF.ICC	0002	ALW	NEV (a jármű-egység által)	Nem
A GNSS-eszköz DF-je	0501	ALW	NEV	Nem
EF EGF_MACertificate	C100	ALW	NEV	Nem
EF CA_Certificate	C108	ALW	NEV	Nem
EF Link_Certificate	C109	ALW	NEV	Nem
EF.EGF	2F2F	SM-MAC	NEV (a jármű-egység által)	Nem

▼B

Fájl/adatelem	Rekord száma	Méret (bájt)		Alapértelmezett értékek
		Min.	Max.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
A GNSS-eszköz DF-je		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC NMEA-adatmondat	‘01’	85	85	
Első GSA NMEA-adatmondat	‘02’	85	85	
Második GSA NMEA-adatmondat	‘03’	85	85	
Harmadik GSA NMEA-adatmondat	‘04’	85	85	
Negyedik GSA NMEA-adatmondat	‘05’	85	85	
Ötödik GSA NMEA-adatmondat	‘06’	85	85	
a külső GNSS-eszköz bővített sorozatszáma az 1. függelék meghatározása szerint (SensorGNSSSerialNumber)	‘07’	8	8	
a biztonságos GNSS adó-vevő operációs rendszerének azonosítója az 1. függelék meghatározása szerint (SensorOSIdentifier)	‘08’	2	2	
A külső GNSS-eszköz típus-jóváhagyási száma az 1. függelék meghatározása szerint (SensorExternalGNSSApprovalNumber)	‘09’	16	16	
A külső GNSS-eszköz biztonsági alkatrészének azonosítója az 1. függelék meghatározása szerint (SensorExternalGNSSSCIdentifier)	‘10’	8	8	
RFU – Későbbi használatra fenntartva	‘11’-től ‘FD’-ig			

4.2.2 *A GNSS-adatok biztonságos továbbítása*

GNS_22 A GNSS-helyzetmeghatározási adatok biztonságos továbbítására csak a következő feltételek teljesülése esetén kerülhet sor:

1. A csatlakoztatási eljárás a 11. függelékben (Közös biztonsági mechanizmusok) leírtak szerint lezárult.

▼B

2. A járműegység és a külső GNSS-eszköz időszakos kölcsönös hitelesítésének és műveletkulcs-egyeztetésének leírása szintén a 11. függelékben található. A közös biztonsági mechanizmusokat az előírt gyakorisággal végrehajtották.

GNS_23 Ha nem zajlik csatlakoztatás vagy kölcsönös hitelesítés vagy műveletkulcs-egyeztetés, minden T. másodpercben (ahol T kisebb vagy egyenlő 10-zel) a járműegység helyzetmeghatározási információkat kér a külső GNSS-eszköztől a következő eljárással:

1. A járműegység a helymeghatározási adatokat és ezzel együtt pontossághígulási adatokat kér a külső GNSS-eszköztől (a GSA NMEA-adatmondatból). A járműegység biztonságos adó-vevőjének az ISO/IEC 7816-4:2013 szabvány szerinti SELECT és READ RECORD(S) parancsokat kell használnia a biztonságos üzenetküldés csak hitelesítésre szolgáló módjában a 11. függelék 11.5. szakaszának megfelelően, ahol a fájlazonosító ‘2F2F’, és a rekord száma az RMC NMEA-adatmondat esetében ‘01’, a GSA NMEA-adatmondat esetében pedig ‘02’,‘03’,‘04’,‘05’,‘06’.

2. Az utoljára fogadott helymeghatározási adatok az EF-ben kerülnek tárolásra ‘2F2F’ azonosítóval, az 1. táblázatban leírt rekordok pedig a biztonságos GNSS adó-vevőben, miközben a biztonságos GNSS adó-vevő legalább 1 Hz-es frekvenciával fogad NMEA-adatokat a GNSS-vevőtől a GNSS-adatinterfészen keresztül.

3. A biztonságos GNSS adó-vevő az APDU válaszüzenet használatával válaszol a járműegység biztonságos adó-vevőjének a biztonságos üzenetküldés csak hitelesítésre szolgáló módjában a 11. függelék 11.5. szakaszának megfelelően.

4. A járműegység biztonságos adó-vevője ellenőrzi a kapott válasz hitelességét és sértetlenségét. Pozitív eredmény esetén a helymeghatározási adatok a GNSS-adatinterfészen keresztül átkerülnek a járműegység processzorába.

5. A járműegység processzora az információknak (pl. a szélességnek, a hosszúságnak, az időnek) az RMC NMEA-adatmondatból való kivonatolásával ellenőrzi a fogadott adatokat. Az RMC NMEA-adatmondat azt az információt is tartalmazza, hogy a helyzet érvényes-e. Ha a helyzet nem érvényes, a helymeghatározási adatok még nem állnak rendelkezésre és nem használhatók a jármű helyzetének rögzítéséhez. Ha a helyzet érvényes, a járműegység processzora a HDOP-értékeket is kivonatolja a GSA NMEA-adatmondatokból, és kiszámítja a rendelkezésre álló műholdas rendszerekre vonatkozó átlagos értéket (azaz abban az esetben, ha rendelkezésre áll a meghatározás).

6. A járműegység processzora az 1. függelék adatszótárában meghatározott formátumban, földrajzi koordinátákként tárolja a járműegységben a fogadott és feldolgozott információkat (pl. a szélességet, a hosszúságot, az időt és a sebességet) a rendelkezésre álló GNSS-rendszerekre vonatkozóan összegyűjtött HDOP-értékek minimumaként kiszámított HDOP-értékkel együtt.

▼B

4.2.3 *A Read Record parancs szerkezete*

Ez a szakasz a Read Record parancs szerkezetéről nyújt részletes tájékoztatást. A biztonságos üzenetküldés (csak hitelesítésre szolgáló mód) a 11. függelék (Közös biztonsági mechanizmusok) szerint hozzáadásra került.

GNS_24 A parancsnak támogatnia kell a biztonságos üzenetküldés csak hitelesítésre szolgáló módját (lásd a 11. függeléket).

GNS_25 Parancsüzenet

Bájt	Hossz	Érték	Leírás
CLA	1	‘0Ch’	Biztonságos üzenetküldés kérése
INS	1	‘B2h’	Rekord olvasása
P1	1	‘XXh’	Rekord száma (a 00 jelenti az aktuális rekordot)
P2	1	‘04h’	A P1-ben megadott számú rekord olvasása
Le	1	‘XXh’	A várt adat hossza. Az olvasandó bájtok száma.

GNS_26 A P1-ben hivatkozott rekord lesz az aktuális rekord.

Bájt	Hossz	Érték	Leírás
#1-#X	X	‘XX..XXh’	Kiolvasott adat
SW	2	‘XXXXh’	Állapotszavak (SW1, SW2)

— Ha a parancs sikeres, akkor a biztonságos GNSS adó-vevő a következőt küldi vissza: ‘**9000**’.

— Ha az adott fájl nem rekordorientált, akkor a biztonságos GNSS adó-vevő a következőt küldi vissza: ‘**6981**’.

— Ha a parancsot P1=‘00’ feltétel mellett használják, de nem áll rendelkezésre aktuális EF, a biztonságos GNSS adó-vevő a következőt küldi vissza: ‘**6986**’ (nem engedélyezett parancs).

— Ha a rekord nem található, akkor a biztonságos GNSS adó-vevő a következőt küldi vissza: ‘**6A 83**’.

— Ha a külső GNSS-eszköz manipulálást észlelt, a következő állapotszavakat kell visszaküldenie: ‘**66 90**’.

GNS_27 A biztonságos GNSS adó-vevőnek támogatnia kell a következő, a menetíró készülékek 2. generációjához tartozó, a 2. függelékben meghatározott parancsokat:

Parancs	Hivatkozás
Select	2. függelék 3.5.1. fejezet
Read Binary	2. függelék 3.5.2. fejezet
Get Challenge	2. függelék 3.5.4. fejezet
PSO: Verify Certificate	2. függelék 3.5.7. fejezet
External Authenticate	2. függelék 3.5.9. fejezet
General Authenticate	2. függelék 3.5.10. fejezet
MSE:SET	2. függelék 3.5.11. fejezet

▼B

4.3. **A külső GNSS-eszköz és a járműegység összekapcsolása, kölcsönös hitelesítése és műveletkulcs-egyeztetése**

A külső GNSS-eszköz és a járműegység összekapcsolásának, kölcsönös hitelesítésének és műveletkulcs-egyeztetésének leírása a 11. függelék (Közös biztonsági mechanizmusok) 11. fejezetében található.

4.4. **Hibakezelés**

Ez a rész azt mutatja be, hogy a külső GNSS-eszköz lehetséges hibaállapotai hogyan kerülnek kezelésre és rögzítésre a járműegységben.

4.4.1 *Kommunikációs hiba a külső GNSS-eszközzel*

GNS_28 Ha a járműegységnek 20 folyamatos percen keresztül nem sikerül kommunikálnia a csatlakoztatott külső GNSS-eszközzel, akkor a járműegységnek létre kell hoznia és a járműegységben rögzítenie kell egy EventFaultType típusú, enum ‘53’H *External GNSS communication fault* eseményt az aktuális időpontot jelző időbélyegzővel. Az esemény létrehozása csak a következő két feltétel teljesülése esetén történik meg: a) az intelligens menetíró készülék nincs kalibrálási üzemmódban, és b) a jármű mozog. Ebben az összefüggésben a kommunikációs hibát az idézi elő, hogy a járműegység biztonságos adó-vevője nem kap válaszüzenetet a 4.2. pontban leírt kérésüzenet után.

4.4.2 *A külső GNSS-eszköz fizikai épségének megsértése*

GNS_29 Ha a külső GNSS-eszköz megsérült, a biztonságos GNSS adó-vevőnek a teljes memóriáját törölnie kell, a kriptográfiai anyagot is beleértve. A GNS_25 és GNS_26 követelményben leírtak szerint a járműegységnek észlelnie kell a manipulálást, ha a válasz állapota ‘6690’. A járműegységnek ezután egy EventFaultType típusú, ‘55’H *Tamper detection of GNSS* eseményt kell létrehoznia.

4.4.3 *A GNSS-vevőből származó helyzetmeghatározási információk hiánya*

GNS_30 Ha a biztonságos GNSS adó-vevő több mint 3 folyamatos órán át nem fogadott adatokat a GNSS-vevőtől, akkor a biztonságos GNSS adó-vevőnek létre kell hoznia egy válaszüzenetet a READ RECORD parancsra, amelyben a rekord száma ‘01’, az adatmező 12 bájtos és mindegyik bájt 0xFF értékre van állítva. A fenti értékkel és adatmezővel rendelkező válaszüzenet fogadását követően a járműegységnek csak akkor kell létrehoznia és rögzítenie egy EventFaultType típusú, enum ‘52’H *external GNSS receiver fault* eseményt az aktuális időpontnak megfelelő időbélyegzővel, ha az alábbi két feltétel teljesül: a) az intelligens menetíró készülék nincs kalibrálási üzemmódban, és b) a jármű mozog.

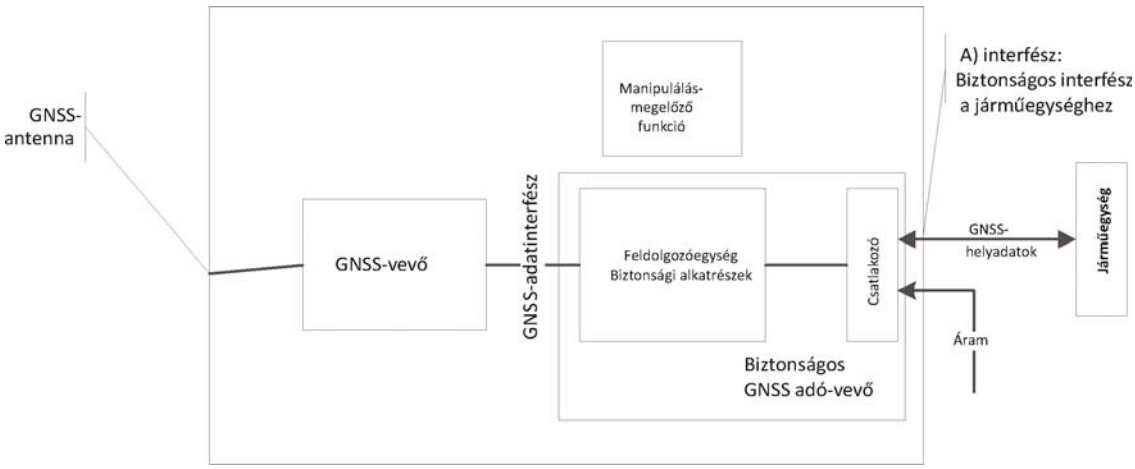
4.4.4 *A külső GNSS-eszköz tanúsítványa lejárt*

GNS_31 Ha a járműegység azt észleli, hogy a kölcsönös hitelesítéshez használt EGF tanúsítvány már nem érvényes, akkor a járműegységnek létre kell hoznia és rögzítenie kell egy EventFaultType típusú, enum *‘56’H External GNSS facility certificate expired* adatrögzítőkészülék-hibát az aktuális időpontnak megfelelő időbélyegzővel. A járműegységnek ennek ellenére fel kell használnia a fogadott GNSS-helyzetmeghatározási adatokat.

▼B

4. ábra

A külső GNSS-eszköz áttekintése



5. KÜLSŐ GNSS-ESZKÖZ NÉLKÜLI JÁRMŰEGYSÉG

5.1. **Konfiguráció**

Ebben a konfigurációban a GNSS-vevő a járműegységen belül található az 1. ábra szerint.

GNS_32 A GNSS-vevőnek adóként kell működnie és NMEA-adatmondatokat kell továbbítania a járműegység processzorához, amelynek legalább 1/10 Hz frekvenciával vevőként kell működnie az előre meghatározott NMEA-adatmondatok vonatkozásában, amelyeknek legalább az RMC és a GSA adatmondatokat magukban kell foglalniuk.

GNS_33 A járműre szerelt külső GNSS-antennát vagy a belső GNSS-antennát csatlakoztatni kell a járműegységhez.

5.2. **Hibakezelés**

5.2.1 *A GNSS-vevőből származó helyzetmeghatározási információk hiánya*

GNS_34 Ha a járműegység több mint 3 folyamatos órán át nem fogadott adatokat a GNSS-vevőtől, akkor a járműegységnek létre kell hoznia és rögzítenie kell egy EventFaultType típusú, enum ‘51’H *Internal GNSS receiver fault* eseményt az aktuális időpontnak megfelelő időbélyegzővel, de csak abban az esetben, ha az alábbi két feltétel teljesül: a) az intelligens menetíró készülék nincs kalibrálási üzemmódban, és b) a jármű mozog.

6. A GNSS IDŐÜTKÖZÉSE

Ha a járműegység 1 percnél nagyobb eltérést észlel a járműegység időmérő funkciója szerinti idő és GNSS-vevőtől származó időadat között, akkor a járműegységnek létre kell hoznia és rögzítenie kell egy EventFaultType típusú, enum *‘0B’H Time conflict (GNSS versus VU internal clock)* eseményt. Ez az esemény a járműegység belső időmérőjének értékével együtt rögzítésre kerül, és automatikus időbeállítást eredményez. Egy időütközés esemény kiváltását követően a járműegység a következő 12 órában nem fogja ellenőrizni az időeltéréseket. A szóban forgó esemény kiváltását el kell kerülni, ha a GNSS-vevő az utolsó 30 nap során nem észlelt érvényes GNSS-jelet. Amint azonban a GNSS-vevő ismét helyzetmeghatározási információkat szolgáltat, az automatikus időbeállításnak meg kell történnie.

▼B

7. A JÁRMŰ MOZGÁSÁVAL KAPCSOLATOS ELLENTMONDÁS

GNS_35 A járműegységnek ki kell váltania és rögzítenie kell egy, a jármű mozgásával kapcsolatos ellentmondást (lásd e függelék 84. követelményét) jelző eseményt az aktuális időpontnak megfelelő időbélyegzővel, amennyiben a mozgásérzékelő alapján számított mozgásadatok ellentmondanak belső GNSS-vevő vagy a külső GNSS-eszköz alapján számított mozgásadatoknak. Ezen ellentmondások észlelése céljából a források közötti sebességkülönbség medián értékét kell használni az alábbiaknak megfelelően:

— Legfeljebb 10 másodpercenként ki kell számítani a GNSS alapján becsült járműsebesség és a mozgásérzékelő alapján becsült járműsebesség különbségének abszolút értékét.

— A medián érték kiszámításához fel kell használni a mozgás utolsó öt perce időablakának valamennyi számított értékét.

— Az abszolút értékben számított legnagyobb értékek kizárása után, a medián értéket a fennmaradó értékek 80 %-ából kell kiszámítani.

A jármű mozgásával kapcsolatos ellentmondás eseményt az idézi elő, ha a medián érték 10 km/h fölött van öt olyan folyamatos percen keresztül, amikor a jármű mozog. Annak érdekében, hogy a menetíró készülékek manipulálásának észlelése megbízhatóbb legyen, tetszőlegesen használhatók a járműmozgás észlelésének egyéb független forrásai is. (Megjegyzés: az utolsó 5 perc mediánjának alkalmazása a kiugró és tranziens értékek mérésének kockázatát mérsékli.) A szóban forgó esemény kiváltását el kell kerülni a következő körülmények között: a) kompon/vonaton való utazás közben, b) ha a GNSS-vevőből származó helyzetmeghatározási információk nem állnak rendelkezésre, és c) kalibrálási üzemmódban.

▼B

13. függelék

ITS-INTERFÉSZ

TARTALOMJEGYZÉK

1. BEVEZETÉS

2. HATÁLY

2.1. Fogalommeghatározások, rövidítések és jelentésük

3. A HIVATKOZOTT RENDELETEK ÉS SZABVÁNYOK

4. AZ INTERFÉSZ MŰKÖDÉSI ELVEI

4.1. Az ITS-interfészen keresztül történő adatátvitel előfeltételei

4.1.1. Az ITS-interfészen keresztül elérhető adatok

4.1.2. Az adatok tartalma

4.1.3. ITS-alkalmazások

4.2. Kommunikációtechnológia

4.3. A PIN hitelesítése

4.4. Az üzenetek formátuma

4.5. A járművezető hozzájárulása

4.6. Szabványos adatok lekérése

4.7. Személyes adatok lekérése

4.8. Az eseményekkel és a hibákkal kapcsolatos adatok lekérése

1. BEVEZETÉS

Ez a függelék azt a kialakítást és azokat az eljárásokat határozza meg, amelyeket az intelligens közlekedési rendszerekhez (ITS) kapcsolódó interfész megvalósításához követni kell a 165/2014/EU rendelet 10. cikkében előírtak szerint.

A rendelet kimondja, hogy a járművek menetíró készülékeit el lehet látni olyan szabványosított interfészekkel, amelyek lehetővé teszik, hogy a menetíró készülék által rögzített vagy előállított adatokat egy külső eszköz működési üzemmódban felhasználja, feltéve, hogy teljesülnek az alábbi feltételek:

a) az interfész nem befolyásolja a menetíró készülék adatainak hitelességét és integritását;

b) az interfész megfelel a rendelet 11. cikkében szereplő részletes rendelkezéseknek;

c) az interfészhez csatlakozó külső eszköz csak akkor fér hozzá a földrajzi helymeghatározási adatokat is magukban foglaló személyes adatokhoz, ha a járművezető, akire az adatok vonatkoznak, ehhez igazolhatóan a hozzájárulását adta.

2. HATÁLY

E függelék arra terjed ki, hogy a külső eszközökön található alkalmazások hogyan tudnak Bluetooth®-kapcsolaton keresztül adatokhoz jutni a menetíró készülékről.

Az ezen az interfészen keresztül elérhető adatokat e dokumentum 1. melléklete mutatja be. Ez az interfész nem zárja ki más interfészek alkalmazását (pl. a CAN buszon keresztül) abból a célból, hogy a járműegység adatait a jármű egyéb feldolgozóegységeihez továbbítsák.

▼B

Ez a függelék a következőket határozza meg:

— az ITS-interfészen keresztül elérhető adatok;

— az adatok továbbításához használt Bluetooth®-profil;

— a lekérdezési és letöltési eljárások, valamint a műveletek sorrendje;

— a menetíró készülék és a külső eszköz közötti párosítási mechanizmus;

— a járművezető számára rendelkezésre álló hozzájárulási mechanizmus.

Ebből következően e függelék nem terjed ki az alábbiakra:

— az adatok gyűjtése és a járműegységben való kezelése (ezt a témát a rendelet egyéb részei tárgyalják vagy a termék kialakításától függ);

— az összegyűjtött adatok bemutatásának módja a külső eszközön található alkalmazás felé;

— az adatok tartalmára vonatkozóan a Bluetooth®-ban (pl. titkosítás) foglaltakon túli adatbiztonsági rendelkezések (melyeket e rendelet egyéb részei tárgyalnak, pl. a közös biztonsági mechanizmusokról szóló 11. függelék);

— az ITS-interfész által használt Bluetooth®-protokollok.

2.1. **Fogalommeghatározások, rövidítések és jelentésük**

E függelék a következő egyedi rövidítéseket és fogalommeghatározásokat alkalmazza:

kommunikáció	Információk/adatok cseréje egy mesteregység (azaz a menetíró készülék) és egy külső egység között a Bluetooth®-kapcsolatot használó ITS-interfész révén.
adatok	Az 1. mellékletben meghatározott adatok.
rendelet	Az Európai Parlament és a Tanács 2014. február 4-i 165/2014/EU rendelete a közúti közlekedésben használt menetíró készülékekről, a közúti közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendelet hatályon kívül helyezéséről és a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról szóló 561/2006/EK európai parlamenti és tanácsi rendelet módosításáról
BR	Basic Rate – Adatátviteli alapsebesség
EDR	Enhanced Data Rate – Fokozott adatátviteli sebesség
GNSS	Global Navigation Satellite System – Globális navigációs műholdrendszer
IRK	Identity Resolution Key – Azonosításfeloldási kulcs
ITS	Intelligent Transport System – Intelligens közlekedési rendszer
LE	Low Energy – Alacsony energiaszint
PIN	Personal Identification Number – Személyi azonosító szám
PUC	Personal Unblocking Code – Személyi feloldó kód
SID	Service Identifier – Szolgáltatóazonosító
SPP	Serial Port Profile – Soros port profilja

▼B

SSP	Secure Simple Pairing – Biztonságos egyszerű párosítás
TRTP	Transfer Request Parameter – Átviteli kérésparaméter
TREP	Transfer Response Parameter – Átviteli válaszparaméter
VU	Vehicle Unit – Járműegység

3. A HIVATKOZOTT RENDELETEK ÉS SZABVÁNYOK

Az e függelékben szereplő előírások az alább felsorolt rendeletek és szabványokra vagy azok részeire hivatkoznak és épülnek. A függelék rendelkezései konkrétan meghatározzák a vonatkozó szabványokat vagy azok vonatkozó részeit. Ellentmondás esetén e függelék rendelkezéseit kell alkalmazni.

E függelék a következő rendeletekre és szabványokra hivatkozik:

— Az Európai Parlament és a Tanács 2014. február 4-i 165/2014/EU rendelete a közúti közlekedésben használt menetíró készülékekről, a közúti közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendelet hatályon kívül helyezéséről és a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról szóló 561/2006/EK európai parlamenti és tanácsi rendelet módosításáról

— Az Európai Parlament és a Tanács 2006. március 15-i 561/2006/EK rendelete a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról, a 3821/85/EGK és a 2135/98/EK tanácsi rendelet módosításáról, valamint a 3820/85/EGK tanácsi rendelet hatályon kívül helyezéséről

— ISO 16844 – 4: Közúti járművek – Menetíró rendszerek – 4. rész: CAN-interfész

— ISO 16844 – 7: Közúti járművek – Menetíró rendszerek – 7. rész: Paraméterek

— Bluetooth® – A soros port profilja – V1.2

— Bluetooth® – Alapverzió 4.2

— NMEA 0183 V4.1 protokoll

4. AZ INTERFÉSZ MŰKÖDÉSI ELVEI

4.1. **Az ITS-interfészen keresztül történő adatátvitel előfeltételei**

A járműegység felel a járműegységben tárolt adatoknak az ITS-interfész bármilyen bevonása nélküli frissítéséért és fenntartásáért. Ennek megvalósítási módja járműegység-specifikus, és nem ebben a függelékben, hanem a rendelet egyéb szakaszaiban van meghatározva.

4.1.1 *Az ITS-interfészen keresztül elérhető adatok*

A járműegység felel az ITS-interfészen keresztül elérhető adatoknak az ITS-interfész bármilyen bevonása nélküli frissítéséért, melynek gyakoriságát a járműegységek gyártói határozzák meg. A járműegység adatai képezik az adatok feltöltésének és frissítésének alapját, melynek módja e rendelet egyéb szakaszaiban van meghatározva, vagy ilyen előírás hiányában a termék kialakításának függvénye, és e függelékben nem szerepel.

▼B

4.1.2 *Az adatok tartalma*

Az adatok tartalmának meg kell felelnie az e függelék 1. mellékletében foglaltaknak.

4.1.3 *ITS-alkalmazások*

Az ITS-alkalmazások az ITS-interfészen keresztül rendelkezésre bocsátott adatokat használják például a járművezetői tevékenység kezelésének e rendelet előírásai szerinti optimalizálása, a menetíró készülék esetleges hibáinak észlelése vagy a GNSS-adatok felhasználása céljából. Az alkalmazásokra vonatkozó előírások nem tartoznak e függelék hatálya alá.

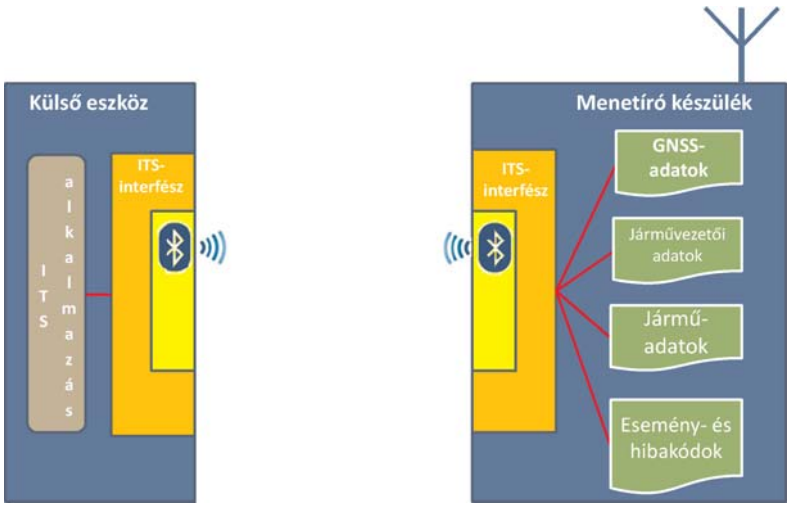
4.2. **Kommunikációtechnológia**

Az ITS-interfész használatával történő adatcserének a 4.2 vagy későbbi verzióval kompatibilis Bluetooth®-interfészen keresztül kell zajlania. A Bluetooth® az engedély nélkül használható, az ipari, tudományos és orvosi alkalmazások (ISM) részére kiosztott 2,4–2,485 GHz-es frekvenciasávban működik. A Bluetooth® 4.2 megerősített adatvédelmi és biztonsági mechanizmusokat kínál, és növeli az adatátvitel sebességét és megbízhatóságát. Ezen előírás vonatkozásában 2. osztályú, 10 méterig terjedő hatótávolságú Bluetooth®-rádiót kell alkalmazni. A Bluetooth® 4.2-vel kapcsolatos további információk a következő weboldalon érhetők el: www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

A kommunikációs kapcsolatot a kommunikációs eszközzel azután kell létrehozni, hogy egy hitelesített eszköz révén lezárult a párosítási eljárás. Mivel a Bluetooth® mester-szolga modellt használ annak irányításához, hogy az eszközök mikor és hol küldhetnek adatokat, a menetíró készülék a mester, a külső eszköz pedig a szolga szerepét fogja betölteni.

Amikor egy külső eszköz első alkalommal került a járműegység hatókörébe, elindítható a Bluetooth® alapú párosítási eljárás (lásd még: 2. melléklet). Az eszközök megosztják egymással a címüket, nevüket, profiljukat és közös titkosítási kulcsukat, amely lehetővé teszi a kapcsolódást a továbbiakban, ha egymás hatókörébe kerülnek. E lépés lezárulása után a külső eszköz megbízhatónak minősül, és képes a menetíró készülékből való adatletöltésre irányuló kéréseket kezdeményezni. Előreláthatólag a Bluetooth® által kínáltakon kívül további titkosítási mechanizmusok hozzáadására nem fog sor kerülni. Mindazonáltal abban az esetben, ha további biztonsági mechanizmusokra lesz szükség, akkor azok meg fognak felelni a 10. függelék (Közös biztonsági mechanizmusok) előírásainak.

A teljes kommunikációs kapcsolat alapelvét a következő ábra mutatja be.



▼B

A járműegységről a külső eszközre történő adatátvitelhez a Bluetooth® SPP-jét, vagyis soros portjának profilját kell használni.

4.3. **A PIN hitelesítése**

Biztonsági okokból a járműegységnek a Bluetooth® alapú párosítástól független PIN kód hitelesítési rendszert kell alkalmaznia. Minden járműegységnek alkalmasnak kell lennie arra, hogy hitelesítés céljából legalább 4 számjegyű PIN kódokat generáljon. Amikor egy külső eszköz és a járműegység közötti párosításra kerül sor, a külső eszköznek minden alkalommal meg kell adnia a helyes PIN kódot, mielőtt adatokat fogadhatna.

A PIN kód sikeres megadásával az eszköz az engedélyezett eszközök listájára kerül. Az engedélyezett eszközök listájának alkalmasnak kell lennie legalább 64, az adott járműegységgel párosított eszköz tárolására.

A helyes PIN kód megadásának három egymás utáni sikertelen kísérlete után az eszköz átmenetileg a nem engedélyezett eszközök listájára kerül. Amíg az eszköz a nem engedélyezett eszközök listáján szerepel, minden kísérlete elutasításra kerül. Ha ezt követően ismét nem sikerül háromszor egymás után megadni a PIN kódot, az egyre hosszabb időtartamú letiltáshoz vezet (lásd: 1. táblázat). A helyes PIN kód megadása feloldja a letiltást és újraindítja a kísérletek számlálását. A PIN kód hitelesítésének folyamatábrája a 2. melléklet 1. ábráján látható.

1. táblázat

A letiltási időtartama a helyes PIN kód megadására irányuló, egymást követő sikertelen kísérleteinek számától függően

Egymást követő sikertelen kísérletek száma	Letiltás időtartama
3	30 másodperc
6	5 perc
9	1 óra
12	24 óra
15	Végleges

A helyes PIN kód megadásának tizenöt (5 × 3) egymás utáni sikertelen kísérlete után az ITS-egység véglegesen a nem engedélyezett eszközök listájára kerül. A végleges letiltást csak a PUC kód megadásával lehet feloldani.

A PUC kódnak 8 számjegyből kell állnia. A kódot gyártónak a járműegységgel együtt kell rendelkezésre bocsátania. A helyes PUC kód megadásának tíz egymás utáni sikertelen kísérlete után az ITS-egység visszavonhatatlanul a nem engedélyezett eszközök listájára kerül.

A gyártó felkínálhatja a PIN kód közvetlenül a járműegységen keresztül történő megváltoztatásának lehetőségét, a PUC kódnak azonban megváltoztathatatlannak kell lennie. A PIN kód megváltoztatásához lehetőleg elő kell írni az aktuális PIN kódnak közvetlenül a járműegységbe való bevitelét.

Ezenkívül az engedélyezett eszközök listáján szereplő valamennyi eszköz a listán marad, amíg a felhasználó manuálisan el nem távolítja őket onnan (pl. a járműegység felhasználó és gép közötti interfészén keresztül vagy más módon). Az ellopott vagy elveszett ITS-egységeket ily módon lehet eltávolítani az engedélyezett eszközök listájáról. Emellett minden olyan ITS-egység, amely 24 óránál hosszabb időre elhagyja a Bluetooth®-kapcsolat hatótávolságát, automatikusan lekerül az engedélyezett eszközök listájáról, és az ilyen egységeknek a kapcsolat újbóli megteremtésekor ismét meg kell adniuk a helyes PIN kódot.

▼B

A járműegység-interfész és a járműegység közötti üzenetek formátuma nincs meghatározva, arról a gyártó dönthet. A szóban forgó gyártónak azonban gondoskodnia kell arról, hogy az ITS-egység és a járműegység-interfész közötti üzenetek formátuma megfeleljen az előírásoknak (lásd az ASN.1 követelményt).

Ezért minden adatkérés esetén, mielőtt bármilyen kezelésre kerülne sor, el kell végezni a küldő hitelesítő adatainak megfelelő ellenőrzését. Ezen eljárás folyamatát a 2. melléklet 2. ábrája mutatja be. A nem engedélyezett eszközök listáján szereplő bármely eszköz automatikusan elutasításra kerül, azon eszközök pedig, amelyek sem az engedélyezett, sem a nem engedélyezett eszközök listáján nem szerepelnek, PIN-kérést kapnak, amelyet teljesíteniük kell, mielőtt az adatkérésük ismét elküldésre kerülne.

4.4. **Az üzenetek formátuma**

Az ITS-egység és a járműegység között küldött összes üzenet szerkezetének három részből kell állnia: fejrész, amely egy célbájtból (TGT), egy forrásbájtból (SCR) és egy hosszbájtból (LEN) áll;

adatmező, amely egy szolgáltatóazonosító bájtból (SID) és változó mennyiségű (legfeljebb 255) adatbájtból áll;

ellenőrző bájt, amely magán a CS-en kívül az üzenet összes bájtja egybájtos összegsorozatának 256-tal történő osztási maradéka.

Az üzenetnek big endian típusúnak kell lennie.

2. táblázat

Általános üzenetformátum

Fejrész			Adatmező					Ellenőrző összeg
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bájt			Maximum 255 bájt					1 bájt

Fejrész

TGT és SRC: az üzenet céleszközének (TGT) és forráseszközének (SRC) azonosítója. A járműegység-interfész alapértelmezett azonosítója „EE”. Ez az azonosító nem módosítható. A kommunikációs szakaszban az ITS-egységnek alapértelmezésben az „A0” azonosítót kell használnia az első üzenetéhez. Ezután a járműegység-interfésznek egyedi azonosítót kell hozzárendelnie az ITS-egységhez, és értesítenie kell az ITS-egységet annak a kommunikációs szakasz további üzeneteihez használandó azonosítójáról.

A LEN bájtnak csak az adatmező „ADAT” részét kell figyelembe vennie (lásd a 2. táblázatot), mivel az első 4 bájt magától értetődik.

A járműegység-interfésznek meg kell erősítenie az üzenetküldő hitelességét a saját azonosítólistája és a Bluetooth®-adatok közötti keresztellenőrzés révén oly módon, hogy ellenőrzi, hogy a megadott azonosítóval rendelkező ITS-egység aktuálisan a Bluetooth®-kapcsolat hatótávolságán belül van-e.

Adatmező

A SID mellett az adatmezőnek a következő paramétereket is tartalmaznia kell: egy átviteli kérésparamétert (TRTP) és a számlálóbájtokat.

▼B

Ha az átvitelre váró adatok hosszabbak, mint az egy üzenetben rendelkezésre álló hely, az üzenet több alüzenetre kerül felosztásra. A fejrésznek és a SID-nek minden alüzenetben azonosnak kell lennie, de az alüzeneteknek tartalmazniuk kell egy 2 bájtból (CC: jelenlegi számláló és CM: legnagyobb számláló) álló számlálót, amely jelzi az alüzenet számát. A hibák ellenőrzésének és a fogadás megszakításának lehetővé tétele érdekében az eszköz minden alüzenetet visszaigazol. A fogadó eszköz képes fogadni az alüzeneteket, kérni azok újbóli átvitelét, és képes arra, hogy felszólítsa a küldő eszközt az átvitel újraindítására vagy megszakítására.

Amennyiben nem alkalmazzák őket, a CC és a CM értékének 0xFF-nek kell lennie.

Például a következő üzenetet

HEADER	SID	TRTP	CC	CM	DATA	CS
3 bájt	255 bájtnál hosszabb					1 bájt

a következőképpen kell továbbítani:

HEADER	SID	TRTP	01	n	DATA	CS
3 bájt	255 bájt					1 bájt

HEADER	SID	TRTP	02	n	DATA	CS
3 bájt	255 bájt					1 bájt

…

HEADER	SID	TRTP	N	N	DATA	CS
3 bájt	Maximum 255 bájt					1 bájt

A 3. táblázat tartalmazza azokat az üzeneteket, amelyek cseréjére a járműegységnek és az ITS-egységnek képesnek kell lennie. Az egyes paraméterek tartalma hexadecimális formában van megadva. Az egyértelműség kedvéért a CC és CM üzenet nem szerepel a táblázatban, ezek teljes formátumát lásd feljebb.

3. táblázat

Az üzenetek részletes tartalma

Üzenet	Fejrész			ADAT			Ellenőrző összeg
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*EGÉSZ SZÁM (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	LOGIKAI (I/H)	
SendPUC	EE	*ITSID*	08	05	FF	8*EGÉSZ SZÁM (0..9)	

▼B

Üzenet	Fejrész			ADAT			Ellenőrző összeg
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	LOGIKAI (I/H)	
RequestRejected	*ITSID*	EE	08	07	FF	Idő	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Adatok	
DataUnavailable							
Nem áll rendelkezésre adat	*ITSID*	EE	02	0A	TREP	10	
A személyes adatok nincsenek megosztva	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Általános elutasítás	*ITSID*	EE	02	0B	SID Req	10	
A szolgáltatás nem támogatott	*ITSID*	EE	02	0B	SID Req	11	
Az alfunkció nem támogatott	*ITSID*	EE	02	0B	SID Req	12	
Az üzenet hossza helytelen	*ITSID*	EE	02	0B	SID Req	13	
A feltételek nem megfelelőek, vagy hiba van a kérési szekvenciában	*ITSID*	EE	02	0B	SID Req	22	
Tartományon kívüli kérés	*ITSID*	EE	02	0B	SID Req	31	
Válasz függőben	*ITSID*	EE	02	0B	SID Req	78	
ITSID eltérés	*ITSID*	EE	02	0B	SID Req	FC	
Az ITSID nem található	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Ezt az üzenetet a járműegység-interfész bocsátja ki, ha egy olyan ITS-egység küld bármilyen adatkérést, amely sem a nem engedélyezett, sem az engedélyezett eszközök listáján nem szerepel.

▼B

SendITSID (SID 02)

Ezt az üzenetet a járműegység-interfész bocsátja ki akkor, ha egy új eszköz küld kérést. Ennek az eszköznek az alapértelmezett „A0” azonosítót kell használnia, mielőtt egyedi azonosítót rendelnének hozzá a kommunikációs szakaszra.

SendPIN (SID 03)

Ezt az üzenetet az ITS-egység bocsátja ki abból a célból, hogy a járműegység-interfész az engedélyezett eszközök listájára helyezze. Ezen üzenet tartalma egy 4 (0 és 9 közötti) EGÉSZ SZÁMBÓL álló kód.

PairingResult (SID 04)

Ezt az üzenetet a járműegység-interfész bocsátja ki azzal a céllal, hogy tájékoztassa az ITS-egység arról, hogy az általa küldött PIN kód helyes volt-e. Az üzenet tartalma egy LOGIKAI adat, melynek értéke „Igaz”, ha a PIN helyes volt, és „Hamis”, ha helytelen.

SendPUC (SID 05)

Ezt az üzenetet az ITS-egység adja ki abból a célból, hogy a járműegység-interfész a nem engedélyezett eszközök listájáról eltávolítsa. Ezen üzenet tartalma egy 8 (0 és 9 közötti) EGÉSZ SZÁMBÓL álló kód.

BanLiftingResult (SID 06)

Ezt az üzenetet a járműegység-interfész bocsátja ki azzal a céllal, hogy tájékoztassa az ITS-egységet arról, hogy az általa küldött PUC kód helyes volt-e. Az üzenet tartalma egy LOGIKAI adat, melynek értéke „Igaz”, ha a PUC helyes volt, és „Hamis”, ha helytelen.

RequestRejected (SID 07)

Ezt az üzenetet a járműegység-interfész bocsátja ki válaszként a „SendPUC” üzeneten kívüli bármely olyan üzenetre, amely a nem engedélyezett eszközök listáján szereplő ITS-egységtől érkezik. Az üzenetnek tartalmaznia kell azt, hogy az ITS-egység még mennyi ideig szerepel a nem engedélyezett eszközök listáján a 3. mellékletben meghatározott „Time” sorozatformátumnak megfelelően.

RequestData (SID 08)

Ezt az üzenetet az ITS-egység bocsátja ki az adatokhoz való hozzáférés céljából. Egy egybájtos átviteli kérésparaméter (TRTP) jelzi a kért adatok típusát. Az adatoknak többféle típusa van:

— standardTachData (TRTP 01): A menetíró készülékből származó, nem személyes adatoknak minősülő adatok.

— personalTachData (TRTP 02): A menetíró készülékből származó, személyes adatoknak minősülő adatok.

— gnssData (TRTP 03): A mindig személyes adatnak minősülő GNSS-adatok.

— standardEventData (TRTP 04): Rögzített eseményadatok, amelyek nem személyes adatoknak minősülnek.

— personalEventData (TRTP 05): Rögzített eseményadatok, amelyek személyesnek minősülnek.

— standardFaultData (TRTP 06): Rögzített hibák, amelyek nem személyesnek minősülnek.

— manufacturerData (TRTP 07): A gyártó által rendelkezésre bocsátott adatok.

▼B

Az egyes adattípusok tartalmára vonatkozó további információkért lásd e függelék 3. mellékletét.

A GNSS-adatok formátumára és tartalmára vonatkozó további információkért lásd a 12. függeléket.

Az eseményadatokra és hibákra vonatkozó további információkért lásd az IB. és IC. mellékletet.

ResquestAccepted (SID 09)

Ezt az üzenetet a járműegység-interfész bocsátja ki, ha az ITS-egység „RequestData” üzenete elfogadásra került. Az üzenet tartalmaz egy egybájtos TREP-et, amely a kapcsolódó RequestData üzenet TRTP bájtja, és tartalmazza az összes kért típusú adatot.

DataUnavailable (SID 0A)

Ezt az üzenetet a járműegység-interfész bocsátja ki akkor, ha valamilyen okból a kért adatok nem állnak rendelkezésre az engedélyezett eszközök listáján szereplő ITS-egységnek való küldésre. Az üzenet tartalmaz egy egybájtos TREP-et, amely a kért adatok TRTP-je, és egy egybájtos hibakódot a 3. táblázat meghatározásai szerint. A következő kódok állnak rendelkezésre:

— Nem áll rendelkezésre adat (10): A járműegység-interfész meg nem határozott okokból nem fér hozzá a járműegység adataihoz.

— A személyes adatok nincsenek megosztva (11): Az ITS-egység személyes adatokat próbál lekérni, de azok nincsenek megosztva.

NegativeAnswer (SID 0B)

Ezeket az üzeneteket a járműegység-interfész bocsátja ki akkor, ha egy kérést az adatok rendelkezésre állásának hiányán kívüli bármilyen más okból nem lehet teljesíteni. Ezek az üzenetek általában a kérés helytelen formátumának (hossz, SID, ITSID ...) következményei, de más okokból is előfordulhatnak. Az adatmezőben szereplő TRTP tartalmazza a kérés SID-jét. Az adatmező magában foglal egy kódot, amely megadja a negatív válasz okát. A következő kódok állnak rendelkezésre:

— Általános elutasítás (kód: 10)

— A művelet olyan okból nem hajtható végre, amely sem alább, sem a *DataUnavailable* szakaszában nem szerepel.

— A szolgáltatás nem támogatott (kód: 11)

— A kérés SID-je nem érthető.

— Az alfunkció nem támogatott (kód: 12)

— A kérés TRTP-je nem érthető. Előfordulhat például, hogy a TRTP hiányzik vagy értéke az elfogadott értékeken kívül esik.

— Az üzenet hossza helytelen (kód: 13)

— A fogadott üzenet hossza helytelen (eltérés van a LEN bájtok és a tényleges üzenethossz között).

— A feltételek nem megfelelőek, vagy hiba van a kérési szekvenciában (kód: 22)

— A kért szolgáltatás nem aktív, vagy a kérésüzenet sorrendje nem megfelelő.

— Tartományon kívüli kérés (kód: 33)

▼B

— A kérésparaméter rekordja (adatmező) érvénytelen.

— Válasz függőben (kód: 78)

— A kért műveletet nem lehet időben teljesíteni, és a járműegység nem áll készen további kérések fogadására.

— *ITSID*-eltérés (kód: FB)

— Az SRC *ITSID* a Bluetooth®-információk összehasonlítása alapján nem felel meg a kapcsolódó eszköznek.

— Az *ITSID* nem található (kód: FC)

— Az SRC *ITSID* egyetlen eszközhöz sem kapcsolódik.

A 3. táblázatban szereplő üzenetek formátumát a 3. mellékletben szereplő ASN.1 kód 1–72. sora (**FormatMessageModule**) határozza meg. Az üzenetek tartalmára vonatkozó további részletek az alábbiakban olvashatók.

4.5. **A járművezető hozzájárulása**

Valamennyi rendelkezésre álló adat a személyes vagy a nem személyes kategóriába van sorolva. A személyes adatokhoz csak akkor lehet hozzáférni, ha a járművezető hozzájárulását adta ehhez, vagyis elfogadta, hogy a menetíró készülékben lévő személyes adatai elhagyhatják a jármű hálózatát és harmadik felek alkalmazásai hozzáférhetnek azokhoz.

A járművezető akkor járul hozzá mindehhez, amikor a járműegység számára az adott pillanatban ismeretlen járművezetői kártya vagy műhelykártya első behelyezésekor a készülék arra kéri a kártya tulajdonosát, hogy járuljon hozzá a menetíró készülékkel kapcsolatos személyes adatainak az opcionális ITS-interfészen keresztüli továbbításához. (Lásd az I. C. melléklet 3.6.2. szakaszát).

A hozzájárulás státuszát (megadva/elutasítva) a menetíró készülék memóriája tárolja.

Több járművezető esetén csak azon járművezetők személyes adatai oszthatók meg az ITS-interfésszel, akik hozzájárulásukat adták ehhez. Ha például a járművet két járművezető vezeti, és csak az első járult hozzá személyes adatainak megosztásához, akkor a második járművezető személyes adatai nem oszthatók meg.

4.6. **Szabványos adatok lekérése**

A 2. melléklet 3. ábrája az ITS-egység által a szabványos adatokhoz való hozzáférés céljából küldött érvényes kérés folyamatát mutatja be. Az ITS-egység szerepel az engedélyezett eszközök listáján és nem személyes adatokat kér, ezért nincs szükség további ellenőrzésre. Az ábrák abból indulnak ki, hogy a 2. melléklet 2. ábráján bemutatott folyamat már rendben lezárult. Az ábrák a 2. ábrán látható *REQUEST TREATMENT* feliratú szürke szövegdoboznak felelnek meg.

A rendelkezésre álló adatok közül az alábbiak minősülnek szabványosnak:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Személyes adatok lekérése**

A személyes adatokra vonatkozó kérés feldolgozásának folyamatát a 2. melléklet 4. ábrája mutatja be. Amint az korábban is említésre került, a járműegység-interfész csak akkor küldhet személyes adatokat, ha a járművezető ehhez egyértelműen hozzájárult (lásd a 4.5. szakaszt). Eltérő esetben a kérést automatikusan vissza kell utasítani.

▼B

A rendelkezésre álló adatok közül az alábbiak minősülnek személyesnek:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Az eseményekkel és a hibákkal kapcsolatos adatok lekérése**

Az ITS-egységeknek képesnek kell lenniük arra, hogy lekérjék a valamennyi váratlan esemény listáját tartalmazó eseményadatokat. Ezek az adatok szabványosnak vagy személyesnek minősülnek, lásd a 3. mellékletet. Valamennyi esemény tartalmának meg kell felelnie az e függelék 1. mellékletében megadott dokumentációnak.

▼B

1. MELLÉKLET

AZ ITS-INTERFÉSZEN KERESZTÜL ELÉRHETŐ ADATOK LISTÁJA

Adat	Forrás	►C2 Adatbesorolás (személyes/nem személyes) ◄
VehicleIdentificationNumber	Járműegység	**nem személyes**
CalibrationDate	Járműegység	**nem személyes**
TachographVehicleSpeed speed instant t	Járműegység	személyes
Driver1WorkingState Selector driver	Járműegység	személyes
Driver2WorkingState	Járműegység	személyes
DriveRecognize Speed Threshold detected	Járműegység	**nem személyes**
Driver1TimeRelatedStates Weekly day time	Járművezetői kártya	személyes
Driver2TimeRelatedStates	Járművezetői kártya	személyes
DriverCardDriver1	Járműegység	**nem személyes**
DriverCardDriver2	Járműegység	**nem személyes**
OverSpeed	Járműegység	személyes
TimeDate	Járműegység	**nem személyes**
HighResolutionTotalVehicleDistance	Járműegység	**nem személyes**
ServiceComponentIdentification	Járműegység	**nem személyes**
ServiceDelayCalendarTimeBased	Járműegység	**nem személyes**
Driver1Identification	Járművezetői kártya	személyes
Driver2Identification	Járművezetői kártya	személyes
NextCalibrationDate	Járműegység	**nem személyes**
Driver1ContinuousDrivingTime	Járművezetői kártya	személyes
Driver2ContinuousDrivingTime	Járművezetői kártya	személyes
Driver1CumulativeBreakTime	Járművezetői kártya	személyes
Driver2CumulativeBreakTime	Járművezetői kártya	személyes
Driver1CurrentDurationOfSelectedActivity	Járművezetői kártya	személyes
Driver2CurrentDurationOfSelectedActivity	Járművezetői kártya	személyes
SpeedAuthorised	Járműegység	**nem személyes**
TachographCardSlot1	Járművezetői kártya	**nem személyes**
TachographCardSlot2	Járművezetői kártya	**nem személyes**
Driver1Name	Járművezetői kártya	személyes
Driver2Name	Járművezetői kártya	személyes

▼B

Adat	Forrás	►C2 Adatbesorolás (személyes/nem személyes) ◄
OutOfScopeCondition	Járműegység	**nem személyes**
ModeOfOperation	Járműegység	**nem személyes**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Járművezetői kártya	személyes
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Járművezetői kártya	személyes
EngineSpeed	Járműegység	személyes
RegisteringMemberState	Járműegység	**nem személyes**
VehicleRegistrationNumber	Járműegység	**nem személyes**
Driver1EndOfLastDailyRestPeriod	Járművezetői kártya	személyes
Driver2EndOfLastDailyRestPeriod	Járművezetői kártya	személyes
Driver1EndOfLastWeeklyRestPeriod	Járművezetői kártya	személyes
Driver2EndOfLastWeeklyRestPeriod	Járművezetői kártya	személyes
Driver1EndOfSecondLastWeeklyRestPeriod	Járművezetői kártya	személyes
Driver2EndOfSecondLastWeeklyRestPeriod	Járművezetői kártya	személyes
Driver1CurrentDailyDrivingTime	Járművezetői kártya	személyes
Driver2CurrentDailyDrivingTime	Járművezetői kártya	személyes
Driver1CurrentWeeklyDrivingTime	Járművezetői kártya	személyes
Driver2CurrentWeeklyDrivingTime	Járművezetői kártya	személyes
Driver1TimeLeftUntilNewDailyRestPeriod	Járművezetői kártya	személyes
Driver2TimeLeftUntilNewDailyRestPeriod	Járművezetői kártya	személyes
Driver1CardExpiryDate	Járművezetői kártya	személyes
Driver2CardExpiryDate	Járművezetői kártya	személyes
Driver1CardNextMandatoryDownloadDate	Járművezetői kártya	személyes
Driver2CardNextMandatoryDownloadDate	Járművezetői kártya	személyes
TachographNextMandatoryDownloadDate	Járműegység	**nem személyes**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Járművezetői kártya	személyes
Driver2TimeLeftUntilNewWeeklyRestPeriod	Járművezetői kártya	személyes
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Járművezetői kártya	személyes
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Járművezetői kártya	személyes

▼B

Adat	Forrás	►C2 Adatbesorolás (személyes/nem személyes) ◄
Driver1CumulativeUninterruptedRestTime	Járművezetői kártya	személyes
Driver2CumulativeUninterruptedRestTime	Járművezetői kártya	személyes
Driver1MinimumDailyRest	Járművezetői kártya	személyes
Driver2MinimumDailyRest	Járművezetői kártya	személyes
Driver1MinimumWeeklyRest	Járművezetői kártya	személyes
Driver2MinimumWeeklyRest	Járművezetői kártya	személyes
Driver1MaximumDailyPeriod	Járművezetői kártya	személyes
Driver2MaximumDailyPeriod	Járművezetői kártya	személyes
Driver1MaximumDailyDrivingTime	Járművezetői kártya	személyes
Driver2MaximumDailyDrivingTime	Járművezetői kártya	személyes
Driver1NumberOfUsedReducedDailyRestPeriods	Járművezetői kártya	személyes
Driver2NumberOfUsedReducedDailyRestPeriods	Járművezetői kártya	személyes
Driver1RemainingCurrentDrivingTime	Járművezetői kártya	személyes
Driver2RemainingCurrentDrivingTime	Járművezetői kártya	személyes
GNSS position	Járműegység	személyes

2. A JÁRMŰVEZETŐ HOZZÁJÁRULÁSA UTÁN ELÉRHETŐ FOLYAMATOS GNSS-ADATOK

Lásd: 12. függelék – GNSS.

3. A JÁRMŰVEZETŐ HOZZÁJÁRULÁSA NÉLKÜL ELÉRHETŐ ESEMÉNYKÓDOK

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Érvénytelen kártya behelyezése	— a 10 legutóbbi esemény,	— az esemény dátuma és időpontja, — az eseményt előidéző kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kártyaütközés	— a 10 legutóbbi esemény,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — a kártyaütközést előidéző két kártya típusa, száma, kiállító tagállama és generációja.
Az utolsó kártyakapcsolat nem megfelelő lezárása	— a 10 legutóbbi esemény,	— a kártyabehelyezés dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — a kártyáról leolvasott utolsó kártyakapcsolat adatai: — a kártyabehelyezés dátuma és időpontja, — a jármű rendszáma (VRN) és a nyilvántartásba vétel szerinti tagállam.

▼B

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Az áramellátás megszakadása (2)	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kommunikációs hiba a távoli kommunikációs eszközzel	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A GNSS-vevőből származó helymeghatározási információk hiánya	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A mozgásadatok hibája	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A jármű mozgásával kapcsolatos ellentmondás	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
A biztonsági rendszer megsértésére irányuló kísérlet	a 10 legutolsó esemény eseménytípusonként,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja (ha lényeges), — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az esemény típusa.

▼B

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Időátfedés	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az adatrögzítő készülék által rögzített dátum és időpont, — GNSS-dátum és -időpont, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.

4. A JÁRMŰVEZETŐ HOZZÁJÁRULÁSA ESETÉN ELÉRHETŐ ESEMÉNYKÓDOK

Esemény	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
Járművezetés megfelelő kártya nélkül	— a leghosszabb esemény az utolsó 10 előfordulási nap mindegyikén, — az öt leghosszabb esemény az utolsó 365 nap folyamán,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Kártya behelyezése járművezetés közben	— az utolsó esemény az utolsó 10 előfordulási nap mindegyikén,	— az esemény dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja, — az ugyanazon a napon történt hasonló események száma.
Gyorshajtás (1)	— a legsúlyosabb esemény az utolsó 10 előfordulási nap mindegyikén (például az, amelynél a legmagasabb volt az átlagsebesség), — az öt legsúlyosabb esemény az utolsó 365 nap folyamán. — a legutóbbi kalibrálást követő első esemény,	— az esemény kezdetének dátuma és időpontja, — az esemény végének dátuma és időpontja, — az esemény alatt mért legnagyobb sebesség, — az esemény alatt mért számtani átlagsebesség, — a járművezetői kártya típusa, száma, kiállító tagállama és generációja (adott esetben), — az ugyanazon a napon történt hasonló események száma.

5. A JÁRMŰVEZETŐ HOZZÁJÁRULÁSA NÉLKÜL ELÉRHETŐ HIBAKÓDOK

Hiba	Tárolási szabályok	Az egyes hibákkal kapcsolatban rögzítendő adatok
Kártyahiba	— a 10 legutóbbi járművezetői kártyahiba.	— a hiba kezdetének dátuma és időpontja, — a hiba végének dátuma és időpontja, — a kártya (kártyák) típusa, száma, kiállító tagállama és generációja.
Az adatrögzítő készülék hibái	— a 10 legutóbbi hiba minden egyes hibatípusra, — a legutóbbi kalibrálást követő első hiba.	— a hiba kezdetének dátuma és időpontja, — a hiba végének dátuma és időpontja, — a hiba típusa, — a hiba kezdetén és/vagy végén behelyezett kártya (kártyák) típusa, száma, kiállító tagállama és generációja.

▼B

Ezt a hibát a kalibrálási üzemmódon kívül bekövetkező bármely alábbi meghibásodásnak elő kell idéznie:

— a járműegység belső hibája,

— nyomtatóhiba,

— kijelzőhiba,

— letöltési hiba,

— érzékelőhiba,

— a GNSS-vevő vagy a külső GNSS-eszköz hibája,

— a távoli kommunikációs eszköz hibája

6. A JÁRMŰVEZETŐ HOZZÁJÁRULÁSA NÉLKÜL RENDELKEZÉSRE ÁLLÓ GYÁRTÓSPECIFIKUS ESEMÉNYEK ÉS HIBÁK

Esemény vagy hiba	Tárolási szabályok	Az egyes eseményekkel kapcsolatban rögzítendő adatok
A gyártó határozza meg	A gyártó határozza meg	A gyártó határozza meg

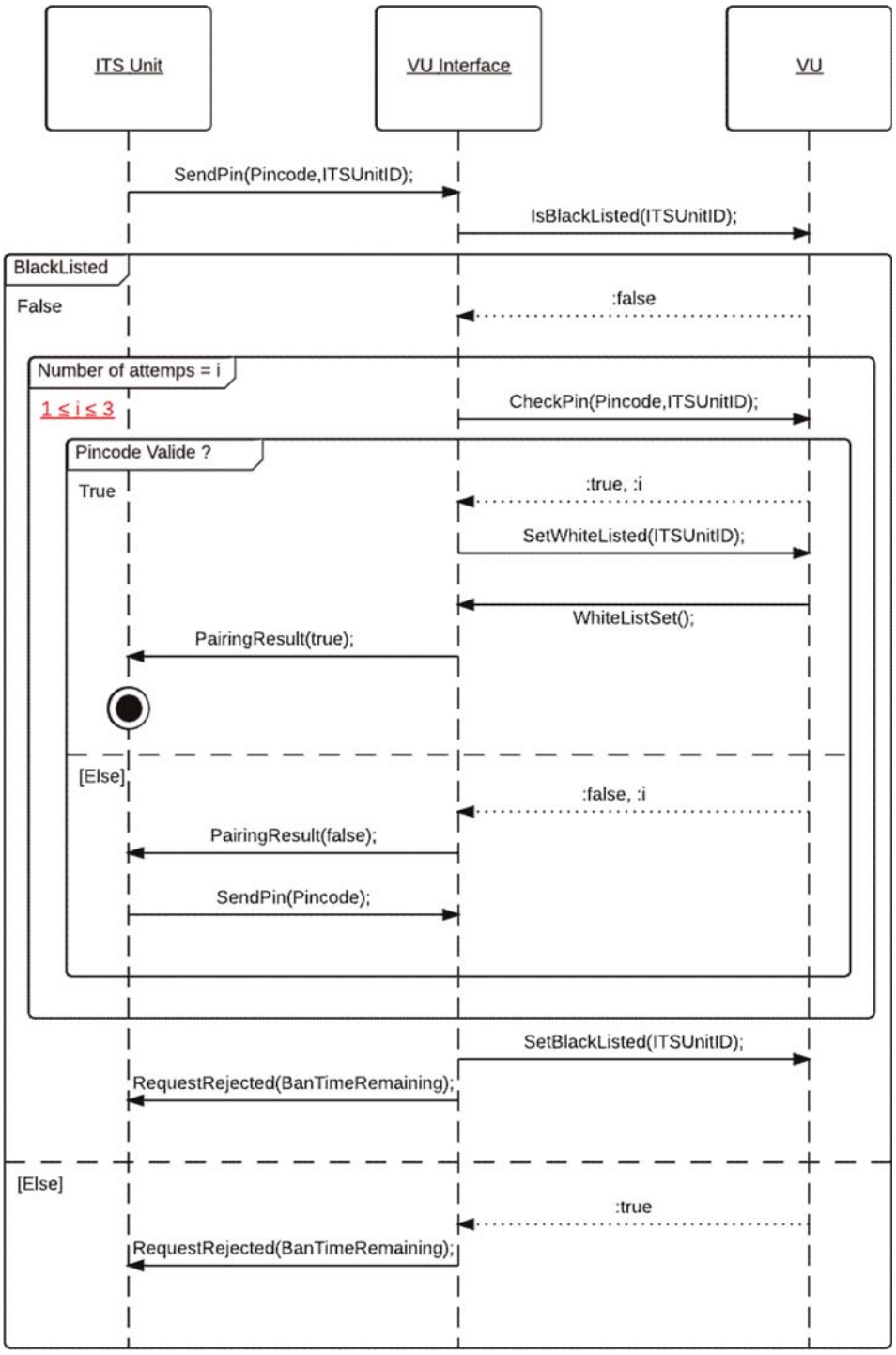
▼B

2. MELLÉKLET

AZ ITS-EGYSÉGGEL TÖRTÉNŐ ÜZENETCSERE FOLYAMATÁBRÁI

1. ábra

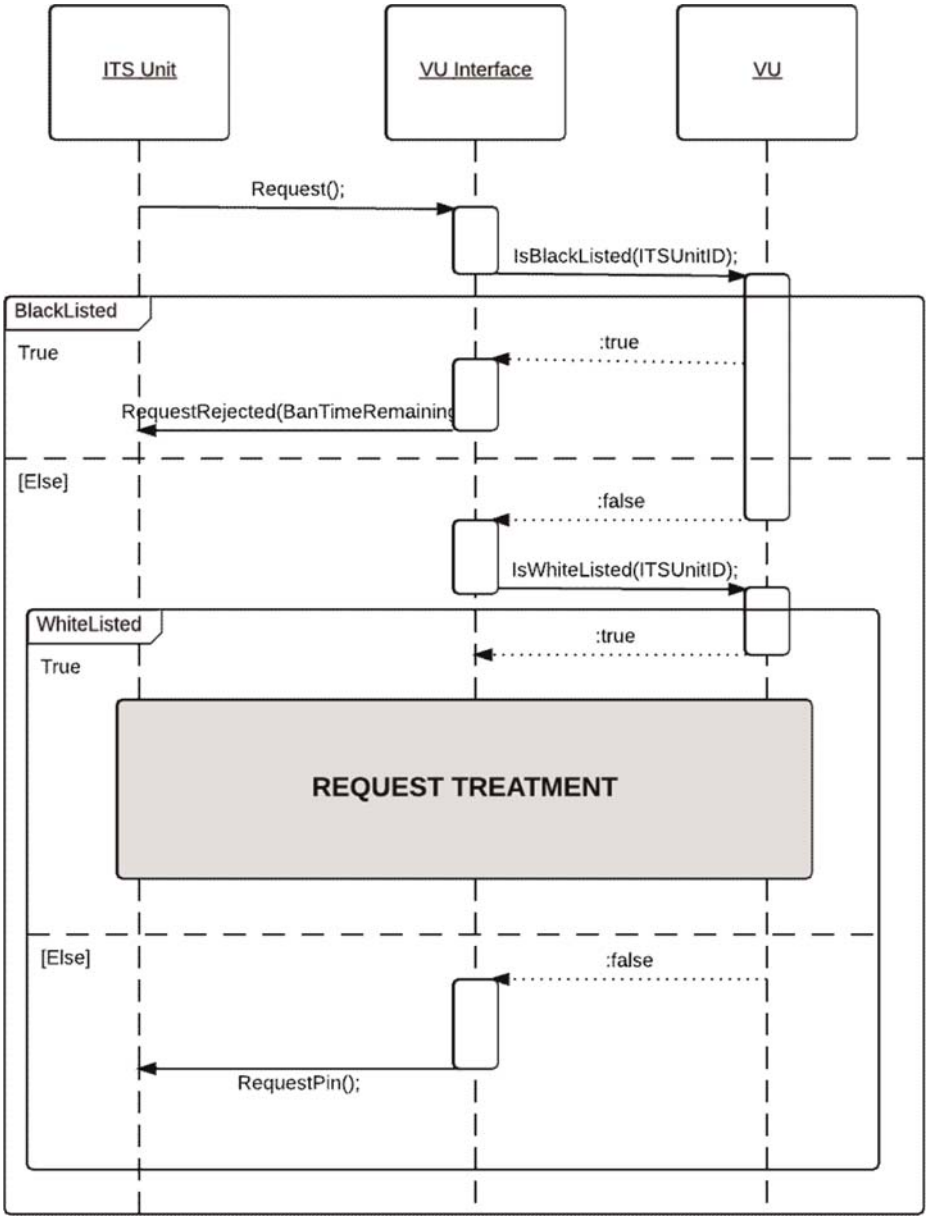
A PIN validálási kísérletének folyamatábrája



▼B

2. ábra

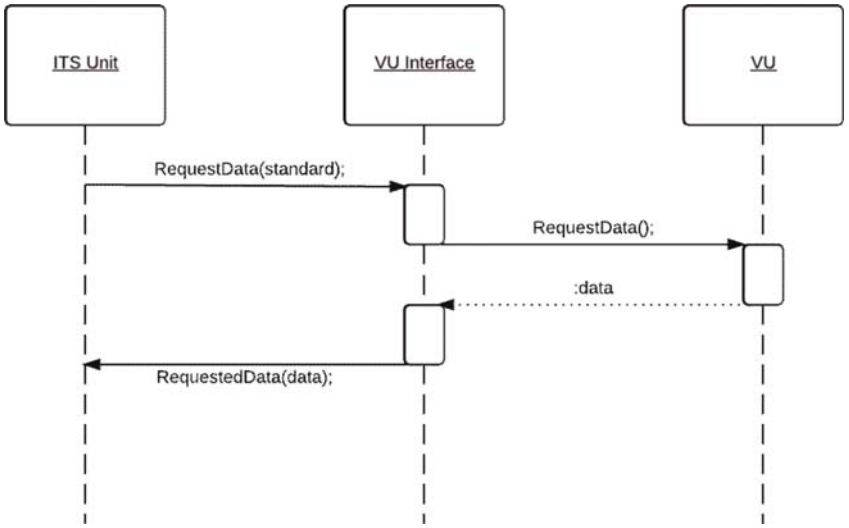
Az ITS-egység hitelesítésének ellenőrzésére vonatkozó folyamatábra



▼B

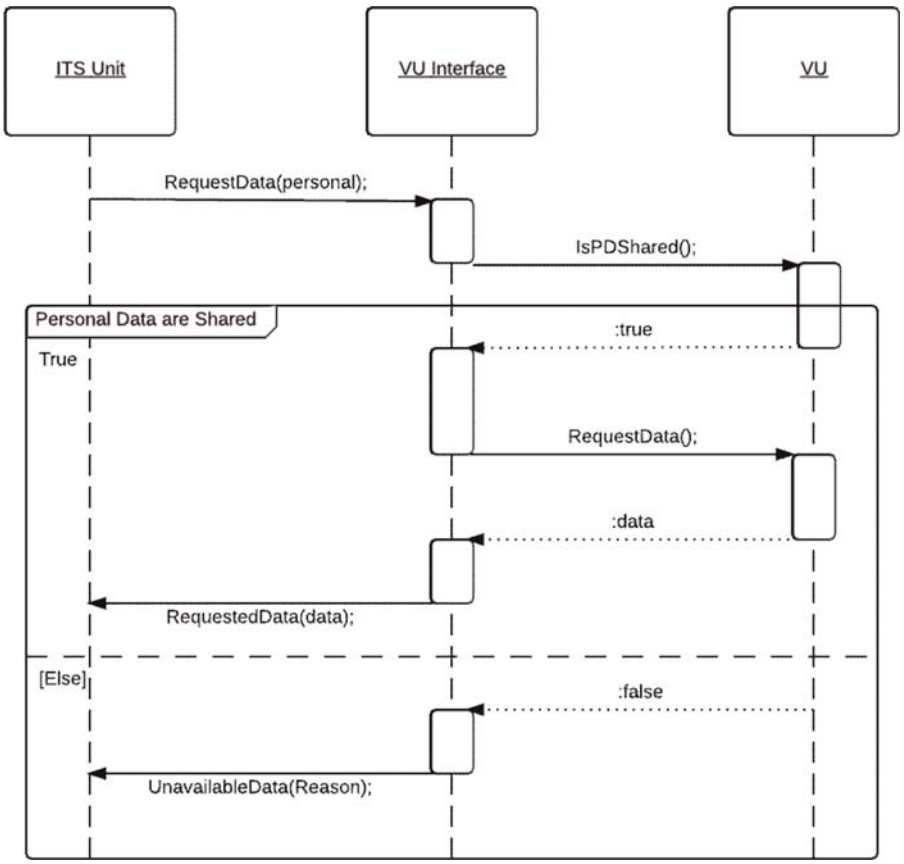
3. ábra

A nem személyesnek minősülő adatok (helyes PIN-hozzáférés utáni) feldolgozására vonatkozó kérés folyamatábrája



4. ábra

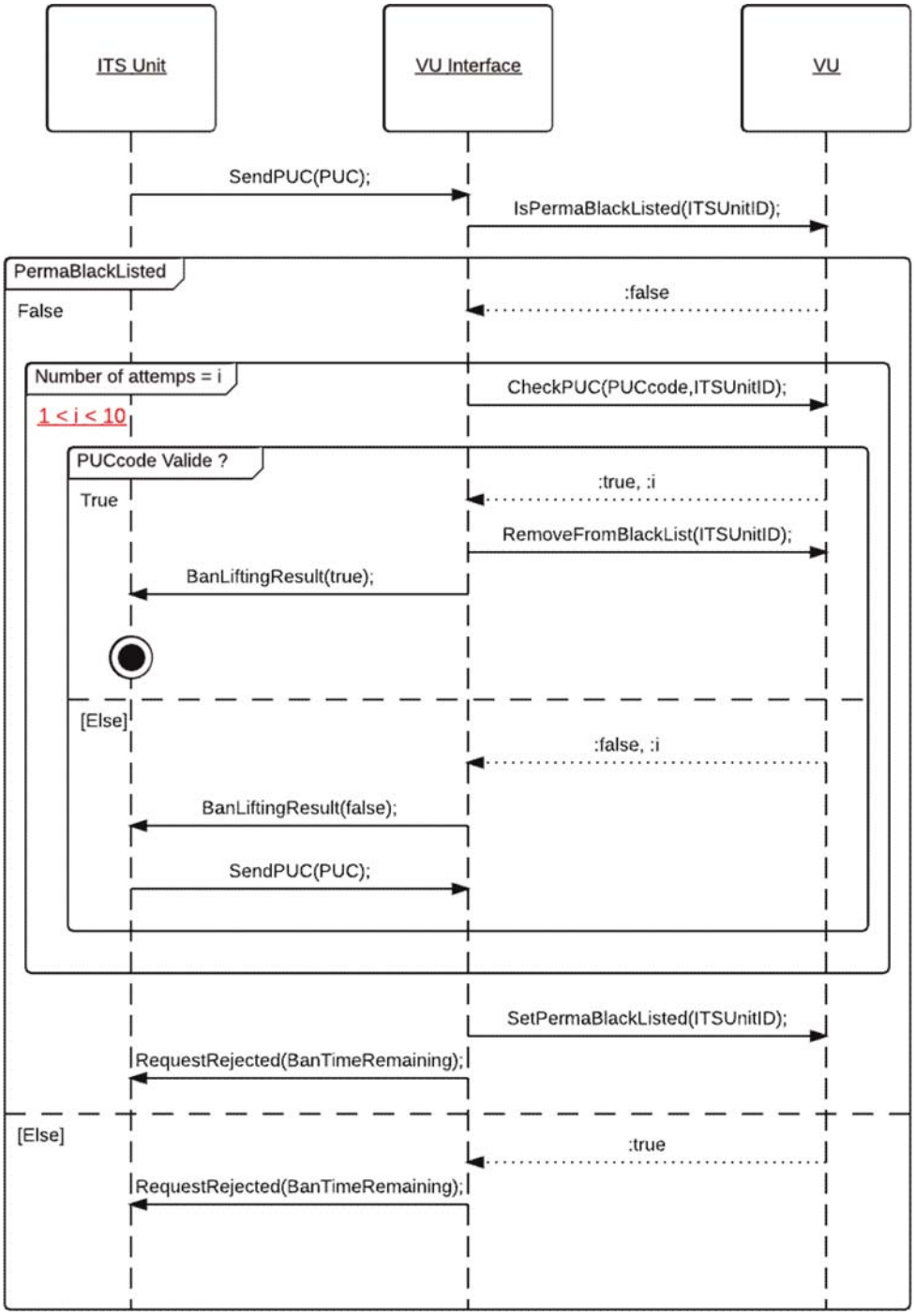
A személyesnek minősülő adatok (helyes PIN-hozzáférés utáni) feldolgozására vonatkozó kérés folyamatábrája



▼B

5. ábra

A PUC validálási kísérletének folyamatábrája



▼B

3. MELLÉKLET

ASN.1 SPECIFICATIONS

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

       CompleteMessage ::=SEQUENCE{
             header Header,
             data DataField,
             checksum Checksum
       }

       ----------------
       --HEADER TYPES--
       ----------------


       Header::=SEQUENCE{
             tgt IDList,
             src IDList,
             len BIT STRING (1..255)
       }

       vuID BIT STRING ::= 'EE'H
       IDList ::=CHOICE{
             vu BIT STRING (vuID),
             itsUnits SEQUENCE OF BIT STRING,
                   --Default hex Value:A0, redefined after first message exchange--
                   --Each ID will be linked to the Bluetooth ID of the device--
             ...
       }

       --------------------
       --DATAFIELDS TYPES--
       --------------------
       DataField ::=SEQUENCE{
             sid BIT STRING,
             trtp BIT STRING,
             subMBytes SubMessageBytes,
             dataField Content,
             ...
       }

       SubMessageBytes ::= SEQUENCE{
             currentSubM BIT STRING,
             totalSubM BIT STRING
       }

       Content ::= CHOICE{
             requestPIN RequestPIN,
             sendITSID SendITSID,
             sendPin SendPIN,
```

▼B

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

▼B

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      -------------------------
      --Messages From ITS Unit--
      -------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

▼B

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

▼B

```
Time ::= SEQUENCE{
       seconds INTEGER (0..59.75), --increment: 0.25s--
       minutes INTEGER (0..59), --increment: 1min--
       hours INTEGER (0..23), --increment: 1h--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       month INTEGER (1..12), --increment: 1month--
       year INTEGER (1985..2235), --increment: 1year--
       locMinOffset INTEGER (-59..59), --increment: 1min--
       locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
       month INTEGER (1..12), --increment: 1month--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
       codePageSurname UTF8String, --See ISO/IEC 8859--
       surname UTF8String,
       codePageFirstname UTF8String, --See ISO/IEC 8859--
       firstname UTF8String,
}

-------------------
--Message Content--
-------------------

StandardTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardTachData),
       personal BOOLEAN (FALSE),
       data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalTachData),
       personal BOOLEAN (TRUE),
       data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&gnssData),
       personal BOOLEAN (TRUE),
       data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardEventData),
       personal BOOLEAN (FALSE),
       data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalEventData),
       personal BOOLEAN (TRUE),
       data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

▼B

```
243                trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                personal BOOLEAN (FALSE),
245                data StandardFault
246          }
247
248          ManufacturerDataContent ::= SEQUENCE{
249                trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                personal BOOLEAN (TRUE),
251                ...
252          }
253
254          ---------------
255          --DATA SHEETS--
256          ---------------
257
258          --Data sheet format follows ISO 16844-7.--
259          StandardTachyDataSheet ::= SEQUENCE{
260                vin UTF8String (SIZE(17)),
261                calibrationDate Date,
262                driveRecognize INTEGER (2 UNION 12),
263                driverCardDriver1 INTEGER (2 UNION 12),
264                driverCardDriver2 INTEGER (2 UNION 12),
265                timeDate Time,
266                highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267    5m--
268                serviceComponentIdentification INTEGER (0..255),
269                serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270    -
271                nextCalibrationDate Date,
272                speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                outOfScopeCondition INTEGER(2 UNION 12),
276                modeOfOperation INTEGER (0..4...), --Maximum 250--
277                registeringMemberState UTF8String,
278          vehicleRegistrationNumber SEQUENCE {
279                      codePageVRN INTEGER (0..255),
280                      vrn OCTET STRING (SIZE(13)),
281                },
282                tachographNextMandatoryDownloadDate Date,
283                ...
284          }
285
286          PersonalTachyDataSheet ::= SEQUENCE{
287                tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289    UNION 1012...),
290                driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291    UNION 1012...),
292
293                driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294    1002 UNION
295                                                 1012 UNION 1102 UNION 1112 UNION
296    10002 UNION 10012 UNION
297                                                 10102 UNION 10112 UNION 11002 UNION
298    11012...),
299                driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300    1002 UNION
```

▼B

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

              overSpeed INTEGER (2 UNION 12),
              driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver1Name DriverName,
              driver2Name DriverName,
              driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
              driver1EndOfLastDailyRestPeriod Time,
              driver2EndOfLastDailyRestPeriod Time,
              driver1EndOfLastWeeklyRestPeriod Time,
              driver2EndOfLastWeeklyRestPeriod Time,
              driver1EndOfSecondLastWeeklyRestPeriod Time,
              driver2EndOfSecondLastWeeklyRestPeriod Time,
              driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1CardExpiryDate Date,
              driver2CardExpiryDate Date,
              driver1CardNextMandatoryDownloadDate Date,
              driver2CardNextMandatoryDownloadDate Date,
              driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
              driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
              driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

▼B

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367    1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369    1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385    END
386
387    EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390    about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408    CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410    AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

▼B

```
PersonalEvent ::= CHOICE{
      lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
      cardInsertionWhileDriving CardInsertionWhileDriving,
      overSpeeding OverSpeeding,
      ...
}

StandardFault ::= CHOICE{
      cardFault CardFault,
      recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
      date GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
```

▼B

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

▼B

14. függelék

TÁVOLI KOMMUNIKÁCIÓS FUNKCIÓ

TARTALOMJEGYZÉK

1 BEVEZETÉS

2 HATÁLY

3 BETŰSZAVAK, FOGALOMMEGHATÁROZÁSOK ÉS JELÖLÉSI MÓDOK

4 MŰKÖDÉSI FORGATÓKÖNYV

4.1 Áttekintés

4.1.1 Az 5,8 GHz-en működő DSRC interfészeken keresztül történő adatátvitel előfeltételei

4.1.2 1a. profil: kézi vagy ideiglenesen az út mentén felállított, irányított, korai távészleléssel történő kommunikációhoz használt leolvasó révén

4.1.3 1b. profil: járműbe beszerelt, irányított, korai távészleléssel történő kommunikációhoz használt leolvasó (REDCR) révén

4.2 Biztonság/sértetlenség

5 A TÁVOLI KOMMUNIKÁCIÓ KIALAKÍTÁSA ÉS A RÁ VONATKOZÓ PROTOKOLLOK

5.1 Kialakítás

5.2 Munkafolyamat

5.2.1 Műveletek

5.2.2 Az DSRC kommunikáció révén kapott adatok értelmezése

5.3 A DSRC fizikai interfész paraméterei a távoli kommunikációhoz

5.3.1 A helyre vonatkozó korlátozások

5.3.2 Feltöltési és letöltési paraméterek

5.3.3 Az antenna kialakítása

5.4 A DSRC protokoll RTM-re vonatkozó követelményei

5.4.1 Áttekintés

5.4.2 Parancsok

5.4.3 Lekérdezési parancssorozat

5.4.4 Adatstruktúrák

5.4.5 Az RtmData elemei, elvégzett műveletek és fogalommeghatározások

5.4.6 Adatátviteli mechanizmus

5.4.7 A DSRC tranzakció részletes leírása

5.4.8 A DSRC teszttranzakció leírása

5.5 A 2015/71/EK irányelv támogatása

5.5.1 Áttekintés

5.5.2 Parancsok

▼B

5.5.3 Lekérdezési parancssorozat

5.5.4 Adatstruktúrák

5.5.5 Az OWS DSRC tranzakcióra vonatkozó ASN.1 modul

5.5.6 Az OwsData elemei, elvégzett műveletek és fogalommeghatározások

5.5.7 Adatátviteli mechanizmusok

5.6 A DSRC-VU és a járműegység (VU) közötti adatátvitel

5.6.1 Fizikai kapcsolat és interfészek

5.6.2 Alkalmazási protokoll

5.7 Hibakezelés

5.7.1 Az adatok rögzítése és közlése az DSRC-VU-ban

5.7.2 A vezeték nélküli kommunikáció hibái

6 A TÁVOLI KOMMUNIKÁCIÓS FUNKCIÓ ÜZEMBE HELYEZÉSE ÉS IDŐSZAKOS VIZSGÁLATA

6.1 Általános rész

6.2 ECHO

6.3 A biztonsági adatok tartalmának érvényesítésére szolgáló tesztek

1 BEVEZETÉS

Ez a függelék azt a kialakítást és azokat az eljárásokat határozza meg, amelyeket a távoli kommunikációs funkciónak (a továbbiakban: kommunikáció) végrehajtásához követni kell a 165/2014/EU rendelet (a továbbiakban: rendelet) 9. cikkében előírtak szerint.

DSC_1 A 165/2014/EU rendelet előírja, hogy a menetíró készüléknek rendelkeznie kell olyan távoli kommunikációs funkcióval, amely lehetővé teszi az illetékes ellenőrző hatóságok meghatalmazottainak, hogy távoli lekérdező készülékkel (a korai távészleléssel történő kommunikációhoz használt leolvasóval [REDCR]), nevezetesen a CEN által az 5,8 GHz-en működő, speciális célú, rövid hatótávolságú adatátvitel (DSRC) területén közzétett szabványoknak megfelelő interfészek révén vezeték nélkül kapcsolódó lekérdező készülékkel kiolvassák a menetíró készülék információit az elhaladó járművekből.

Fontos megérteni, hogy ez a funkció csak előzetes szűrésre, azaz azoknak a járműveknek a kiválasztására szolgál, amelyeken alapos ellenőrzést kell végezni, és nem helyettesíti a 165/2014/EU rendelet rendelkezéseiben meghatározott hivatalos vizsgálati eljárást. Lásd az e rendelet preambulumában a (9) preambulumbekezdést, amely megállapítja, hogy a menetíró készülék és az ellenőrző hatóságok közötti, közúti ellenőrzés céljából folyó távoli kommunikáció elősegíti a célzott közúti ellenőrzéseket.

DSC_2 Az *adatok* cseréjét a *kommunikáció* keretében kell végrehajtani; a *kommunikációnak* 5,8 GHz-en folyó DSRC vezeték nélküli kommunikáció révén megvalósított vezeték nélküli kapcsolatnak kell lennie, amely megfelel ennek a mellékletnek, és amelyet az EN 300 674-1 szabvány {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short

▼B

Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)} megfelelő paraméterei szerint vizsgálnak.

DSC_3 *Kommunikációnak* a kommunikációs berendezéssel csak a megfelelő rádiókommunikációs eszközt [*korai távészleléssel történő kommunikációhoz használt leolvasót (REDCR)*] használó illetékes ellenőrző hatóság berendezés kérésére kell létrejönnie.

DSC_4 Az adatok sértetlenségének biztosítása érdekében az *adatoknak* biztonságosnak kell lenniük.

DSC_5 A továbbított *adatokhoz* csak az 561/2006/EK rendelet és a 165/2014/EU rendelet megsértésének ellenőrzésére felhatalmazott illetékes ellenőrző hatóságok, valamint a műhelyek férhetnek hozzá, de utóbbiak csak annyiban, amennyiben ez a menetíró készülék helyes működésének ellenőrzéséhez szükséges.

DSC_6 A *kommunikáció* során közölt *adatokat* az esetlegesen manipulált vagy nem megfelelően alkalmazott menetíró készülékkel rendelkező járművek célzott közúti ellenőrzéséhez szükséges adatokra kell korlátozni.

DSC_7 Az *adatok* sértetlenségét és biztonságát az adatok járműegységen (VU) belüli biztosításával, valamint azzal kell elérni, hogy csak a biztonságos hasznos adatokat és a biztonságra vonatkozó adatokat (lásd: 5.4.4) szabad az 5,8 GHz-es DSRC távoli kommunikációs eszközön keresztül továbbítani, ami azt jelenti, hogy csak az illetékes ellenőrző hatóságok arra jogosult személyzete rendelkezik a megfelelő eszközökkel ahhoz, hogy megértse a *kommunikáció* során továbbított adatokat, és ellenőrizze azok hitelességét. Lásd: 11. függelék Általános biztonsági mechanizmusok.

DSC_8 Az *adatoknak* tartalmazniuk kell a legutóbbi frissítésük időbélyegzőjét.

DSC_9 A biztonsági adatok tartalma kizárólag az illetékes ellenőrző hatóságok számára és ellenőrzésének keretében ismert, valamint azon felek számára, amelyekkel a hatóságok megosztják azt, továbbá kívül esik az e függelék tárgyát képező *kommunikációra* vonatkozó rendelkezéseken, eltekintve attól, hogy a *kommunikáció* keretében minden hasznosadat-csomaggal egy biztonságiadat-csomag is továbbításra kerül.

DSC_10 Ugyanannak az architektúrának és berendezésnek alkalmasnak kell lennie arra, hogy az itt meghatározott architektúra révén egyéb adatkoncepciókat (például a tömegadatok fedélzeti elérhetőségét) is megvalósítsanak.

DSC_11 Fontos tisztázni, hogy a 165/2014/EU rendelet 7. cikkének rendelkezéseivel összhangban a járművezető személyazonosságára vonatkozó adatok nem kerülnek továbbításra a *kommunikáció* keretében.

2 HATÁLY

E függelék hatálya annak meghatározására terjed ki, hogy az illetékes ellenőrző hatóságok meghatalmazottai meghatározott, 5,8 GHz-en folyó, vezeték nélküli DSRC kommunikáció révén miként szerzik meg azon *adatokat* egy célzott járműből, amelyek alapján eldönthető, hogy a

▼B

célzott jármű potenciálisan megsérti a 165/2014/EU rendeletet, és ezért fontolóra kell venni annak megállítását további vizsgálat céljából.

A 165/2014/EU rendelet előírja, hogy az összegyűjtött adatoknak azon adatokra kell korlátozódniuk, vagy azon adatokra kell vonatkozniuk, amelyek egy, a 165/2014/EU rendelet 9. cikkében meghatározott lehetséges jogsértést állapítanak meg.

E forgatókönyv szerint a kommunikációra rendelkezésre álló idő korlátozott, mivel a *kommunikáció* célzott és rövid hatótávolságú. Emellett az illetékes ellenőrző hatóságok a menetíró készülékek távoli ellenőrzésére (RTM) szolgáló, szóban forgó kommunikációs eszközt más alkalmazásokra is használhatják (például a nehéz tehergépjárműveknek a 2015/719/EK irányelvben meghatározott maximális tömegének és méreteinek ellenőrzésére), és az ilyen műveletek az illetékes ellenőrző hatóságok döntésétől függően lehetnek különállóak, vagy következhetnek egymás után.

Ez a függelék a következőt határozza meg:

— a kommunikációhoz használandó kommunikációs berendezések, eljárások és protokollok,

— azok a szabványok és előírások, amelyeknek a rádióberendezésnek meg kell felelnie,

— az *adatok* megjelenítése a *kommunikációs* berendezés számára,

— a lekérdezési és letöltési eljárások és a műveletek sorozata,

— a továbbítandó *adatok*,

— a *kommunikáció* keretében továbbított *adatok* esetleges értelmezése,

— a *kommunikációhoz* kapcsolódó biztonsági adatokra vonatkozó rendelkezések,

— az *adatok* rendelkezésre állása az illetékes ellenőrző hatóságok számára,

— a *korai távészleléssel történő kommunikációhoz használt leolvasó* miként kérhet le különböző rakomány- és flotta-adatkoncepciókat.

Fontos tisztázni, hogy ez függelék nem határozza meg a következőket:

— az *adat*gyűjtés működése és irányítása a járműegységben (VU) (ami a terméktervezés függvénye lesz, hacsak nincs meghatározva a 165/2014/EU rendelet egy másik helyén),

— az összegyűjtött adatok megjelenítési formája az illetékes ellenőrző hatóságok meghatalmazottja számára, vagy a kritériumok, amelyek alapján az illetékes ellenőrző hatóságok döntenek arról, hogy mely járműveket állítsák meg (ez a terméktervezés függvénye lesz, hacsak nincs meghatározva a 165/2014/EU rendelet egy másik helyén vagy az illetékes ellenőrző hatóságok szakpolitikai határozatában). Fontos tisztázni, hogy a *kommunikáció* csak annak érdekében bocsátja az *adatokat* az illetékes ellenőrző hatóságok rendelkezésére, hogy azok megalapozott döntéseket hozhassanak,

▼B

— az *adatok* tartalmára vonatkozó adatbiztonsági rendelkezések (például titkosítás) [amelyeket a 11. függelékben (Közös biztonsági mechanizmusok) kell meghatározni],

— az ugyanazzal az architektúrával és berendezéssel megszerezhető, az RTM-től eltérő adatkoncepciók részletei,

— a járműegységek (VU-k) és a DSRC-VU közötti magatartás és kezelés, vagy a DSRC-VU-n belüli magatartás (az *adatoknak* egy REDCR kérésére történő szolgáltatásán kívül).

3 BETŰSZAVAK, FOGALOMMEGHATÁROZÁSOK ÉS JELÖLÉSI MÓDOK

Ebben a függelékben a következő, erre a függelékre jellemző betűszavak és fogalommeghatározások szerepelnek:

antenna	Olyan elektromos berendezés, amely rádió-adóberendezéssel vagy rádió-vevőkészülékkel kombinálva az elektromos áramot rádióhullámokká alakítja, és fordítva. Működés közben a rádió-adóberendezés rádiófrekvencián rezgő elektromos áramot ad rá az antenna csatlakozókapcsaira, az antenna pedig elektromágneses hullámok (rádióhullámok) formájában sugározza szét az elektromos áram energiáját. Vételi üzemmódban az antenna fogja az elektromágneses hullám energiájának egy részét, parányi feszültség keletkezik a csatlakozókapcsokon, amelyet azután egy vevőkészülék felerősít.
kommunikáció	Információk/adatok cseréje a DSRC-REDCR és a DSRC-VU között mester-szolga kapcsolatban, a 5. szakasznak megfelelően, az adatok megszerzése érdekében.
adatok	Meghatározott formátumú (lásd: 5.4.4) biztonságos adatok, amelyeket a *DSRC-REDCR* kért le, és a *DSRC-VU* szolgáltatott a *DSRC-REDCR*-nek egy 5,8 GHz-en működő DSRC-kapcsolaton keresztül, az alábbi 5. pontban meghatározottak szerint.
165/2014/EU rendelet	Az Európai Parlament és a Tanács 2014. február 4-i 165/2014/EU rendelete a közúti közlekedésben használt menetíró készülékekről, a közúti

▼B

	közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendelet hatályon kívül helyezéséről és a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról szóló 561/2006/EK európai parlamenti és tanácsi rendelet módosításáról
AID	Alkalmazásazonosító
BLE	Alacsony energiafelhasználású Bluetooth-technológia
BST	Irányadó szolgáltatási táblázat
CIWD	Kártya behelyezése járművezetés közben
CRC	Ciklikus redundanciaellenőrzés
DSC (n)	meghatározott DRSC függelékre vonatkozó követelmény azonosítója
DSRC	Speciális célú, rövid hatótávolságú adatátvitel
DSRC-REDCR	DSRC – A korai távészleléssel történő kommunikációhoz használt leolvasó.
DSRC-VU	DSRC – Járműegység. Ez az 1C mellékletben meghatározott korai távészlelő eszköz.
DWVC	Érvényes kártya nélküli járművezetés
EID	Elemazonosító
LLC	Logikai kapcsolatvezérlés
LPDU	LLC Protokoll-adategység
OWS	Fedélzeti tömegmérő rendszer
PDU	Protokoll-adategység
REDCR	A korai távészleléssel történő kommunikációhoz használt leolvasó Ez az 1C mellékletben meghatározott, a korai távészleléssel történő kommunikációhoz használt leolvasó.
RTM	A menetíró készülékek távoli ellenőrzése
SM-REDCR	Biztonsági modul – A korai távészleléssel történő kommunikációhoz használt leolvasó
TARV	Telematikai alkalmazások a szabályozás hatálya alá tartozó járművekhez (ISO 15638 szabványsorozat)

▼B

VU	Járműegység
VUPM	A járműegység hasznos memóriája
VUSM	A járműegység biztonsági modulja
VST	Jármű szolgáltatási táblázata
WIM	Mozgó tömeg mérése
WOB	Fedélzeti tömegmérés

Az ebben a függelékben meghatározott előírás részben vagy egészben a következő rendeletekre és szabványokra utal, illetve azoktól függ. E függelék pontjai a vonatkozó szabványokra, illetve a szabványok vonatkozó szakaszaira hivatkoznak. Ellentmondás esetén e függelék pontjai elsőbbséget élveznek. Amennyiben – ellentmondás esetén – e függelék nem határozza meg egyértelműen az előírást, elsőbbséget élvez az ERC 70-03 ajánlásnak megfelelő működés (és az EN 300 674-1 szabványban meghatározott megfelelő paraméterek szerinti vizsgálat), amelyet csökkenő sorrendben az EN 12795, az EN 12253 és az EN 12834 szabvány, valamint az EN 13372 szabvány 6.2., 6.3., 6.4. és 7.1. szakasza követ.

Az e függelékben hivatkozott rendeletek és szabványok a következők:

[1] Az Európai Parlament és a Tanács 2014. február 4-i 165/2014/EU rendelete a közúti közlekedésben használt menetíró készülékekről, a közúti közlekedésben használt menetíró készülékekről szóló 3821/85/EGK tanácsi rendelet hatályon kívül helyezéséről és a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról szóló 561/2006/EK európai parlamenti és tanácsi rendelet módosításáról.

[2] Az Európai Parlament és a Tanács 2006. március 15-i 561/2006/EK rendelete a közúti szállításra vonatkozó egyes szociális jogszabályok összehangolásáról, a 3821/85/EGK és a 2135/98/EK tanácsi rendelet módosításáról, valamint a 3820/85/EGK tanácsi rendelet hatályon kívül helyezéséről (EGT-vonatkozású szöveg).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz.

▼B

[7] EN 12795 Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics – Dedicated short-range communication – Application layer.

[9] EN 13372 Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication

4 MŰKÖDÉSI FORGATÓKÖNYV

4.1 **Áttekintés**

A 165/2014/EU rendelet meghatározott és ellenőrzött forgatókönyveket határoz meg, amelyek keretében a *kommunikációt* alkalmazni kell.

A támogatott forgatókönyvek a következők:

„Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader”.

4.1.1 *Az 5,8 GHz-en működő DSRC interfészeken keresztül történő adatátvitel előfeltételei*

MEGJEGYZÉS: Az előfeltételek kontextusának megértéséhez lásd az alábbi 14.3. ábrát.

4.1.1.1 A járműegységben (VU) tárolt adatok

DSC_12 A járműegység (VU) feladata, hogy a DSRC kommunikációs funkció közreműködése nélkül 60 másodpercenként frissítse és karbantartsa a járműegységben (VU) tárolandó adatokat. Ennek megvalósítási módját, amely a járműegység (VU) részét képezi, nem ez a függelék, hanem a 165/2014/EU rendelet 1C mellékletének „*Távoli kommunikáció a célzott közúti ellenőrzések céljára*” című 3.19. szakasza határozza meg.

4.1.1.2 A DSRC-VU eszköznek biztosított adatok

DSC_13 A járműegység (VU) feladata, hogy a DSRC kommunikációs funkció közreműködése nélkül frissítse a DSRC tachográfadatokat (*adatok*), amint a járműegységben (VU) tárolt adatok a 4.1.1.1. pontban (DSC_12 szakasz) meghatározott időközönként frissítésre kerülnek.

DSC_14 A járműegység (VU) adatai alapján kell feltölteni és frissíteni az *adatokat*; ennek megvalósítási módját az 1C melléklet „*Távoli kommunikáció a célzott közúti ellenőrzések céljára*” című 3.19. szakasza határozza meg, vagy ha nem tartalmaz ilyen meghatározást, akkor az a terméktervezés függvénye, és nem ez a függelék határozza meg. A DSRC-VU eszköz és a járműegység (VU) közötti kapcsolat kialakítását lásd az 5.6. szakaszban.

▼B

4.1.1.3 Az adatok tartalma

DSC_15 Az *adatok* tartalmát és formáját úgy kell kialakítani, hogy titkosítás után strukturálni lehessen őket, és az e függelék 5.4.4. pontjában (Adatstruktúra) meghatározott formában és formátumban hozzáférhetővé lehessen őket tenni.

4.1.1.4 Az adatok megjelenítése

DSC_16 A 4.1.1.1. pontban meghatározott eljárásoknak megfelelően rendszeresen frissített *adatokat* a *DSRC-VU* számára történő megjelenítés előtt biztosítani kell, és biztonságos adatkoncepció-értékként kell az *adatok* aktuális verziójaként a *DSRC-VU*-ban való ideiglenes tároláshoz megjeleníteni. Ezek az adatok a *VUSM*-ből továbbításra kerülnek a DSRC *VUPM* funkciójához. A *VUSM* és a *VUPM* egyaránt funkció, és nem feltétlenül fizikai egységek. Az e funkciók végrehajtására szolgáló fizikai megvalósulások formája a terméktervezés függvénye, hacsak nincs meghatározva a 165/2014/EU rendelet egy másik helyén.

4.1.1.5 Biztonsági adatok

DSC_17 A biztonsági adatokat (*securityData*), beleértve a *REDCR* számára az *adatok* visszafejtésének elvégzéséhez szükséges adatokat a 11. függelékben (Közös biztonsági mechanizmusok) meghatározott módon kell biztosítani, és adatkoncepció-értékként kell a *securityData* aktuális verziójaként, az e függelék 5.4.4. pontjában meghatározott formában, a *DSRC-VU*-ban való ideiglenes tároláshoz megjeleníteni.

4.1.1.6 A DSRC interfészeken keresztül történő átvitelhez rendelkezésre álló VUPM adatok

DSC_18 Az ASN.1 modul teljes meghatározásához az 5.4.4. pontban található az adatkoncepció, amelynek a DSRC VUPM funkciójában mindig elérhetőnek kell lennie, hogy a *REDCR* kérésére azonnal továbbítani lehessen.

Az 1. kommunikációs profil általános áttekintése

Ez a profil arra a használati esetre vonatkozik, amikor az illetékes ellenőrző hatóságok meghatalmazottja rövid hatótávolságú adatátvitellel működő, korai távészleléssel történő kommunikációhoz használt leolvasóval (*REDCR*) (amely az 5. pontban leírtak szerint az ERC 70-03 ajánlásnak megfelelően működik, és amelyet az EN 300 674-1 szabványban meghatározott megfelelő paraméterek szerint vizsgálnak) távolról azonosít olyan járművet, amely potenciálisan megsérti a 165/2014/EU rendeletet. A jármű azonosítása után az illetékes ellenőrző hatóságok lekérdezést ellenőrző meghatalmazottja dönt arról, hogy a járművet leállítsák-e, vagy sem.

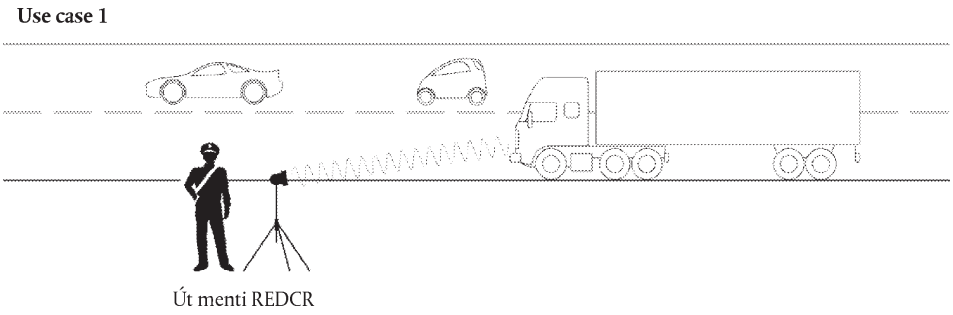
4.1.2 *1a. profil: kézi vagy ideiglenesen az út mentén felállított, irányított, korai távészleléssel történő kommunikációhoz használt leolvasó révén*

Ebben az esetben az illetékes ellenőrző hatóságok meghatalmazottja az út mentén helyezkedik el, és az út széléről a megcélzott jármű szélvédőjének közepe felé irányít egy háromlábú állványra szerelt kézi vagy hasonló hordozható *REDCR*-t. A lekérdezés 5,8 GHz-en működő DSRC interfészek révén történik, amelyek az 5. pontban leírtak szerint az ERC 70-03 ajánlásnak megfelelően működnek, és amelyeket az EN 300 674-1 szabványban meghatározott megfelelő paraméterek szerint vizsgálnak. Lásd a 14.1. ábrát (1. használati eset).

▼B

14.1. ábra

Út menti lekérdezés 5,8 GHz-es DSRC segítségével

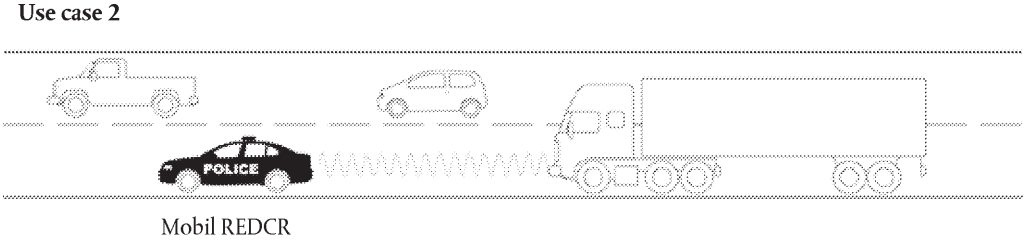


4.1.3 *1b. profil: járműbe beszerelt, irányított, korai távészleléssel történő kommunikációhoz használt leolvasó (REDCR) révén*

Ebben az esetben az illetékes ellenőrző hatóságok meghatalmazottja egy mozgó járműben helyezkedik el, és vagy a járműből egy kézi, hordozható *REDCR*-t irányít a megcélzott jármű szélvédőjének közepe felé, vagy az *REDCR* úgy van a járműbe beszerelve vagy arra felszerelve, hogy a megcélzott jármű szélvédőjének közepe felé irányuljon, amikor a korai távészleléssel történő kommunikációhoz használt leolvasó járműve meghatározott helyzetben van a megcélzott járműhöz képest (például közvetlenül előtte van a forgalomban). A lekérdezés 5,8 GHz-en működő DSRC interfészek révén történik, amelyek az 5. pontban leírtak szerint az ERC 70-03 ajánlásnak megfelelően működnek, és amelyeket az EN 300 674-1 szabványban meghatározott megfelelő paraméterek szerint vizsgálnak. Lásd a 14.2. ábrát (2. használati eset).

14.2. ábra

Járműből történő lekérdezés 5,8 GHz-es DSRC segítségével



4.2 **Biztonság/sértetlenség**

Annak érdekében, hogy a távoli kommunikáció révén letöltött adatok hitelességét és sértetlenségét ellenőrizni lehessen, a biztonságos *adatokat* a 11. függelékkel (Közös biztonsági mechanizmusok) összhangban kell ellenőrizni és visszafejteni.

5 A TÁVOLI KOMMUNIKÁCIÓ KIALAKÍTÁSA ÉS A RÁ VONATKOZÓ PROTOKOLLOK

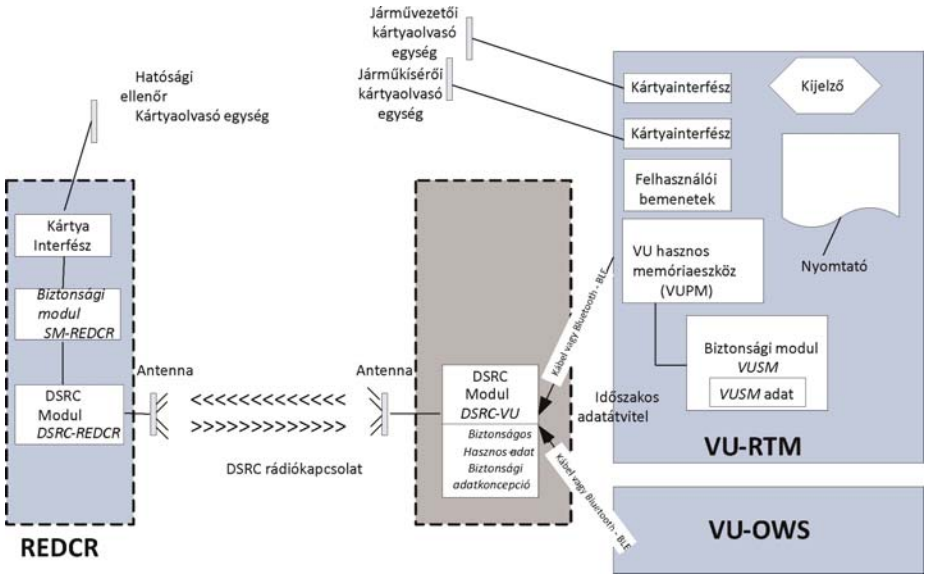
5.1 **Kialakítás**

Az intelligens menetíró készülék távoli kommunikációs funkciójának kialakítását a 14.3. ábra mutatja be.

▼B

14.3. ábra

A távoli kommunikációs funkció kialakítása



DSC_19 A következő funkciók a járműegységben (VU) valósulnak meg:

— biztonsági modul (*VUSM*). Ennek a járműegységben (VU) megvalósuló funkciónak a feladata az *adatok* biztosítása, amelyeket a *DSRC-VU*-nak távoli kommunikációval továbbítania kell az illetékes ellenőrző hatóságok meghatalmazottja számára,

— a biztonságos adatokat a VUSM memória tárolja. A 4.1.1.1. pontban (DSC_12) meghatározott időközönként a járműegység (VU) titkosítja és feltölti a DSRC-VU memóriájában tárolt RTMdatakoncepciót (amely az ebben a függelékben meghatározott hasznosadat-koncepciók és biztonságiadat-koncepciók értékeit foglalja magában). A biztonsági modul működése, amelyet a 11. függelék (Közös biztonsági mechanizmusok) határoz meg, kívül esik e függelék hatályán, eltekintve attól, hogy minden alkalommal, amikor a VUSM adatok változnak, naprakész adatokat kell szolgáltatnia a járműegység (VU) kommunikációs eszközének,

— a járműegység (VU) és a DSRC-VU közötti kommunikáció folyhat vezetéken vagy alacsony energiafelhasználású Bluetooth-technológiával (BLE), és a DSRC-VU fizikai elhelyezkedését illetően össze lehet építve az antennával a jármű szélvédőjén, lehet a járműegység (VU) belsejében, vagy valahol a kettő között,

— a DSRC-VU-nak rendelkeznie kell egy megbízható energiaforrással, amely mindenkor rendelkezésre áll. Az energiával való ellátás módja tervezési kérdés,

— a DSRC-VU memóriájának maradandó memóriának kell lennie annak érdekében, hogy a DSRC-VU akkor is megőrizze az adatokat, amikor a jármű gyújtása ki van kapcsolva,

— ha a járműegység (VU) és a DSRC-VU között a kommunikáció BLE-n keresztül történik, és az áramforrás egy nem tölthető elem, akkor a DSRC-VU áramforrását minden egyes időszakos vizsgálat alkalmával ki kell cserélni, és

▼B

a DSRC-VU berendezés gyártójának felelőssége azt biztosítani, hogy a tápegység kitartson az egyik időszakos vizsgálattól a következő időszakos vizsgálatig úgy, hogy az adatokhoz a teljes időtartam alatt hiba nélküli, illetve folyamatos, rendes hozzáférést biztosít egy REDCR számára,

— a VU RTM „hasznos memóriája” (*VUPM*). Ennek a járműegységben (VU) megvalósuló funkciónak a feladata rendelkezésre bocsátani, illetve frissíteni az *adatokat*. Az *adatok* („TachographPayload”) tartalma, amelyet az alábbi 5.4.4./5.4.5. pont határoz meg, a 4.1.1.1. pontban (DSC_12 szakasz) meghatározott időközönként kerül frissítésre,

— DSRC-VU. Ez a funkció, amely az antennán belül vagy ahhoz kapcsolódva és a járműegységgel (VU) vezetékes vagy vezeték nélküli (BLE) kapcsolat révén folyó kommunikáció keretében valósul meg, tárolja az aktuális adatokat (*VUPM-adatok*), és kezeli a 5,8 GHz-es DSRC eszközzel történő lekérdezésre adott választ. A DSRC eszköz lekapcsolása vagy a jármű rendes működése során a DSRC eszköz működésének befolyásolása a 165/2014/EU rendelet megsértésének minősül.

— A biztonsági modul (REDCR) (*SM-REDCR*) a járműegységből (VU) származó adatok visszafejtésére és sértetlenségük ellenőrzésére szolgáló funkció. Ennek megvalósítási módját nem ez a függelék, hanem a 11. függelék (Közös biztonsági mechanizmusok) határozza meg.

— A DSRC-eszköz (REDCR) (*DSRC-REDCR*) magában foglal egy 5,8 GHz-es adó-vevőt, valamint az azzal összefüggő firmware-t és szoftvert, amelyek a *DSRC-VU*-val folyó *kommunikációt* bonyolítják le e függeléknek megfelelően.

— A *DSRC-REDCR* lekérdezi a megcélzott jármű *DSRC-VU*-ját, megszerzi az *adatokat* (a megcélzott jármű aktuális *VUPM-adatait*) a DSRC-kapcsolaton keresztül, valamint feldolgozza a kapott adatokat, és eltárolja azokat az *SM-REDCR*-ben.

— A *DSRC-VU* antennáját (az antenna) úgy kell elhelyezni (általában a jármű szélvédőjének közepén vagy annak közelében…), hogy optimális legyen a DSRC kommunikáció a jármű és az út menti antenna között. Könnyű gépjárművek esetében a szélvédő felső részére eső beszerelés a megfelelő.

— Az antenna előtt vagy annak közelében nem lehetnek fém tárgyak (pl. névtáblák, matricák, fényvisszaverődés-gátló (színezett) fóliaszalagok, napellenzők, nyugalmi állapotban lévő ablaktörlő), amelyek zavarhatják a kommunikációt.

— Az antennát úgy kell felszerelni, hogy célzókészüléke megközelítőleg párhuzamos legyen az útfelülettel.

▼B

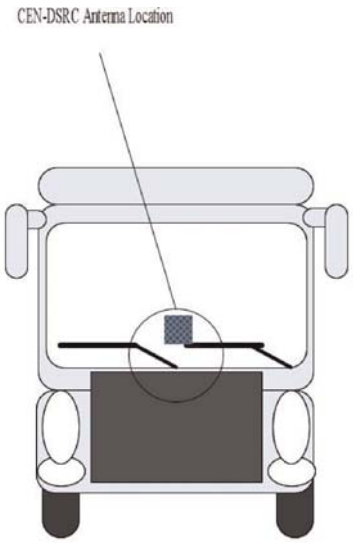
DSC_20 Az antennát és a kommunikációt, amelyeknek az 5. pontban leírtak szerint az ERC 70-03 ajánlásnak megfelelően kell működniük, az EN 300 674-1 szabványban meghatározott megfelelő paraméterek szerint kell vizsgálni. Az antenna és a kommunikáció az Elektronikus Hírközlési Bizottság (Electronic Communications Committee, ECC) 228. számú jelentésében leírt technikákat, pl. szűrőket alkalmazhatnak az interferencia kockázata ellen a CEN által az 5,8 GHz-en működő, speciális célú, rövid hatótávolságú adatátvitel (DSRC) területén közzétett szabványoknak megfelelő kommunikációban.

DSC_21 A DSRC-antennát vagy közvetlenül a szélvédőre vagy annak közelében felszerelt modulon belül, vagy egy külön erre a célra szolgáló, olyan kábelen keresztül kell csatlakoztatni a DSRC-VU-hoz, amely úgy van kialakítva, hogy megnehezítse az illegális szétkapcsolást. A lekapcsolás vagy az antenna működésének befolyásolása a 165/2014/EU rendelet megsértésének minősül. Az antenna takarása vagy működési teljesítményének más módon történő kedvezőtlen befolyásolása a 165/2014/EU rendelet megsértésének minősül.

DSC_22 Az antenna alakényezője nincs meghatározva, ez kereskedelmi döntés lesz kell mindaddig, amíg a beszerelt DSRC-VU megfelel az alábbi 5. szakaszban meghatározott megfelelőségi követelményeknek. Az antennának, amelyet a DSC_19 szakaszban meghatározott és a 14.4. ábrán bemutatott módon (ovális vonal) kell elhelyezni, hatékonyan támogatnia kell a 4.1.2. és a 4.1.3. pontban leírt használati eseteket.

14.4. ábra

Példa arra, hogy hogyan kell elhelyezni az 5,8 GHz-es DSRC antennát a rendelet hatálya alá tartozó járművek szélvédője mögött



Az *REDCR* és antennájának alakényezője a leolvasó körülményeitől (háromlábú állványra szerelt, kézi, járműbe beszerelt stb. leolvasó) és az illetékes ellenőrző hatóságok meghatalmazottja által alkalmazott eljárásmódtól függően változhat.

A kijelző és/vagy értesítési funkció arra szolgál, hogy a távoli kommunikációs funkció eredményeit bemutassa az illetékes ellenőrző hatóságok meghatalmazottjának. A kijelzés történhet képernyőn, kinyomatként, hangjelzésként vagy az ilyen értesítések kombinációjaként. A kijelzés és/vagy értesítés formája az illetékes ellenőrző hatóságok meghatalmazottjai és a berendezés kialakítása által meghatározott követelmények függvénye, és nem ez a függelék határozza meg.

▼B

DSC_23 Az *REDCR*-nek, amelynek kialakítása és alaktényezője a kereskedelmi tervezés függvénye, az ERC 70-03 ajánlásnak megfelelően kell működnie, továbbá meg kell felelnie az e függelékben (5.3.2. szakasz) meghatározott tervezési és teljesítmény-előírásoknak, így biztosítva a lehető legnagyobb mértékű rugalmasságot a piac számára ahhoz, hogy minden illetékes ellenőrző hatóság konkrét lekérdezési forgatókönyvének megfelelő berendezést lehessen tervezni és biztosítani.

DSC_24 A *DSRC-VU*-nak, amelynek kialakítása és alaktényezője, valamint járműegységen (VU) belül vagy kívül való elhelyezése a kereskedelmi tervezés függvénye, az ERC 70-03 ajánlásnak megfelelően kell működnie, továbbá meg kell felelnie az e függelékben (5.3.2. pont) és az ebben az 5.1. pontban meghatározott tervezési és teljesítmény-előírásoknak.

DSC_25 A *DSRC-VU*-nak azonban ésszerű mértékben alkalmasnak kell lennie arra, hogy nyílt iparági szabványon alapuló kapcsolat és protokollok révén más intelligens járműberendezések (például a járművek tömegének fedélzeti mérésére szolgáló berendezések) adatkoncepció-értékeit is fogadják, amennyiben az ilyen adatkoncepciókat egyedi és ismert alkalmazásazonosítók/fájlnevek azonosítják, valamint a protokollok alkalmazására vonatkozó utasításokat az Európai Bizottság rendelkezésére bocsátják, és ingyenesen elérhetővé teszik a megfelelő berendezések gyártói számára.

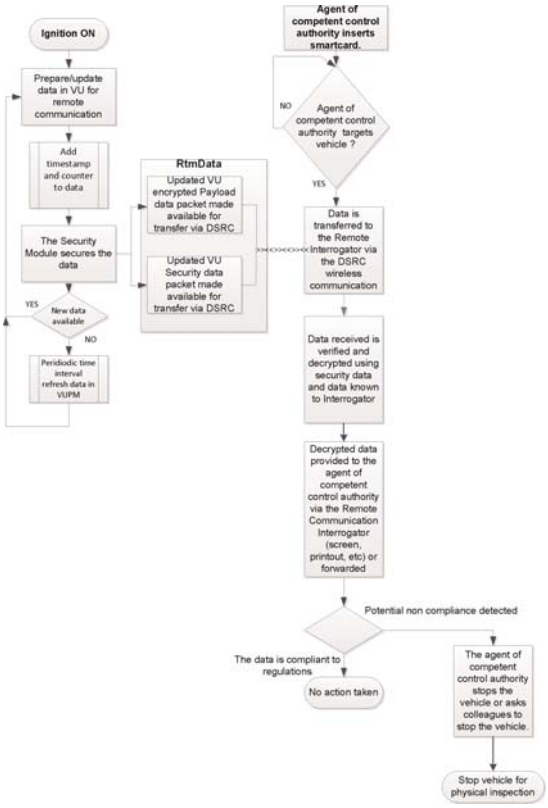
5.2 **Munkafolyamat**

5.2.1 *Műveletek*

A műveletek folyamatát a 14.5. ábra mutatja be.

14.5. ábra

A távoli kommunikációs funkció munkafolyamata



▼B

A lépések leírása a következő:

a. Amikor a jármű működik (a gyújtás be van kapcsolva) a menetíró készülék adatokat szolgáltat a VU funkciónak. A VU funkció előkészíti az *adatokat* a (titkosított) távoli kommunikációs funkció számára, és (a 4.1.1.1–4.1.1.2. pontban meghatározott módon) frissíti a *DSRC-VU* memóriájában tárolt *VUPM*-et. Az összegyűjtött *adatokat* az alábbi 5.4.4–5.4.5. pontban meghatározott módon kell formázni.

b. Minden alkalommal, amikor az *adatok* frissülnek, a biztonságiadat-koncepcióban meghatározott időbélyegzőt is frissíteni kell.

c. A *VUSM* funkció a 11. függelékben meghatározott eljárásokkal összhangban biztosítja az adatokat.

d. Minden alkalommal, amikor az *adatok* frissülnek (lásd a 4.1.1.1–4.1.1.2. szakaszt), az *adatokat* továbbítani kell a *DSRC-VU*-nak, ahol felülírják a korábbi adatokat annak érdekében, hogy mindig frissített aktuális adatok álljanak rendelkezésre továbbításra egy *REDCR* általi lekérdezés esetén. Amikor a járműegység (VU) elküldi az *adatokat* a DSRC-VU-nak, azoknak azonosíthatónak kell lenniük az *RTMData* fájlnév vagy az ApplicationID és az Attribute azonosítók révén.

e. Ha az illetékes ellenőrző hatóságok egy meghatalmazottja egy adott járművet kíván megcélozni, és a megcélzott járműből begyűjteni az *adatokat*, az illetékes ellenőrző hatóságok meghatalmazottjának először be kell helyeznie az intelligens kártyáját az *REDCR*-be, hogy létrejöhessen a *kommunikáció*, és az *SM-REDCR* ellenőrizhesse a kártya hitelességét, és visszafejtse az adatokat.

f. Az illetékes ellenőrző hatóságok meghatalmazottja ezután megcélozza a járművet, és távoli kommunikáció keretében lekéri az adatokat. Az *REDCR* 5,8 GHz-en működő DSRC interfészen keresztül munkamenetet nyit a megcélzott jármű *DSRC-VU* egységével, és lekéri az *adatokat*. Az *adatok* az 5.4. pontban meghatározott módon az alkalmazás GET szolgáltatását használó DSRC Attribútumként továbbításra kerül az *REDCR* számára a vezeték nélküli kommunikációs rendszeren keresztül. Az Attribútum tartalmazza a titkosított hasznos adatokat és a DSRC biztonsági adatokat.

g. Az adatokat a *REDCR* berendezés elemzi, és biztosítja az illetékes ellenőrző hatóságok meghatalmazottja számára.

h. Az illetékes ellenőrző hatóság meghatalmazottja az adatok alapján dönt arról, hogy megállítsa-e a járművet részletes vizsgálat céljából, vagy sem, vagy megkérje-e az illetékes ellenőrző hatóság egy másik meghatalmazottját, hogy állítsa meg a járművet.

5.2.2 *Az DSRC kommunikáció révén kapott adatok értelmezése*

DSC_26 Az 5,8 GHz-en működő interfészen keresztül kapott adatok jelentésének és importjának az alábbi, 5.4.4. és 5.4.5. pontban meghatározott jelentésre és importra kell korlátozódniuk, és az ott meghatározott célok keretében kell őket értelmezni. A 165/2014/EU rendelet rendelkezéseinek megfelelően az *adatok* csak arra használhatók fel, hogy olyan megfelelő információval szolgáljanak az illetékes ellenőrző hatóság

▼B

számára, amely segítséget nyújt a hatóságnak annak eldöntésében, hogy mely járművet állítsa meg fizikai vizsgálat céljából, ezután az *adatokat* az 165/2014/EU rendelet 9. cikkével összhangban meg kell semmisíteni.

5.3 **A DSRC fizikai interfész paraméterei a távoli kommunikációhoz**

5.3.1 *A helyre vonatkozó korlátozások*

DSC_27 A járművek 5,8 GHz-en működő DSRC interfészen keresztül történő távoli lekérdezése nem alkalmazható működő 5,8 GHz-es DSRC kapu 200 méteres körzetén belül.

5.3.2 *Feltöltési és letöltési paraméterek*

DSC_28 A menetíró készülékek távoli ellenőrzésére alkalmazott berendezésnek meg kell felelnie az ERC 70-03 ajánlásnak, ezenkívül az említett ajánlás és az alábbi 14.1. és 14.2. táblázatban meghatározott paramétereknek megfelelően kell működnie.

DSC_29 Továbbá az egyéb szabványosított, 5,8 GHz-en működő DSRC rendszerek működési paramétereivel való kompatibilitás biztosítása érdekében, a menetíró készülékek távoli ellenőrzésére alkalmazott berendezésnek meg kell felelnie az EN 12253 és az EN 13372 szabvány paramétereinek.

Ezek a következők:

▼C2

14.1. táblázat

Letöltési paraméterek

Tétel	Paraméter	Érték(ek)	Megjegyzés
D1	Letöltési vivőjel-frekvenciák	Egy REDCR négy lehetséges frekvenciát alkalmazhat: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Az ERC 70-03 ajánlásnak megfelelően. A vivőjel-frekvenciákat megválaszthatja a közúti rendszert megvalósító fél, azokat a DSRC-VU szintjén nem kell ismerni. (Összhangban az EN 12253 és az EN 13372 szabvánnyal)
D1a (*)	A vivőjel-frekvenciák tűrése	± 5 ppm	(Összhangban az EN 12253 szabványnyal)
D2 (*)	Az RSU (REDCR) adóberendezés spektrummaszkja	Az ERC 70-03 ajánlásnak megfelelően. Az REDCR-nek meg kell felelnie az EN 12253 szabványban meghatározott B, C osztálynak. Ez a melléklet nem ír elő egyéb konkrét követelményt	Az egymáshoz közel elhelyezkedő lekérdezők közötti interferencia korlátozására szolgáló paraméter (az EN 12253 és az EN 13372 szabvány meghatározása szerint).
D3	Az OBU (DSRC-VU) minimális frekvenciatartománya	5,795–5,815 GHz	(Összhangban az EN 12253 szabványnyal)
D4 (*)	Maximális E.I.R.P.	Az ERC 70-03 ajánlásnak (engedélymentes) és a nemzeti szabályozásnak megfelelően. Maximum + 33 dBm	(Összhangban az EN 12253 szabványnyal)

▼C2

Tétel	Paraméter	Érték(ek)	Megjegyzés
D4a	EIRP szögmaszk	A lekérdezőegység tervezője által megadott és közzétett specifikáció szerint	(Összhangban az EN 12253 szabvánnyal)
D5	Polarizáció	Órával ellentétes irányú, körkörös	(Összhangban az EN 12253 szabvánnyal)
D5a	Keresztpolarizáció	XPD: Az irányzóvonalban: (REDCR) RSU t ≥ 15 Db (DSRC-VU) OBU r ≥ 10 dB A – 3 dB zónában: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(Összhangban az EN 12253 szabvánnyal)
D6 (*)	Moduláció	Kétszintű amplitúdómoduláció	(Összhangban az EN 12253 szabvánnyal)
D6a (*)	Modulációs index	0,5 … 0,9	(Összhangban az EN 12253 szabvánnyal)
D6b	Szemábra	≥ 90 % (idő)/≥ 85 % (amplitúdó)	
D7 (*)	Adatkódolás	FM0 Az „1” bit csak a bitintervallum elején és végén tartalmaz jelváltást. Az „1” bithez képest a „0” bit egy további jelváltást tartalmaz a bitintervallum közepén.	(Összhangban az EN 12253 szabvánnyal)
D8 (*)	Átviteli sebesség	500 kBit/s	(Összhangban az EN 12253 szabvánnyal)
D8a	A bitóra tűrése	± 100 ppm-nél jobb	(Összhangban az EN 12253 szabvánnyal)
D9 (*)	Bithibaarány (BER) kommunikáció esetében	$\leq 10^{-6}$ ha az OBU-nál (DSRC-VU) a beeső teljesítmény a [D11a–D11b] pont által meghatározott tartományba esik.	(Összhangban az EN 12253 szabvánnyal)
D10	Az OBU-t (DSRC-VU) felélesztő jel	Az OBU-nak (DSRC-VU) fel kell élednie, ha 11 vagy több oktettet tartalmazó keretet kap (a bevezetőt is beleértve)	Különleges felélesztési mintára nincs szükség. A DSRC-VU feléledhet, ha 11-nél kevesebb oktettet tartalmazó keretet kap (Összhangban az EN 12253 szabvánnyal)
D10a	Maximális kezdési idő	≤ 5 ms	(Összhangban az EN 12253 szabvánnyal)
D11	Kommunikációs zóna	Olyan térbeli zóna, amelyben a D9a szerinti BER elérhető	(Összhangban az EN 12253 szabvánnyal)
D11a (*)	Teljesítmény (felső) határa kommunikáció esetében.	– 24 dBm	(Összhangban az EN 12253 szabvánnyal)

▼C2

Tétel	Paraméter	Érték(ek)	Megjegyzés
D11b (*)	Teljesítmény (alsó) határa kommunikáció esetében.	Beeső teljesítmény: – 43 dBm (irányzóvonal) – 41 dBm (– 45° és + 45° között, ami az út felületével párhuzamos síknak felel meg, ha a DSRC-VU-t később szerelik be a járműbe (Azimuth))	(Összhangban az EN 12253 szabvánnyal) Megnövelt követelmény a vízszintes szögek esetében (± 45°-ig) az e mellékletben meghatározott használati esetek miatt.
D12 (*)	A (DSRC-VU) levágási teljesítményszintje	– 60 dBm	(Összhangban az EN 12253 szabvánnyal)
D13	Bevezető	A bevezető kötelező.	(Összhangban az EN 12253 szabvánnyal)
D13a	A bevezető hossza és szerkezete	16 bit ± 1 FM0-kódolású „1” bit	(Összhangban az EN 12253 szabvánnyal)
D13b	Bevezető hullámforma	Az alacsony és a magas szint egymás után váltakozó sorozata, ahol az impulzus hossza 2 μs. A tűrést a D8a adja meg.	(Összhangban az EN 12253 szabvánnyal)
D13c	Követő bitek	Az RSU (REDCR) maximum 8 bitet továbbíthat a vége jelölő után. Az OBU (DSRC-VU) ezeket a további biteket nem köteles figyelembe venni.	(Összhangban az EN 12253 szabvánnyal

(*) – Ezeken a letöltési paramétereken megfelelőségi vizsgálatokat kell végezni az EN 300 674-1 szabványban előírt megfelelő paramétervizsgálatnak megfelelően.

14.2. táblázat

Feltöltési paraméterek

Tétel	Paraméter	Érték(ek)	Megjegyzés
U1 (*)	Segédvivőjel-frekvenciák	Az OBU-nak (DSRC-VU) 1,5 MHz-en és 2,0 MHz-en kell működnie. Az RSU-nak (REDCR) 1,5 MHz-en vagy 2,0 MHz-en vagy mindkettőn kell működnie. U1-0: 1,5 MHz U1-1: 2,0 MHz	A segédvivőjel-frekvencia kiválasztása (1,5 MHz vagy 2,0 MHz) a kiválasztott, EN 13372 szabvány szerinti profiltól függ.
U1a (*)	A segédvivőjel-frekvenciák tűrése	± 0,1 %	(Összhangban az EN 12253 szabvánnyal)
U1b	Oldalsávok alkalmazása	Mindkét oldalon azonos adat	(Összhangban az EN 12253 szabvánnyal)
U2 (*)	Az OBU (DSRC-VU) adóberendezés spektrummaszkja	Az EN 12253 szabvány szerint 1) Sávon kívüli teljesítmény: lásd: ETSI EN 300674-1	(Összhangban az EN 12253 szabvánnyal)

▼C2

Tétel	Paraméter	Érték(ek)	Megjegyzés
		2) Sávon belüli teljesítmény: [U4a] dBm 500 kHz-en 3) Kibocsátás más feltöltési csatornán: U2(3)-1 = – 35 dBm 500 kHz-en	
U4a (*)	Egy oldalsáv maximális EIRP-je (irányzóvonal)	Két lehetőség: U4a-0: – 14 dBm U4a-1: – 21 dBm	A berendezés tervezője által megadott és közzétett specifikáció szerint
U4b (*)	Egy oldalsáv maximális EIRP-je (35°)	Két lehetőség: — Nem alkalmazható — – 17 dBm	A berendezés tervezője által megadott és közzétett specifikáció szerint
U5	Polarizáció	Órával ellentétes irányú, körkörös	(Összhangban az EN 12253 szabvánnyal)
U5a	Keresztpolarizáció	XPD: Az irányzóvonalban: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB A – 3 dB zónában: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(Összhangban az EN 12253 szabvánnyal)
U6	Segédvivőjel-moduláció	2-PSK A segédvivőjellel szinkronizált kódolt adatok: A kódolt adatok váltásai egybeesnek a segédvivőjel jelváltásaival.	(Összhangban az EN 12253 szabvánnyal)
U6b	Működési periódus	Működési periódus 50 % ± α, α ≤ 5 %	(Összhangban az EN 12253 szabvánnyal)
U6c	Vivőjel-moduláció	A modulált segédvivőjel szorzása a vivőjellel.	(Összhangban az EN 12253 szabvánnyal)
U7 (*)	Adatkódolás	NRZI (Nincs jelváltás az „1” bit elején, van jelváltás a „0” bit elején, nincs jelváltás a biten belül)	(Összhangban az EN 12253 szabvánnyal)
U8 (*)	Átviteli sebesség	250 kbit/s	(Összhangban az EN 12253 szabvánnyal)
U8a	A bitóra tűrése	± 1 000 ppm	(Összhangban az EN 12253 szabvánnyal)
U9	Bithibaarány (BER) kommunikáció esetében	$\leq 10^{-6}$	(Összhangban az EN 12253 szabvánnyal)

▼C2

Tétel	Paraméter	Érték(ek)	Megjegyzés
U11	Kommunikációs zóna	Az a térbeli zóna, amelyben a DSRC-VU úgy helyezkedik el, hogy átvitelét az REDCR az U9a pontban megadottnál kisebb BER-érték mellett fogadja.	(Összhangban az EN 12253 szabvánnyal)
U12a (*)	Átalakítási nyereség (alsó határ)	1 dB mindkét oldalsáv esetében Szögtartomány: Körkörösen szimmetrikus az irányzóvonal és ± 35° között, valamint – 45° és + 45° között, ami az út felületével párhuzamos síknak felel meg, ha a DSRC-VU-t később szerelik be a járműbe (Azimuth))	Nagyobb, mint a vízszintes szögekre vonatkozóan (± 45°-ig) megadott értéktartomány az e mellékletben meghatározott használati esetek miatt.
U12b (*)	Átalakítási nyereség (felső határ)	10 dB mindkét oldalsáv esetében	Kisebb, mint a két oldalsávra vonatkozóan megadott értéktartomány az irányzóvonal körül elképzelt ± 45° nyílásszögű kúpon belül
U13	Bevezető	A bevezető kötelező.	(Összhangban az EN 12253 szabvánnyal)
U13a	Bevezető Hossza és szerkezete	32–36 μs csak a segédvivőjellel modulálva, majd 8 NRZI-kódolású „0” bit.	(Összhangban az EN 12253 szabvánnyal)
U13b	Követő bitek	Az DSRC-VU maximum 8 bitet továbbíthat a vége jelölő után. Az RSU (REDCR) ezeket a további biteket nem köteles figyelembe venni.	(Összhangban az EN 12253 szabvánnyal)

(*) – Ezeken a feltöltési paramétereken megfelelőségi vizsgálatokat kell végezni az EN 300 674-1 szabványban előírt megfelelő paramétervizsgálatnak megfelelően.

▼B

5.3.3 *Az antenna kialakítása*

5.3.3.1 REDCR antenna

DSC_30 Az *REDCR* antennának, amelynek kialakítása a kereskedelmi tervezés függvénye, az 5.3.2. pontban meghatározott korlátozások mellett kell működnie, amelyeket úgy adaptáltak, hogy a *DSRC-REDCR* leolvasási teljesítménye optimális legyen azon meghatározott célból és leolvasási körülmények között, amelyek közötti működésre az *REDCR*-t tervezték.

5.3.3.2 A járműegység (VU) antennája

DSC_31 A *DSRC-VU* antennának, amelynek kialakítása a kereskedelmi tervezés függvénye, az 5.3.2. pontban meghatározott korlátozások mellett kell működnie, amelyeket úgy adaptáltak, hogy a *DSRC-REDCR* leolvasási teljesítménye optimális legyen azon meghatározott célból és leolvasási körülmények között, amelyek közötti működésre az *REDCR*-t tervezték.

▼B

DSC_32 A járműegység (VU) antennáját a fenti 5.1. pontban meghatározott módon a jármű szélvédőjére vagy annak közelében kell felszerelni.

DSC_33 A tesztkörnyezetben, egy műhelyben (lásd a 6.3. szakaszt) egy, a fenti 5.1. szakasz szerint felerősített DSRC-VU antennának 1 000 leolvasás átlaga alapján az esetek több mint 99 %-ában, 2 és 10 méter közötti távolságból sikeresen kapcsolódnia kell a szabványos tesztkommunikációhoz, és sikeresen továbbítania kell az e függelékben meghatározott RTM tranzakciót.

5.4 **A DSRC protokoll RTM-re vonatkozó követelményei**

5.4.1 *Áttekintés*

DSC_34 Az *adatoknak* az 5,8 GHz-es DSRC interfészkapcsolaton keresztül történő letöltésére vonatkozó tranzakciós protokollnak követnie kell a következő lépéseket. Ez a szakasz egy ideális körülmények között lezajló tranzakció menetét írja le, a továbbítás megismétlése vagy a kommunikáció megszakadása nélkül.

MEGJEGYZÉS: Az inicializálási fázis (1. lépés) célja, hogy megteremtse a kommunikációt az *REDCR* és azon DSRC-VU-k között, amelyek már beléptek az 5,8 GHz-es DSRC (mester-szolga) tranzakciós zónába, de még nem teremtettek kommunikációs kapcsolatot az *REDCR*-rel, és értesítse az alkalmazásfolyamatokat.

— **1. lépés** Inicializálás. Az *REDCR* elküld egy keretet, benne egy irányadó szolgáltatási táblázatot (BST), amely tartalmazza a támogatott szolgáltatásjegyzékben szereplő alkalmazások azonosítóit (AID). Az RTM alkalmazásban ez az a szolgáltatás, amelynek az AID értéke = 2 (Freight&Fleet). A *DSRC-VU* értékeli a kapott BST-t, és a Freight&Fleet tartományban támogatott alkalmazások jegyzékével válaszol (lásd alább), vagy ha egyik sem támogatott, akkor nem válaszol. Ha az *REDCR* nem kínál olyan szolgáltatást, amelynek az esetében AID=2, akkor a DSRC-VU nem válaszol az REDCR-nek.

— **2. lépés** A *DSRC-VU* privát ablak kiosztására vonatkozó kérést tartalmazó keretet küld.

— **3. lépés** Az *REDCR* privát ablak kiosztását tartalmazó keretet küld.

— **4. lépés** A *DSRC-VU* a kiosztott privát ablak révén keretet küld, amely tartalmazza a jármű szolgáltatási táblázatát (VST). Ez a VST tartalmazza mindazon különböző alkalmazáspéldányok jegyzékét, amelyeket ez a *DSRC-VU* támogat, és amelyek esetében AID=2. A különböző példányokat egyedileg generált EID-k révén kell azonosítani, amelyek mindegyikéhez kapcsolódnia kell egy Application Context Mark (alkalmazáskörnyezeti jel) paraméterértéknek, amely az alkalmazásra és a támogatott szabványra utal.

— **5. lépés** Ezután az *REDCR* elemzi a kínált VST-t, és vagy befejezi a kapcsolatot (RELEASE), mivel semmi nem érdekli abból, amit a VST kínál (azaz olyan *DSRC-VU*-tól kapott VST-t, amely nem támogatja az RTM tranzakciót), vagy ha megfelelő VST-t kapott, elindítja valamelyik alkalmazás egy példányát.

▼B

— **6. lépés** Ehhez az REDCR az RTM adatok lekérésére irányuló parancsot tartalmazó keretet küld, amely (a DSRC-VU által a VST-ben meghatározott) RTM alkalmazáspéldánynak megfelelő azonosítót megadva azonosítja az RTM alkalmazáspéldányt, és privát ablakot oszt ki.

— **7. lépés** A *DSRC-VU* az újonnan kiosztott privát ablak révén egy olyan keretet küld, amely tartalmazza a VST-ben megadott RTM alkalmazáspéldánynak megfelelő, címzett azonosítót, amelyet az *RtmData* attribútum (hasznos elem + biztonsági elem) követ.

— **8. lépés** Ha a kérelem több szolgáltatásra irányul, az ‘n’ érték a következő szolgáltatáshivatkozási számra változik, és a folyamat megismétlődik.

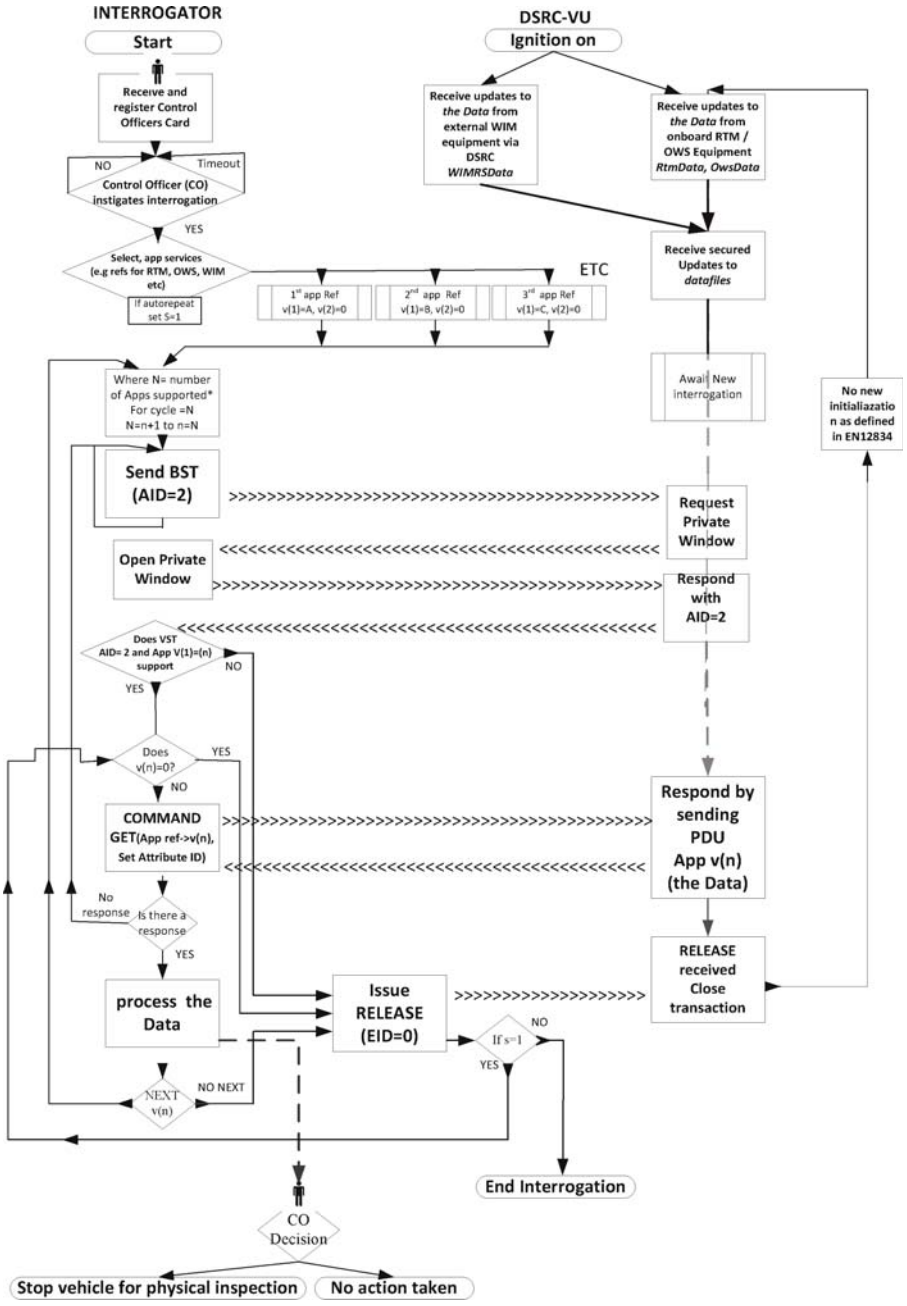
— **9. lépés** Az *REDCR* a munkamenet befejezése céljából a *DSRC-VU*-nak egy RELEASE parancsot tartalmazó keretet küldve visszaigazolja az adatok fogadását, VAGY ha nem igazolta vissza az adatok sikeres fogadását, az LDPU visszalép a 6. lépéshez.

A tranzakciós protokoll képi ábrázolását lásd a 14.6. ábrán.

▼B

14.6. ábra

Az 5,8 GHz-es DSRC keretében végrehajtott RTM folyamata



5.4.2 *Parancsok*

DSC_35 Az RTM tranzakció szakaszában kizárólag a következő parancsok kerülnek alkalmazásra

— **INITIALISATION.request**: Az REDCR által szétküldött parancs, amely magában foglalja az REDCR által támogatott alkalmazások meghatározását.

— **INITIALISATION.response**: Válasz a DSRC-VU-tól, amely megerősíti a kapcsolatot, és tartalmazza a támogatott alkalmazáspéldányok jegyzékét, valamint jellemzőket és azt, hogy mikén kell azokat megcímezni (EID).

▼B

— **GET.request**: Az *REDCR* által a *DSRC-VU*-nak küldött parancs, amely meghatározza a VST-ben kapott, meghatározott EID révén megcímzendő alkalmazáspéldányt, és arra utasítja a *DSRC-VU*-t, hogy az *adatokkal* együtt a kiválasztott tulajdonságo(ka)t is küldje el. A GET parancs célja az, hogy az *REDCR* megszerezze az *adatokat* a *DSRC-VU*-tól.

— **GET.response**: A DSRC-VU válasza, amely tartalmazza a kért *adatokat*.

— **ACTION.request ECHO**: A *DSRC-VU*-t arra utasító parancs, hogy adatokat küldjön vissza *DSRC-VU*-ból az *REDCR*-nek. Az ECHO parancs célja az, hogy lehetővé tegye a műhelyek és a típus-jóváhagyási vizsgálatokat végző létesítmények számára, hogy biztonsági hitelesítő adatokhoz való hozzáférés nélkül meg tudják vizsgálni, hogy működik-e a DSRC kapcsolat.

— **ACTION.response ECHO**: A DSRC VU válasza az ECHO parancsra.

— **EVENT_REPORT.request RELEASE**: A *DSRC-VU*-t arról tájékoztató parancs, hogy a tranzakció befejeződött. A RELEASE parancs célja az, hogy befejezze a *DSRC-VU*-val folyó munkamenetet. A RELEASE parancs fogadása után a *DSRC-VU* semmilyen további lekérdezésre nem reagál az aktuális kapcsolat keretében. Meg kell jegyezni, hogy az EN 12834 szabvány szerint a DSRC-VU csak akkor kapcsolódhat másodszor ugyanahhoz a lekérdezőhöz, ha 255 másodpercen át a kommunikációs zónán kívül volt, vagy ha a lekérdező irányadó azonosítója megváltozik.

5.4.3 *Lekérdezési parancssorozat*

DSC_36 A parancs és válasz sorozata szempontjából a tranzakció leírása a következő:

▼C2

Sorrend	Feladó		Vevő	Leírás	Művelet
1	REDCR	>	DSRC-VU	A kommunikációs kapcsolat inicializálása – Kérés	A REDCR BST-t sugároz
2	*DSRC-VU*	>	*REDCR*	*A kommunikációs kapcsolat inicializálása – Válasz*	*Ha a BST támogatja, hogy AID = 2, akkor a DSRC-VU privát ablakot kér*
3	REDCR	>	DSRC-VU	Privát ablak megadása	Privát ablak kiosztását tartalmazó keretet küld
4	*DSRC-VU*	>	*REDCR*	*VST-t küld*	*VST-t tartalmazó keretet küld*
5	REDCR	>	DSRC-VU	Adott EID tekintetében az Attribútumban tárolt adatra vonatkozó GET.request üzenetet küld	
6	*DSRC-VU*	>	*REDCR*	*Adott EID tekintetében Get-response üzenetet küld a kért Attribútummal*	*Elküldi az Attribútumot (RTMData, OWSData….) az adatokkal az adott EID tekintetében*

▼C2

Sorrend	Feladó		Vevő	Leírás	Művelet
7	REDCR	>	DSRC-VU	Más Attribútum adatára vonatkozó GET.request üzenetet küld (értelemszerűen)	
8	*DSRC-VU*	>	*REDCR*	*Get-response üzenetet küld a kért Attribútummal*	*Elküldi az Attribútumot az adatokkal az adott EID tekintetében*
9	REDCR	>	DSRC-VU	Nyugtázza a sikeres adatfogadást	RELEASE utasítást küld, amely zárja a tranzakciót
10	*DSRC-VU*			*Zárja a tranzakciót*	

▼B

A tranzakciósorozatra és a kicserélt keretek tartalmára vonatkozó példát az 5.4.7. és a 5.4.8. pont határozza meg.

5.4.4 *Adatstruktúrák*

DSC_37 Az 5,8 GHz-es DSRC interfészen keresztül továbbított *adatok* szemantikai struktúrájának összhangban kell állnia az ebben a függelékben leírtakkal. Ezen adatok strukturálásának módját ez a pont határozza meg.

DSC_38 A hasznos adatok (RTM adatok) a következők összefűzéséből állnak

1. EncryptedTachographPayload, amely az ASN.1 jelölésű, az 5.4.5. pontban meghatározott TachographPayload titkosítása. A titkosítási módszer leírása a 11. függelékben található.

2. az 11. függelékben meghatározott DSRCSecurityData.

DSC_39 Az RTM Data címzése RTM attribútum=1, és átvitele abban a tárolóban történik, amelyre igaz, hogy RTM tároló=10.

DSC_40 Az RTM Context Mark (RTM környezeti jel) azonosítja a TARV szabványsorozatból a támogatott szabványrészt (az RTM a 9. résznek felel meg)

Az RTM alkalmazáson belüli RSDC adatokra vonatkozó ASN.1 modulmeghatározás meghatározása a következő:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        rtmData                     [10]   RtmData,
        rtmContextmark              [11]   Rtm-ContextMark,
        reserved12                  [12]   NULL,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Az RtmData elemei, elvégzett műveletek és fogalommeghatározások*

DSC_41 A járműegység (VU) által kiszámítandó és a DSRC-VU-ban a biztonságos adatok frissítéséhez felhasznált adatértékeket a 14.3. táblázatban meghatározott szabályok szerint kell kiszámítani:

▼C2

14.3. táblázat

Az RtmData elemei, elvégzett műveletek és fogalommeghatározások

(1) RTM adatelem	(2) A járműegység által végrehajtott művelet		(3) ASN.1 adatok meghatározása

RTM1
A jármű rendszámtáblája
	A járműegységnek az RTM1 *tp15638VehicleRegistrationPlate* adatelem értékét az 1. függelékben (*VehicleRegistrationIdentification*) meghatározott *VehicleRegistrationIdentification* adattípusra rögzített érték alapján kell megadnia	A jármű rendszámtáblája karaktersorként kifejezve	`tp15638VehicleRegstrationPlate LPN,`
			`--A jármű rendszámtáblája az ISO 14906 szabványból átvéve az EN 15509 szabványban meghatározott korlátozással,`
			`nevezetesen egy SOROZAT, amely magában foglalja az országkódot, amelyet egy alfabetikus mutató, majd maga a rendszám követ, amely mindig 14 oktett (nullákkal kiegészítve), így az EN 15509 LPN típus hossza mindig 17 oktett, amelyből 14 az „igazi” rendszám.`

RTM2 **Gyorshajtási esemény**	A járműegységnek logikai értéket kell generálnia az RTM2 tp15638SpeedingEvent adatelemre. A tp15638SpeedingEvent értékét a járműegységnek az 1C. mellékletben meghatározottak szerint a járműegységben az előfordulás utolsó 10 napján rögzített gyorshajtási események számából kell kiszámítania.	1 (IGAZ) – Azt jelzi, hogy az előfordulás utolsó 10 napján a sebességet érintő szabálytalanságokra kerül sor	`tp15638speedingEvent LOGIKAI,`

▼C2

(1) RTM adatelem	(2) A járműegység által végrehajtott művelet		(3) ASN.1 adatok meghatározása
	Ha az előfordulás utolsó 10 napján legalább egy tp15638SpeedingEvent van, akkor a tp15638SpeedingEvent értékét IGAZ-ra kell állítani. MÁSKÜLÖNBEN ha nincsenek események az előfordulás utolsó 10 napján, akkor a tp15638SpeedingEvent értékét HAMIS-ra kell állítani.		
RTM3 **Érvényes kártya nélküli járművezetés**	A járműegységnek logikai értéket kell generálnia az RTM3 tp15638DrivingWithoutValidCard adatelemre. A járműegységnek az Igaz értéket kell hozzárendelnie a tp15638DrivingWithoutValidCard változóhoz, ha a járműegység az előfordulás utolsó 10 napján legalább egy, az 1C melléklet meghatározása szerinti „Járművezetés megfelelő kártya nélkül” típusú eseményt rögzített. MÁSKÜLÖNBEN ha nincsenek események az előfordulás utolsó 10 napján, akkor a tp15638DrivingWithoutValidCard változó értékét HAMIS-ra kell állítani.	1 (IGAZ) = Érvénytelen kártya használatát jelzi	`tp15638DrivingWithoutValidCard LOGIKAI,`
RTM4 **Érvényes járművezetői kártya**	A járműegységnek logikai értéket kell generálnia az RTM4 tp15638DriverCard adatelemre a járműegységben tárolt és az 1. függelékben meghatározott adatok alapján. Ha nincs jelen érvényes járművezetői kártya, akkor a járműegységnek a változó értékét IGAZ-ra kell állítania MÁSKÜLÖNBEN ha jelen van érvényes járművezetői kártya, akkor a járműegységnek a változó értékét HAMIS-ra kell állítania	0 (HAMIS) = Érvényes járművezetői kártyát jelez	`tp15638DriverCard LOGIKAI,`
RTM5 **Kártya behelyezése járművezetés közben**	A járműegységnek logikai értéket kell generálnia az RTM5 adatelemre. A járműegységnek az IGAZ értéket kell hozzárendelnie a tp15638CardInsertion változóhoz, ha a járműegység az adatai között az előfordulás utolsó 10 napján legalább egy, az 1C melléklet meghatározása szerinti „Kártya behelyezése járművezetés közben” típusú eseményt rögzített. MÁSKÜLÖNBEN ha nincsenek ilyen események az előfordulás utolsó 10 napján, akkor a tp15638CardInsertion változó értékét HAMIS-ra kell állítani.	1 (IGAZ) – Azt jelzi, hogy az előfordulás utolsó 10 napján kártya behelyezése történt járművezetés közben	`tp15638CardInsertion LOGIKAI,`
RTM6 **Mozgásadatok hibája**	A járműegységnek logikai értéket kell generálnia az RTM6 adatelemre. A járműegységnek az IGAZ értéket kell hozzárendelnie a tp15638MotionDataError változóhoz, ha a járműegység az adatai között az előfordulás utolsó 10 napján legalább egy, az 1C melléklet meghatározása szerinti „Mozgásadatok hibája” típusú eseményt rögzített. MÁSKÜLÖNBEN ha nincsenek ilyen események az előfordulás utolsó 10 napján, akkor a tp15638MotionDataError változó értékét HAMIS-ra kell állítani.	1 (IGAZ) – Azt jelzi, hogy az előfordulás utolsó 10 napján a mozgásadatok hibája fordult elő	`tp15638motionDataError LOGIKAI,`

▼C2

(1) RTM adatelem	(2) A járműegység által végrehajtott művelet		(3) ASN.1 adatok meghatározása
RTM7 **A jármű mozgásával kapcsolatos ellentmondás**	A járműegységnek logikai értéket kell generálnia az RTM7 adatelemre. A járműegységnek az IGAZ értéket kell hozzárendelnie a tp15638vehicleMotionConflict változóhoz, ha a járműegység az adatai között az előfordulás utolsó 10 napján legalább egy „A jármű mozgásával kapcsolatos ellentmondás” típusú eseményt rögzített (»0A«H érték). MÁSKÜLÖNBEN ha nincsenek események az előfordulás utolsó 10 napján, akkor a tp15638vehicleMotionConflict változó értékét HAMIS-ra kell állítani.	1 (IGAZ) – Azt jelzi, hogy az előfordulás utolsó 10 napján a jármű mozgásával kapcsolatos ellentmondás fordult elő	`tp15638vehicleMotionConflict LOGIKAI,`
RTM8 **2. járművezetői kártya**	A járműegységnek logikai értéket kell generálnia az RTM8 adatelemre az 1C melléklet („A járművezető tevékenységére vonatkozó adatok” SZEMÉLYZET és JÁRMŰKÍSÉRŐ) alapján. Ha jelen van egy 2. érvényes járművezetői kártya, akkor a járműegységnek a változó értékét IGAZ-ra kell állítania MÁSKÜLÖNBEN ha nincs jelen 2. érvényes járművezetői kártya, akkor a járműegységnek a változó értékét HAMIS-ra kell állítania	1 (IGAZ) = Azt jelzi, hogy egy második járművezetői kártya van behelyezve	`tp156382ndDriverCard LOGIKAI,`
RTM9 **Aktuális tevékenység**	A járműegységnek logikai értéket kell generálnia az RTM9 adatelemre. Ha a járműegységben rögzített aktuális tevékenység az 1C melléklet meghatározása szerinti, „JÁRMŰVEZETÉSTŐL” eltérő tevékenység, akkor a járműegységnek a változó értékét IGAZ-ra kell állítania MÁSKÜLÖNBEN ha a járműegységben rögzített aktuális tevékenység „JÁRMŰVEZETÉS”, akkor a járműegységnek a változó értékét HAMIS-ra kell állítania	1 (IGAZ) = egyéb tevékenység van kiválasztva; 0 (HAMIS) = járművezetés van kiválasztva	`tp15638currentActivityDriving LOGIKAI`
RTM10 **Az utolsó kapcsolat lezárása**	A járműegységnek logikai értéket kell generálnia az RTM10 adatelemre. Ha az utolsó kártyakapcsolat lezárása az 1C melléklet meghatározása szerint nem megfelelően történt, akkor a járműegységnek a változó értékét IGAZ-ra kell állítania. MÁSKÜLÖNBEN ha az utolsó kártyakapcsolat lezárása megfelelően történt, akkor a járműegységnek a változó értékét HAMIS-ra kell állítania.	1 (IGAZ) = a lezárás nem megfelelően történt 0 (HAMIS) = a lezárás megfelelően történt	`tp15638 lastSessionClosed LOGIKAI`
RTM11 **Az áramellátás megszakadása**	A járműegységnek egész számú értéket kell generálnia az RTM11 adatelemre. A járműegységnek az 1C melléklet meghatározása szerinti „Áramellátás megszakadása” típusú, a 165/2014/EU rendelet 9. cikke szerinti, „az áramellátás leghosszabb megszakadásával” egyenlő értéket kell hozzárendelnie a tp15638PowerSupplyInterruption változóhoz.	— Ahányszor az áramellátás megszakadt az előfordulás utolsó 10 napján	`tp15638powerSupplyInterruption EGÉSZ SZÁM (0..127),`

▼C2

(1) RTM adatelem	(2) A járműegység által végrehajtott művelet		(3) ASN.1 adatok meghatározása
	MÁSKÜLÖNBEN ha az előfordulás utolsó 10 napján nincsenek Áramellátás megszakadása típusú események, az egész szám értékét 0-ra kell beállítani.		
RTM12 **Érzékelőhiba**	A járműegységnek egész számú értéket kell generálnia az RTM12 adatelemre. A járműegységnek a következő értéket kell hozzárendelnie a sensorFault változóhoz: — 1 ha »35«H Érzékelőhiba típusú esemény került rögzítésre az utolsó 10 napon, — 2 ha (»51«H vagy »52«H sorszámú belső vagy külső) GNSS-vevőhiba típusú esemény került rögzítésre az utolsó 10 napon, — 3 ha »53«H Külső GNSS-kommunikációs hiba típusú esemény került rögzítésre az előfordulás utolsó 10 napján, — 4 ha Érzékelőhiba és GNSS-vevőhiba típusú esemény egyaránt rögzítésre került az előfordulás utolsó 10 napján, — 5 ha Érzékelőhiba és Külső GNSS-kommunikációs hiba típusú esemény egyaránt rögzítésre került az előfordulás utolsó 10 napján, — 6 ha GNSS-vevőhiba és Külső GNSS-kommunikációs hiba típusú esemény egyaránt rögzítésre került az előfordulás utolsó 10 napján, — 7 ha mindhárom érzékelőhiba rögzítésre került az előfordulás utolsó 10 napján. MÁSKÜLÖNBEN 0 értéket kell hozzárendelnie, ha nem került rögzítésre esemény az előfordulás utolsó 10 napján	— érzékelőhiba egy oktett az adatszótár szerint	`tp15638SensorFault EGÉSZ SZÁM (0..255),`
RTM13 **Időbeállítás**	A járműegységnek egész számú értéket kell generálnia (timeReal az 1. függelékből) az RTM13 adatelemre az 1C mellékletben meghatározott, Időbeállításra vonatkozó meglévő adatok alapján. A járműegységnek azt az időértéket kell hozzárendelnie, amikor az utolsó időbeállítási eseményre sor került. MÁSKÜLÖNBEN ha a járműegység adatai között nincs az 1C melléklet meghatározása szerinti „Időbeállítás” típusú esemény, akkor 0 értéket kell beállítania	Az utolsó időbeállítás ideje	`tp15638TimeAdjustment EGÉSZ SZÁM(0..4294967295),`
RTM14 **A biztonsági rendszer megsértésére irányuló kísérlet**	A járműegységnek egész számú értéket kell generálnia (timeReal az 1. függelékből) az RTM14 adatelemre az 1C mellékletben meghatározott, A biztonsági rendszer megsértésére irányuló kísérlet eseményre vonatkozó meglévő adatok alapján. A járműegységnek a járműegységben rögzített utolsó „A biztonsági rendszer megsértésére irányuló kísérlet” típusú esemény idejének értékét kell beállítania.	A biztonsági rendszer megsértésére irányuló utolsó kísérlet ideje — Alapértelmezett érték = 0x00FF	`tp15638LatestBreachAttempt EGÉSZ SZÁM(0..4294967295),`

▼C2

(1) RTM adatelem	(2) A járműegység által végrehajtott művelet		(3) ASN.1 adatok meghatározása
	MÁSKÜLÖNBEN ha a járműegység adatai között nincs az 1C melléklet meghatározása szerinti „A biztonsági rendszer megsértésére irányuló kísérlet” típusú esemény, akkor 0x00FF értéket kell beállítania.		
RTM15 **Utolsó kalibrálás**	A járműegységnek egész számú értéket kell generálnia (timeReal az 1. függelékből) az RTM15 adatelemre az 1C mellékletben meghatározott, az Utolsó kalibrálásra vonatkozó meglévő adatok alapján. A járműegységnek be kell állítania a legutóbbi két kalibrálás (RTM15 és RTM16) idejének értékét, amelyeket az 1. függelékben meghatározott VuCalibrationData tartalmazza. A járműegységnek az RTM15 értékét a legutóbbi kalibrálási rekord timeReal értékére kell beállítania.	Az utolsó kalibrálás ideje adat	tp15638LastCalibrationData EGÉSZ SZÁM(0..4294967295),
RTM16 **Előző kalibrálás**	A járműegységnek egész számú értéket (timeReal az 1. függelékből) kell generálnia az utolsó kalibrálás rekordját megelőző kalibrálási rekord RTM16 adatelemére MÁSKÜLÖNBEN ha nem volt előző kalibrálás, akkor a járműegységnek az RTM16 értékét 0-ra kell beállítani.	Az előző kalibrálás ideje adat	tp15638PrevCalibrationData EGÉSZ SZÁM(0..4294967295),
RTM17 **A tachográf csatlakoztatásának dátuma**	Az RTM17 adatelemre a járműegységnek egész számú értéket (timeReal az 1. függelékből) kell generálnia. A járműegységnek a kezdeti beépítés idejének értékét kell beállítania. A járműegységnek ezt az adatot a vuCalibrationRecords sorozat azon VuCalibrationData adatából (1. függelék) kell vennie, amelynél teljesül, hogy CalibrationPurpose egyenlő: »03«H	A tachográf csatlakoztatásának dátuma	tp15638DateTachoConnected EGÉSZ SZÁM(0..4294967295),
RTM18 **Aktuális sebesség**	A járműegységnek egész számú értéket kell generálnia az RTM18 adatelemre. A járműegységnek az RTM16 értékét az RtmData legutóbbi frissítésének idején rögzített utolsó aktuális sebességre kell beállítania.	Utolsó rögzített aktuális sebesség	tp15638CurrentSpeed EGÉSZ SZÁM (0..255),
RTM19 **Időbélyegző**	Az RTM19 adatelemre a járműegységnek egész számú értéket kell generálnia (timeReal az 1. függelékből). A járműegységnek az RTM19 értékét az RtmData legutóbbi frissítésének idejére kell beállítania.	Az aktuális TachographPayload rekord időbélyegzője	tp15638Timestamp EGÉSZ SZÁM(0..4294967295)

▼B

5.4.6 *Adatátviteli mechanizmus*

DSC_42 Az inicializálási szakasz után a REDCR előzetesen meghatározott hasznos adatokat kér, amelyeket azután a *DSRC-VU* a kiosztott ablakban továbbít. Az REDCR a GET paranccsal adatokat kér le.

▼B

DSC_43 Az adatokat minden DSRC cseréhez a PER (csomagolt kódolási szabályok) szerint kell kódolni.

5.4.7 *A DSRC tranzakció részletes leírása*

DSC_44 Az inicializálást a DSC_44–DSC_48 szakasz és a 14.4–14.9. táblázat szerint kell elvégezni. Az inicializálási szakaszban az REDCR küldeni kezd egy keretet, amely az EN 12834 szabványnak, valamint az EN 13372 szabvány 6.2., 6.3., 6.4. és 7.1. szakaszának megfelelő irányadó szolgáltatási táblázatot (BST) tartalmaz, amelynek beállításait a következő 14.4. táblázat tartalmazza.

▼C2

14.4. táblázat

Inicializálás – A BST keret beállításai

Mező	Beállítások
Link Identifier	Szórási cím
BeaconId	Az EN 12834 szabványnak megfelelően
Time	Az EN 12834 szabványnak megfelelően
Profile	Nincs kiterjesztés, 0-t vagy 1-et kell használni
MandApplications	Nincs kiterjesztés, EID nem található meg, Parameter nem található meg, AID = 2 Freight&Fleet
NonMandApplications	Nem található meg
ProfileList	Nincs kiterjesztés, profilok száma a listán = 0
Fragmentation header	Nincs tördelés
Layer 2 settings	Parancs-PDU, UI-parancs

▼B

A következő 14.5. táblázat a 14.4. táblázatban megadott beállításokra vonatkozó gyakorlati példát mutat be, jelezve a bitkódolásokat.

▼C2

14.5. táblázat

Inicializálás – Példa a BST keret tartalmára

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Broadcast ID	1111 1111	Szórási cím
3	MAC Control Field	1010 0000	Parancs-PDU
4	LLC Control field	0000 0011	UI-parancs

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
5	Fragmentation header	1xxx x001	Nincs tördelés
6	BST	1000	Inicializálási kérés
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand alkalmazások nem találhatók meg
		xxx	Gyártóazonosító
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727) }	xxx	27 bit hosszú azonosító áll rendelkezésre a gyártó tárolására
9		xxxx xxxx	
10		xxxx xxxx	
11		xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bit UNIX valós idő
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Nincs kiterjesztés. Példaprofil 0
17	MandApplications SEQUENCE (SIZE(0..127,…)) OF {	0000 0001	Nincs kiterjesztés, mandApplications száma = 1
18	SEQUENCE {		
	OPTION indicator	0	EID nem található meg
	OPTION indicator	0	Parameter nem található meg
	AID DSRCApplicationEntityID}}	00 0010	Nincs kiterjesztés. AID = 2 Freight&Fleet

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
19	ProfileList SEQUENCE (0..127,…) OF Profile}	0000 0000	Nincs kiterjesztés, profilok száma a listán = 0
20	FCS	xxxx xxxx	Keretellenőrző összeg
21		xxxx xxxx	
22	Flag	0111 1110	Vége jelölő

▼B

DSC_45 Amikor a *DSRC-VU* BST-t fogad, az EN 12795 szabványnak és az EN 13372 szabvány 7.1.1. szakaszának megfelelő, kimondottan az RTM-re vonatkozó beállításokkal nem rendelkező privát ablak kiosztását. A 14.6. táblázat egy, a bitkódolásra vonatkozó példát mutat be.

▼C2

14.6. táblázat

Inicializálás – Privát ablak kiosztására vonatkozó kérés keretének tartalma

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Privát ablak kérése
7	FCS	xxxx xxxx	Keretellenőrző összeg
8		xxxx xxxx	
9	Flag	0111 1110	Vége jelölő

▼B

DSC_46 Az REDCR ezután az EN 12795 szabványnak és az EN 13372 szabvány 7.1.1. szakaszának megfelelő, kimondottan az RTM-re vonatkozó beállításokkal nem rendelkező privát ablak kiosztásával válaszol.

A 14.7. táblázat egy, a bitkódolásra vonatkozó példát mutat be.

▼C2

14.7. táblázat

Inicializálás – Privát ablak kiosztására vonatkozó keret tartalma

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Privát ablak kiosztása
7	FCS	xxxx xxxx	Keretellenőrző összeg
8		xxxx xxxx	
9	Flag	0111 1110	Vége jelölő

▼B

DSC_47 Amikor a *DSRC-VU* megkapja a privát ablak kiosztását, a kiosztott privát ablak révén elküldi az EN 12834 szabványnak, valamint az EN 13372 szabvány 6.2., 6.3., 6.4. és 7.1. szakaszának megfelelő, a jármű szolgáltatási táblázatát (VST), amelynek beállításait a 14.8. táblázat tartalmazza.

▼C2

14.8. táblázat

Inicializálás – A VST keret beállításai

Mező	Beállítások
Private LID	Az EN 12834 szabványnak megfelelően
VST parameters	Fill = 0, majd minden egyes támogatott alkalmazás esetében: EID megtalálható, paraméter megtalálható, AID = 2, EID az OBU által generálva
Parameter	Nincs kiterjesztés, Tartalmazza az RTM környezeti jelet
ObeConfiguration	A választható ObeStatus mező jelen lehet, de az REDCR nem használhatja
Fragmentation header	Nincs tördelés
Layer 2 settings	Parancs-PDU, UI-parancs

▼B

DSC_48 A *DSRC-VU* támogatja a „Freight and Fleet” alkalmazást, amelyet a 2-es alkalmazásazonosító azonosít. Más alkalmazásazonosítók is támogathatók, azok ebben az VST-ben azonban nem lesznek jelen, mivel a BST csak azokat az alkalmazásokat kéri, amelyek esetében AID=2. Az „Alkalmazások” mező tartalmazza a *DSRC-VU*-ban támogatott alkalmazáspéldányok jegyzékét. Valamennyi támogatott alkalmazáspéldány esetében RTM Context Mark (RTM környezeti jel) formájában meg van adva a megfelelő szabvány hivatkozása, amelyet a vonatkozó szabványt, a vonatkozó részt (az RTM esetében ez a 9. rész) és esetleg a verzióját képviselő OBJECT IDENTIFIER, valamint egy a DSRC-UV által generált EID alkot, és amely hozzá van rendelve az adott alkalmazáspéldányhoz.

A 14.9. táblázat a 14.8. táblázatban megadott beállításokra vonatkozó gyakorlati példát mutat be, jelezve a bitkódolásokat.

▼C2

14.9. táblázat

Inicializálás – Példa a VST keret tartalmára

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Parancs-PDU
7	LLC Control field	0000 0011	UI-parancs
8	Fragmentation header	1xxx x001	Nincs tördelés
9	VST SEQUENCE {	1001	Inicializálási válasz
	Fill BIT STRING (SIZE(4))	0000	Nincs használatban és 0-ra van beállítva
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Nincs kiterjesztés. Példaprofil 0
11		0000 0001	Nincs kiterjesztés, 1 alkalmazás
12	SEQUENCE {		
	OPTION indicator	1	EID megtalálható
	OPTION indicator	1	Parameter megtalálható
	AID DSRCApplicationEntityID	00 0010	Nincs kiterjesztés. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Az OBU-ban van meghatározva, és az alkalmazáspéldányt azonosítja.
14	Parameter Container {	0000 0010	Nincs kiterjesztés, Választott tároló = 02, Oktettkarakterlánc
15		0000 1000	Nincs kiterjesztés, az RTM környezeti jel hossza = 8

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
16	Rtm-ContextMark::= SEQUENCE {	0000 0110	A támogatott szabvány, rész és verzió objektumazonosítója. Példa: ISO (1) Szabvány (0) TARV (15638) 9. rész (9) 1. verzió (1). Az első oktett a 06H, ami az objektumazonosító. A második oktett a 06H, ami a hossza. A következő 6 oktett kódolja a például szolgáló objektumazonosítót. Fontos megjegyezni, hogy a szekvenciának csak egy eleme van jelen (a választható RtmCommProfile elem hiányzik)
17	StandardIdentifier standardIdentifier	0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus nem található meg
25	EquipmentClass INTEGER (0..32767)	xxx xxxx	
		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	A DSRC-VU gyártójának azonosítója az ISO 14816 szabvány szerinti nyilvántartásban leírt módon
27		xxxx xxxx	
28	FCS	xxxx xxxx	Keretellenőrző összeg
29		xxxx xxxx	
30	Flag	0111 1110	Vége jelölő

▼B

DSC_49 Az REDCR ezután az adatok olvasása érdekében kiad egy, az EN 13372 szabvány 6.2., 6.3. és 6.4. szakaszában, valamint az EN 12834 szabványban meghatározott GET parancsnak megfelelő GET parancsot, amelynek beállításait a 14.10. táblázat tartalmazza.

▼C2

14.10. táblázat

Megjelenítés – A GET Request keretének beállításai

Mező	Beállítások
Invoker Identifier (IID)	Nem található meg
Link Identifier (LID)	Adott DSRC-VU címének csatolása
Chaining	Nincs
Element Identifier (EID)	A VST-ben meghatározott módon. Nincs kiterjesztés

▼C2

Mező	Beállítások
Access Credentials	Nincs
AttributeIdList	Nincs kiterjesztés, 1 attribútum, AttributeID = 1 (RtmData)
Fragmentation	Nincs
Layer2 settings	Parancs-PDU, Lekérdezett ACn-parancs

▼B

A 14.11. táblázat egy, a RTM adatok olvasására vonatkozó példát mutat be.

▼C2

14.11. táblázat

Megjelenítés – Példa a GET Request keretre

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Parancs-PDU
7	LLC Control field	n111 0111	Lekérdezett ACn parancs, n bit
8	Fragmentation header	1xxx x001	Nincs tördelés
9	Get.request SEQUENCE {	0110	Get kérés
	OPTION indicator	0	Access Credentials nem található meg
	OPTION indicator	0	IID nem található meg
	OPTION indicator	1	AttributeIdList megtalálható
	Fill BIT STRING(SIZE(1))	0	0-ra van beállítva.
10	EID INTEGER(0..127,…)	xxxx xxxx	Az RTM alkalmazáspéldány EID-je a VST-ben meghatározott módon. Nincs kiterjesztés
11	AttributeIdList SEQUENCE OF { AttributeId}}	0000 0001	Nincs kiterjesztés, attribútumok száma = 1
12		0000 0001	AttributeId = 1, RtmData. Nincs kiterjesztés
13	FCS	xxxx xxxx	Keretellenőrző összeg
14		xxxx xxxx	
15	Flag	0111 1110	Vége jelölő

▼B

DSC_50 Amikor a *DSRC-VU* GET kérést kap, a kért adatokkal az EN 13372 szabvány 6.2., 6.3. és 6.4. szakaszában, valamint az EN 12834 szabványban meghatározott GET válasznak megfelelő GET választ küld, amelynek beállításait a 14.12. táblázat tartalmazza.

▼C2

14.12. táblázat

Megjelenítés – A GET Response keretének beállításai

Mező	Beállítások
Invoker Identifier (IID)	Nem található meg
Link Identifier (LID)	Az EN 12834 szabványnak megfelelően
Chaining	Nincs
Element Identifier (EID)	A VST-ben meghatározott módon.
Access Credentials	Nincs
Fragmentation	Nincs
Layer2 settings	Válasz-PDU, Válasz rendelkezésre áll és a parancs elfogadva, ACn-parancs

▼B

A 14.13. táblázat egy, a RTM adatok olvasására vonatkozó példát mutat be.

▼C2

14.13. táblázat

Megjelenítés – Példa a Response keret tartalmára

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Válasz-PDU
7	LLC Control field	n111 0111	Válasz rendelkezésre áll, az ACn-parancs n bit
8	LLC Status field	0000 0000	Válasz rendelkezésre áll és a parancs elfogadva
9	Fragmentation header	1xxx x001	Nincs tördelés
10	Get.response SEQUENCE {	0111	Get válasz

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
	OPTION indicator	0	IID nem található meg
	OPTION indicator	1	Attribute List megtalálható
	OPTION indicator	0	A visszaküldött állapot nem található meg
	Fill BIT STRING(SIZE(1))	0	Nincs használatban
11	EID INTEGER(0..127,…)	xxxx xxxx	Válasz az RTM alkalmazáspéldánytól. Nincs kiterjesztés,
12	AttributeList SEQUENCE OF {	0000 0001	Nincs kiterjesztés, attribútumok száma = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Nincs kiterjesztés, AttributeId = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Nincs kiterjesztés, Választott tároló = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Keretellenőrző összeg
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Vége jelölő

▼B

DSC_51 Az REDCR ezután kiad egy, az EN 13372 szabvány 6.2., 6.3. és 6.4. szakaszának, valamint az EN 12834 szabvány 7.3.8. szakaszának megfelelő EVENT_REPORT, RELEASE parancsot, amely amelynek nincs kimondottan az RTM-re vonatkozó beállítása. A 14.14. táblázat egy, a RELEASE utasítás bitkódolására vonatkozó példát mutat be.

▼C2

14.14. táblázat

Befejezés. Az EVENT_REPORT Release keret tartalma

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	

▼C2

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
5		xxxx xxxx	
6	MAC Control field	1000 s000	A keret parancs-LPDU-t tartalmaz
7	LLC Control field	0000 0011	UI-parancs
8	Fragmentation header	1xxx x001	Nincs tördelés
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Access Credentials nem található meg
	OPTION indicator	0	Az esemény paramétere nem található meg
	OPTION indicator	0	IID nem található meg
	Mode BOOLEAN	0	Nincs várt válasz
10	EID INTEGER (0..127,…)	0000 0000	Nincs kiterjesztés, EID = 0 (Rendszer)
11	EventType INTEGER (0..127,…)}	0000 0000	Eseménytípus 0 = Kiadás
12	FCS	xxxx xxxx	Keretellenőrző összeg
13		xxxx xxxx	
14	Flag	0111 1110	Vége jelölő

▼B

DSC_52 A *DSRC-VU*-nak nem kell válaszolnia a Release parancsra. A kommunikáció ezután lezárul.

5.4.8 *A DSRC teszttranzakció leírása*

DSC_53 Az adatok biztosítását magukban foglaló teljes teszteket a 11. függelékben (Közös biztonsági mechanizmusok) meghatározott módon, a biztonsági eljárásokhoz hozzáféréssel rendelkező, jogosult személyeknek kell elvégezniük a fentiekben meghatározott rendes GET parancs segítségével.

DSC_54 Az üzembe helyezési és az időszakos teszteket, amelyek visszafejtést és a visszafejtett adatok megértését igénylik, a 11. függelékben (Közös biztonsági mechanizmusok) és a 9. függelékben (Típusjóváhagyás – A minimálisan megkövetelt vizsgálatok felsorolása) meghatározott módon kell elvégezni.

Az alapszintű DSRC kommunikációt azonban lehet tesztelni az ECHO paranccsal. Az ilyen tesztek elvégzése előírás lehet üzembe helyezés, időszakos vizsgálat esetén, vagy elvégzésüket előírhatja az illetékes ellenőrző hatóság vagy az 165/2014/EU rendelet (lásd a lenti 6. pontot).

▼B

DSC_55 Ilyen alapszintű kommunikációs teszt elvégzéséhez az ECHO parancsot az REDCR adja ki egy munkamenet közben, azaz az inicializálási szakasz sikeres elvégzése után. Az interakciók sorozata tehát hasonló egy lekérdezéséhez:

— 1. lépés Az *REDCR* elküld egy irányadó szolgáltatási táblázatot (BST), amely tartalmazza a támogatott szolgáltatásjegyzékben szereplő alkalmazások azonosítóit (AID). Az RTM alkalmazásokban ez az a szolgáltatás, amelynek AID értéke = 2.

A *DSRC-VU* értékeli a kapott BST-t, és ha azt határozza meg, hogy a BST a Freight&Fleet (AID = 2) szolgálttást kéri, akkor a *DSRC-VU* válaszol. Ha az *REDCR* nem kínál olyan szolgáltatást, amelynek esetében AID=2, akkor a *DSRC-VU* leállítja a tranzakciót az *REDCR*-rel.

— 2. lépés A *DSRC-VU* privát ablak kiosztására vonatkozó kérést küld.

— 3. lépés Az REDCR privát ablak kiosztására vonatkozó üzenetet küld.

— 4. lépés A *DSRC-VU* a kiosztott privát ablak révén elküldi a jármű szolgáltatási táblázatát (VST). Ez a VST tartalmazza mindazon különböző alkalmazáspéldányok jegyzékét, amelyeket ez a *DSRC-VU* támogat, és amelyek esetében AID=2. A különböző példányokat egyedi EID-k révén kell azonosítani, amelyek mindegyikéhez kapcsolódnia kell egy paraméterértéknek, amely a támogatott alkalmazás példányára utal.

— 5. lépés Ezután az *REDCR* elemzi a kínált VST-t, és vagy befejezi a kapcsolatot (RELEASE), mivel semmi nem érdekli abból, amit a VST kínál (azaz olyan *DSRC-VU*-tól kapott VST-t, amely nem RTM VU), vagy, ha megfelelő VST-t kapott, elindítja valamelyik alkalmazás egy példányát.

— 6. lépés Az *REDCR* (ECHO) parancsot ad ki a meghatározott *DSRC-VU*-nak, és privát ablakot oszt ki.

— 7. lépés A *DSRC-VU* az újonnan kiosztott privát ablak révén ECHO válaszkeretet küld.

A következő táblázatok az ECHO parancsok cseréjével járó munkamenetre vonatkozó gyakorlati példát mutatnak be.

DSC_56 Az inicializálást az 5.4.7. pont (DSC_44–DSC_48 szakasz) és a 14.4–14.9. táblázat szerint kell elvégezni.

DSC_57 Az REDCR ezután kiad egy az ISO 14906 szabványnak megfelelő ACTION, ECHO parancsot, amely 100 oktettet tartalmaz, és amelynek nincs kimondottan az RTM-re vonatkozó beállítása. A 14.15. táblázatban bemutatja az REDCR által küldött keret tartalmát.

▼C2

14.15. táblázat

Példa az ACTION, ECHO kérés keretére

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott DSRC-VU címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Parancs-PDU
7	LLC Control field	n111 0111	Lekérdezett ACn parancs, n bit
8	Fragmentation header	1xxx x001	Nincs tördelés
9	ACTION.request SEQUENCE {	0000	Műveletkérés (ECHO)
	OPTION indicator	0	Access Credentials nem található meg
	OPTION indicator	1	Műveletparaméter megtalálható
	OPTION indicator	0	IID nem található meg
	Mode BOOLEAN	1	Válaszra vár
10	EID INTEGER (0..127,…)	0000 0000	Nincs kiterjesztés, EID = 0 (Rendszer)
11	ActionType INTEGER (0..127,…)	0000 1111	Nincs kiterjesztés, ECHO művelettípusra vonatkozó kérés
12	ActionParameter CONTAINER {	0000 0010	Nincs kiterjesztés, Választott tároló = 2
13		0110 0100	Nincs kiterjesztés. A karakterlánc hossza = 100 oktett
14		xxxx xxxx	Visszaküldendő adatok
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Keretellenőrző összeg
115		xxxx xxxx	
116	Flag	0111 1110	Vége jelölő

▼B

DSC_58 Amikor a *DSRC-VU* ECHO kérést kap, 100 oktettnyi adatot tartalmazó ECHO választ küld az ISO 14906 szabványnak megfelelően, az RTM-re vonatkozó konkrét beállítások nélkül visszaküldve a kapott parancsot. A 14.16. táblázat egy bitszintű kódolásra vonatkozó példát mutat be.

▼C2

14.16. táblázat

Példa az ACTION, ECHO válasz keretére

Oktett száma	Attribútum/Mező	Bitek az oktettben	Leírás
1	FLAG	0111 1110	Kezdés jelölő
2	Private LID	xxxx xxxx	Adott járműegység címének csatolása
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Válasz-PDU
7	LLC Control field	n111 0111	ACn-parancs n bit
8	LLC status field	0000 0000	Válasz rendelkezésre áll
9	Fragmentation header	1xxx x001	Nincs tördelés
10	ACTION.response SEQUENCE {	0001	MŰVELETRE adott válasz (ECHO)
	OPTION indicator	0	IID nem található meg
	OPTION indicator	1	Válaszparaméter megtalálható
	OPTION indicator	0	A visszaküldött állapot nem található meg
	Fill BIT STRING (SIZE (1))	0	Nincs használatban
11	EID INTEGER (0..127,…)	0000 0000	Nincs kiterjesztés, EID = 0 (Rendszer)
12	ResponseParameter CONTAINER {	0000 0010	Nincs kiterjesztés, Választott tároló = 2
13		0110 0100	Nincs kiterjesztés. A karakterlánc hossza = 100 oktett
14		xxxx xxxx	Visszaküldött adatok
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Keretellenőrző összeg
115		xxxx xxxx	
116	Flag	0111 1110	Vége jelölő

▼B

5.5 **A 2015/71/EK irányelv támogatása**

5.5.1 *Áttekintés*

DSC_59 A nehéz tehergépjárművek maximális tömegéről és méreteiről szóló 2015/719/EK irányelv támogatása érdekében az OWS adatoknak az 5,8 GHz-es DSRC interfészkapcsolaton keresztül történő letöltésére vonatkozó tranzakciós protokollnak meg kell egyeznie az RTM adatok esetében alkalmazott tranzakciós protokollal (lásd az 5.4.1. pontot), azzal az egyetlen különbséggel, hogy a TARV szabványra vonatkozó objektumazonosítónak az ISO 15638 (TARV) szabvány WOB/OWS-re vonatkozó 20. részére kell hivatkoznia.

5.5.2 *Parancsok*

DSC_60 OWS tranzakció esetében ugyanazokat a parancsokat kell alkalmazni, mint egy RTM tranzakció esetében.

5.5.3 *Lekérdezési parancssorozat*

DSC_61 OWS adatok esetében a lekérdezési parancssorozat ugyanaz, mint RTM adatok esetében.

5.5.4 *Adatstruktúrák*

DSC_62 A hasznos adatok (OWS adatok) a következők összefűzéséből állnak

1. EncryptedOwsPayload, amely az ASN.1 jelölésű, az 5.5.5. pontban meghatározott OwsPayload titkosítása. A titkosítási módszernek ugyanannak kell lennie, mint az RtmData esetében, amelyet a 11. függelék határoz meg.

2. A DSRCSecurityData adatokat ugyanazokkal az algoritmusokal kell kiszámítani, mint az RtmData esetében, amelyet a 11. függelék határoz meg.

▼B

5.5.5 *Az OWS DSRC tranzakcióra vonatkozó ASN.1 modul*

DSC_63 Az RTM alkalmazáson belüli RSDC adatokra vonatkozó ASN.1 modulmeghatározás meghatározása a következő:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT, iid ABSENT, attrIdList})
OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData :: = SEQUENCE {
     encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
OwsPayload as per Appendix 11 --}),
     DSRCSecurityData OCTET STRING
     }
OwsPayload :: = SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
           recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
goods vehicle                                                    -- with 10 Kg
resolution.
           axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                              -- of axles for 10 axles.
           axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                            -- with 10 Kg resolution.
           tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
     }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
     }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= CHOICE {
     integer                    [0]    INTEGER,
     bitstring                  [1]    BIT STRING,
     octetstring                [2]    OCTET STRING (SIZE (0..127, ...)),
     universalString            [3]    UniversalString,
     beaconId                   [4]    BeaconID,
     t-apdu                     [5]    T-APDUs,
     dsrcApplicationEntityId    [6]    DSRCApplicationEntityID,
     dsrc-Ase-Id                [7]    Dsrc-EID,
     attrIdList                 [8]    AttributeIdList,
     attrList                   [9]    AttributeList{RtmContainer},
     reserved10                 [10]   NULL,
     OwsContextmark             [11]   Ows-ContextMark,
     OwsData                    [12]   OwsData,
     reserved13                 [13]   NULL,
     reserved14                 [14]   NULL,
     time                       [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
     }}

END
```

▼B

5.5.6 *Az OwsData elemei, elvégzett műveletek és fogalommeghatározások*

Az OwsData elemeinek meghatározása támogatja a nehéz tehergépjárművek maximális tömegéről és méreteiről szóló 2015/719/EK irányelvet. Jelentésük a következő:

— recordedWeight a tehergépjárműnek az EN ISO 14906 szabványnak megfelelően, 10 kg-os felbontással mért össztömege. Például a 2 500-as érték 25 tonna tömegnek felel meg.

— axlesConfiguration a tengelyek számával ábrázolja a tehergépjármű-összeállítást. A konfiguráció meghatározása 20 bites bitmaszkkal történik (az EN ISO 14906 alapján kibővítve).

Egy 2 bites bitmaszk egy tengely konfigurációjának felel meg a következő formátumban:

— A 00B érték azt jelenti, hogy az érték „nem áll rendelkezésre”, mivel a jármű nem rendelkezik a tengelyre jutó terhelés adatának gyűjtéséhez szükséges berendezéssel.

— A 01B érték azt jelenti, hogy a tengely nincs jelen.

— A 10B érték azt jelenti, hogy a tengely jelen van, a tömeg kiszámítása és az adatgyűjtés megtörtént, és az adat az axlesRecordedWeight mezőben elérhető.

— A 11B érték jövőbeni használatára van fenntartva.

Az utolsó 4 bit jövőbeli használatára van fenntartva.

A tengelyek száma										
A vontató tengelyeinek száma			A pótkocsi tengelyeinek száma							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bit)

— axlesRecordedWeight az egyes tengelyeken mért tömeget adja meg 10 kg-os felbontással. Minden egyes tengelyt két oktett képvisel. Például a 150-es érték 1 500 kg tömegnek felel meg.

A többi adattípus meghatározása az 5.4.5. pontban található.

5.5.7 *Adatátviteli mechanizmusok*

DSC_64 OWS adatok esetében a lekérdező és a járműben található DSRC eszköz közötti adatátvitel mechanizmusa ugyanaz, mint RTM adatok esetében (lásd az 5.4.6. pontot).

DSC_65 A maximális tömegadatokat gyűjtő platform és a járműben található DSRC eszköz közötti adatátvitelnek az 5.6. pontban meghatározott fizikai kapcsolaton, interfészeken és protokollon kell alapulnia.

5.6 **A DSRC-VU és a járműegység (VU) közötti adatátvitel**

5.6.1 *Fizikai kapcsolat és interfészek*

DSC_66 A járműegység (VU) és a *DSRC-VU* közötti kapcsolat lehet fizikai, vezetékes kapcsolat vagy Bluetooth v4.0 BLE technológián alapuló, rövid hatótávolságú, vezeték nélküli adatátvitel.

▼B

DSC_67 A választott fizikai kapcsolattól és interfésztől függetlenül a következő követelményeknek teljesülniük kell:

DSC_68 a) Annak érdekében, hogy a járműegység (VU) és a DSRC-VU, illetve különböző DSRC-VU tételek szállítására különböző szállítókkal lehessen szerződést kötni, a járműegység (VU) és a DSRC-VU közötti kapcsolatnak nyílt szabványon alapuló kapcsolatnak kell lennie. A járműegységnek (VU) a következők egyikével kell kapcsolódnia a DSRC-VU-hoz:

i) legalább 2 méter hosszú, rögzített vezeték a DIN 41612 szabványnak megfelelő H11 csatlakozóval – 11 pólusú csatlakozódugasz a DSRC-VU-tól, amely összeillik a járműegység készülékének hasonló, DIN/ISO szabvány szerinti csatlakozóaljzatával,

ii) alacsony energiafelhasználású Bluetooth-technológia (BLE),

iii) szabványos, az ISO 11898 vagy az SAE J1939 szabványnak megfelelő kapcsolat.

DSC_69 b) az interfészek, valamint a járműegység (VU) és a DSRC-VU közötti kapcsolat meghatározásának támogatnia kell az 5.6.2. pontban meghatározott alkalmazásprotokoll-parancsokat, és

DSC_70 c) a járműegységnek (VU) és a DSRC-VU-nak egyaránt támogatnia kell a kapcsolaton keresztül történő adatátvitelt a teljesítmény és az energiaellátás tekintetében.

5.6.2 *Alkalmazási protokoll*

DSC_71 A járműegység (VU) távoli kommunikációs eszköze és a DSRC-VU közötti alkalmazásprotokoll feladata, hogy időközönként továbbítsa a távoli kommunikációs adatokat a járműegységtől (VU) a DSRC-nek.

DSC_72 A fő parancsok meghatározása a következő:

1. A kommunikációs kapcsolat inicializálása – Kérés

2. A kommunikációs kapcsolat inicializálása – Válasz

3. Adatok küldése az RTM alkalmazás és az RTM adatok által meghatározott hasznos adatok azonosítójával

4. Az adatok visszaigazolása

5. A kommunikációs kapcsolat befejezése – Kérés

6. A kommunikációs kapcsolat befejezése – Válasz

DSC_73 Az ASN1.0 szerint az előző parancsok a következőképpen határozhatók meg:

▼B

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 A parancsok és a paraméterek leírása a következő:

— Az `RCDT-Communication Link Initialization - Request` a kommunikációs kapcsolat inicializálására szolgál. A parancsot a járműegység (VU) küldi a DSRC-VU-nak. A LinkIdentifier-t a járműegység (VU) állítja be és küldi a DSRC-VU-nak egy meghatározott kommunikációs kapcsolat nyomon követésére.

(*Megjegyzés:* Ez a jövőbeli kapcsolatok és olyan egyéb alkalmazások/modulok támogatására szolgál, mint a járművek tömegének fedélzeti mérése).

— Az `RCDT-Communication Link Initialization - Response` választ a DSRC-VU a kommunikációs kapcsolat inicializálására irányuló kérésre adott válaszként alkalmazza. A parancsot a DSRC-VU küldi a járműegységnek (VU). A parancs az inicializálás eredményét úgy adja meg, hogy a válasz = 1 (siker) vagy =0 (hiba).

DSC_75 A kommunikációs kapcsolat inicializálását csak azt követően kell elvégezni, hogy megtörtént a telepítés, a kalibrálás és a motor/járműegység (VU) bekapcsolása.

▼B

— Az RCDT-Send Data révén a járműegység (VU) elküldi az aláírt RCDTData adatokat (azaz *a távoli kommunikációs adatokat*) a DSRC-VU-nak. Az adatok továbbítására 60 másodpercenként kerül sor. A DataTransactionId paraméter azonosítja az adott adatátvitelt. A LinkIdentifier annak biztosítására is szolgál, hogy a megfelelő kapcsolat helyes legyen.

— Az RCDT-Data Acknowledgment parancsot a DSRC-VU küldi, hogy visszajelzést adjon a járműegységnek (VU) arról, hogy megkapta az adatokat a DataTransactionId paraméter által azonosított RCDT-Send Data parancs nyomán. A válasz paramétere = 1 (siker) vagy = 0 (hiba). Ha a járműegység (VU) több mint három 0-val egyenlő választ kap, vagy ha a járműegység (VU) nem kap RCDT Data Acknowledgement visszaigazolást egy korábban elküldött, egy meghatározott DataTransactionId paraméter által azonosított RCDT–Send Data parancs nyomán, akkor a járműegység (VU) eseményt generál és rögzít.

— Az RCDT-Communication Link Termination request kérést a járműegység (VU) küldi a DSRC-VU-nak, hogy lezárjon egy meghatározott LinkIdentifier azonosítóhoz tartozó kapcsolatot.

DSC_76 A DSRC-VU vagy egy járműegység (VU) újraindításakor a meglévő kommunikációs kapcsolatokat el kell távolítani, mivel a járműegység (VU) hirtelen leállása miatt még lehetnek függőben lévő kapcsolatok.

— Az RCDT-Communication Link Termination – Response választ a DSRC-VU küldi a járműegységnek (VU), hogy visszaigazolja a járműegység (VU) meghatározott LinkIdentifier azonosítóhoz tartozó kapcsolat lezárására irányuló kérését.

5.7 **Hibakezelés**

5.7.1 *Az adatok rögzítése és közlése az DSRC-VU-ban*

DSC_77 A már biztonságos *adatot* a *VUSM* funkciónak kell szolgáltatnia a *DSRC-VU* számára. A *VUSM*-nek ellenőriznie kell, hogy a *DSRC-VU*-ban rögzített adat megfelelően lett-e rögzítve. A járműegységből (*VU*) a *DSRC-VU* memóriájába történő adatátvitel hibáit EventFaultType típusú, ‘62’H enumerációs értékű Remote Communication Facility communication fault eseményként kell rögzíteni és jelenteni az időbélyegzővel együtt.

DSC_78 A járműegységnek (VU) fenn kell tartania egy, az ellenőrök által könnyen azonosítható, egyedi névvel ellátott fájlt a járműegység (VU) belső kommunikációs hibáinak („VU internal communication failures”) rögzítése érdekében.

DSC_79 Ha a VUPM kísérletet tesz arra, hogy VU adatokat szerezzen meg a biztonsági modultól (hogy továbbítsa azokat a VU-DSRC-nek), de nem jár sikerrel, ezt a hibát EventFaultType típusú, *‘62’H* enumerációs értékű *Remote Communication Facility communication fault* eseményként kell rögzítenie az időbélyegzővel együtt. A kommunikációs hiba felismerése

▼B

akkor történik, amikor egy `RCDT Send Data` parancsra válaszul egymás után több mint háromszor nem érkezik meg a hozzá kapcsolódó `RCDT Data Acknowledgment` üzenet (azaz ugyanazzal a DataTransactionId azonosítóval a `Send Data and Acknowledgment` üzenetek között).

5.7.2 *A vezeték nélküli kommunikáció hibái*

DSC_80 A kommunikációs hiba kezelésének meg kell felelnie a vonatkozó DSRC szabványoknak, nevezetesen az EN 300 674-1, az EN 12253, az EN 12795 és az EN 12834 szabványnak, valamint az EN 13372 szabvány megfelelő paramétereinek.

5.7.2.1 *Titkosítási és aláíráshibák*

DSC_81 A titkosítási és aláíráshibákat a 11. függelékben (Közös biztonsági mechanizmusok) meghatározott módon kell kezelni, és ezek a hibák nem jelennek meg a DSRC adatátvitellel kapcsolatos hibaüzenetekben.

5.7.2.2 *A hibák rögzítése*

A DSRC dinamikus vezeték nélküli kommunikáció olyan környezetben működik, amelyben bizonytalanok a légköri és az interferencia-feltételek, különösen a hordozható REDCR és mozgó jármű kombinációjával működő alkalmazásban. Ezért különbséget kell tenni az „olvasási hiba” és a „hiba” feltétele között. Egy vezeték nélküli interfészen keresztülfutó tranzakció esetében általános az olvasási hiba, amelynek általában az a következménye, hogy ismételt kísérletet kell tenni, azaz újra el kell küldeni a BST-t és a szekvenciát, ami a legtöbb esetben sikeres kommunikációs kapcsolathoz és adatátvitelhez vezet, hacsak a megcélzott jármű az ismételt küldéshez szükséges idő alatt ki nem kerül a hatótávolságból. (Egy sikeres olvasás több kísérlet és ismételt próbálkozás eredménye is lehet).

Olvasási hibát okozhat, ha az antennák párosítása nem megfelelő (hibás irányítás), ha az egyik antenna le van árnyékolva (ami lehet szándékos, de egy másik jármű jelenléte is okozhatja), ha rádióinterferencia lép fel különösen 5,8 GHz-hez közeli frekvencián működő WIFI-vel vagy egyéb nyílt hozzáférésű, vezeték nélküli kommunikációval, de okozhatja radarinterferencia vagy kedvezőtlen légköri körülmény (pl. vihar), vagy egyszerűen a DSRC kommunikáció hatósugarából való kikerülés. Az egyedi olvasási hibákat természetüknél fogva nem lehet rögzíteni, egyszerűen azért, mert a kommunikációra nem került sor.

Amennyiben azonban az illetékes ellenőrző hatóság meghatalmazottja megcéloz egy járművet, és kísérletet tesz a *DSRC-VU* kiolvasására, de ezt nem követi sikeres adatátvitel, ez a hiba lehet szándékos manipulálás következménye, ezért az illetékes ellenőrző hatóság meghatalmazottjának megfelelő eszközzel kell rendelkeznie arra, hogy naplózza a hibát, és riassza a távolabb lévő kollégákat az esetleges jogsértés miatt. Ezután a kollégák megállíthatják a járművet, és elvégezhetik annak fizikai ellenőrzését. Mivel azonban nem történt sikeres kommunikáció, a DSRC-VU nem képes adatokat szolgáltatni a hibáról. Ez a jelentés ezért az REDCR berendezés kialakításának függvénye lesz.

Az „olvasási hiba” technikai értelemben eltér a „hibától”. Ebben az összefüggésben a „hiba” azt jelenti, hogy a kapott érték helytelen.

▼B

A *DSRC-VU*-nak továbbított adatok már biztonságosak, ezért azokat az adatok szolgáltatójának kell ellenőriznie (lásd az 5.4. pontot).

A későbbiekben rádióinterfészen továbbított adatok ellenőrzése a kommunikáció szintjén, ciklikus redundanciaellenőrzéssel történik. Ha a ciklikus redundanciaellenőrzés érvényesíti, akkor az adat helyes. Ha a ciklikus redundanciaellenőrzés nem érvényesíti, akkor az adat ismételten továbbításra kerül. Annak valószínűsége, hogy helytelen adatok sikeresen átjutnak a ciklikus redundanciaellenőrzésen, statisztikailag annyira kicsi, hogy figyelmen kívül hagyható.

Ha a ciklikus redundanciaellenőrzés nem érvényesíti az adatot, és nincs idő a helyes adat ismételt továbbítására és fogadására, akkor az eredmény nem hiba lesz, hanem egy speciális olvasásihiba-típus egy példánya.

Az egyedüli értelmezhető hibaadat, amely rögzíthető, az olyan, sikeresen kezdeményezett tranzakciók száma, amelyek nem végződtek az REDCR-nek történő sikeres adatátvitelben.

DSC_82 Az *REDCR* ezért időbélyegzővel ellátva rögzíti azon alkalmak számát, amikor egy DSRC lekérdezés inicializálási szakasza sikeres, de a tranzakció azelőtt befejeződik, hogy az REDCR sikeresen lekérdezné az *adatokat*. Ennek az adatnak hozzáférhetőnek kell lennie az illetékes ellenőrző hatóság meghatalmazottja számára, és az adatot el kell tárolni az REDCR berendezés memóriájában. Ennek megvalósítási módja a termékfejlesztésen vagy az illetékes ellenőrző hatóság előírásán múlik.

Az egyedüli értelmezhető hibaadat, amely rögzíthető, azon alkalmak száma, amikor az REDCR nem képes visszafejteni a kapott *adatokat*. Meg kell azonban jegyezni, hogy ez csak az REDCR szoftver hatékonyságára vonatkozik. Előfordulhat, hogy az adatokat technikailag vissza lehet fejteni, de szemantikailag nincs értelmük.

DSC_83 Az *REDCR* ezért időbélyegzővel ellátva rögzíti azon alkalmak számát, amikor sikertelen kísérletet tett a DSRC interfészen keresztül kapott adatok visszafejtésére.

6 A TÁVOLI KOMMUNIKÁCIÓS FUNKCIÓ ÜZEMBE HELYEZÉSE ÉS IDŐSZAKOS VIZSGÁLATA

6.1 **Általános rész**

DSC_84 A távoli kommunikációs funkció esetében a tervek a tesztek két típusát tartalmazzák:

1) ECHO teszt a *DSRC-REDCR >>-:-<DSRC-VU vezeték nélküli* kommunikációs csatorna érvényesítésére;

2) a folyamat elejétől a végéig tartó biztonsági teszt annak biztosítása érdekében, hogy egy műhelykártyával hozzá lehessen férni a járműegység (VU) által létrehozott, titkosított és aláírással ellátott, és a vezeték nélküli kommunikációs csatornán keresztül továbbított adattartalomhoz.

6.2 **ECHO**

Ez a pont olyan rendelkezéseket tartalmaz, amelyek kifejezetten annak tesztelésére szolgálnak, hogy a *DSRC-REDCR >>-:-<DSRC-VU* kapcsolat funkcionálisan aktív-e.

▼B

Az ECHO parancs célja az, hogy lehetővé tegye a műhelyek és a típusjóváhagyási vizsgálatokat végző létesítmények számára, hogy biztonsági hitelesítő adatokhoz való hozzáférés nélkül meg tudják vizsgálni, hogy működik-e a DSRC kapcsolat. A tesztelő berendezésének ezért csak arra kell képesnek lennie, hogy DSRC kommunikációt inicializáljon (BST-t küldjön olyan szolgáltatást kérve amelynek az AID értéke = 2), majd ECHO parancsot küldjön, és feltételezve, hogy a DSRC működik, fogadja az ECHO választ. További részletekért lásd az 5.4.8. pontot. Amennyiben a helyes válasz megérkezik, igazolni lehet, hogy a DSRC kapcsolat (*DSRC-REDCR* >>-:-<*DSRC-VU*) helyesen működik.

6.3 **A biztonsági adatok tartalmának érvényesítésére szolgáló tesztek**

DSC_85 Ezt a tesztet az adatfolyam folyamat elejétől a végéig tartó biztonságának igazolására hajtják végre. Ilyen teszthez DSRC tesztleolvasó szükséges. A DSRC tesztleolvasó ugyanazokkal a funkciókkal rendelkezik, és megvalósítása ugyanazon előírások szerint történik, mint a bűnüldöző szervek által használt leolvasó esetében, azzal a különbséggel, hogy a DSRC tesztleolvasó felhasználójának azonosítására nem ellenőrző kártyát, hanem műhelykártyát kell használni. A tesztet az intelligens menetíró készülék kezdeti aktiválását követően vagy a kalibrálási eljárás végén lehet végrehajtani. Aktiválás után a járműegység generálja a biztonságos korai észlelési adatokat, és továbbítja azokat a DSRC-VU-nak.

DSC_86 A műhely személyzetének a jármű előtt 2 és 10 méter közötti távolságban kell elhelyeznie a DSRC tesztleolvasót.

DSC_87 Ezután a műhely személyzete műhelykártyát helyez a DSRC tesztleolvasóba, hogy a járműegységtől (VU) kérje a korai észlelési adatok lekérését. A sikeres lekérdezés után a műhely személyzete hozzáfér a kapott adatokhoz, hogy megvizsgálja, sikeres volt-e az adatok sértetlenségének validálása és az adatok visszafejtése.

▼B

15. Függelék

MIGRÁLÁS: KÜLÖNFÉLE GENERÁCIÓJÚ KÉSZÜLÉKEK EGYÜTTES MŰKÖDTETÉSE

TARTALOMJEGYZÉK

1. FOGALOMMEGHATÁROZÁSOK

2. ÁLTALÁNOS ELŐÍRÁSOK

2.1. A rendszerek közötti váltás áttekintése

2.2. A járműegység és a kártyák közötti interoperabilitás

2.3. A járműegység és a mozgásérzékelő közötti interoperabilitás

2.4. A járműegységek, tachográfkártyák és adatletöltésre szolgáló berendezések közötti interoperabilitás

2.4.1 Az ide általi közvetlen kártyaletöltés

2.4.2 Járműegységen keresztül történő kártyaletöltés

2.4.3 Járműegység adatainak letöltése

2.5. A járműegység és a kalibrálóberendezés közötti interoperabilitás

3. A BEVEZETÉS IDŐPONTJA ELŐTTI IDŐSZAKBAN ELVÉGZENDŐ FŐBB INTÉZKEDÉSEK

4. A BEVEZETÉS IDŐPONTJA UTÁNI IDŐSZAKRA VONATKOZÓ RENDELKEZÉSEK

1. FOGALOMMEGHATÁROZÁSOK

E függelék alkalmazásában a következő fogalommeghatározásokat kell használni:

intelligens menetíró rendszer*:* e melléklet meghatározása szerint (1. fejezet, bbb. fogalommeghatározás);

első generációs menetíró rendszer*:* e rendelet meghatározása szerint (2. cikk, 1. fogalommeghatározás);

második generációs menetíró rendszer*:* e rendelet meghatározása szerint (2. cikk, 7. fogalommeghatározás);

a bevezetés időpontja*:* e melléklet meghatározása szerint (1. fejezet, ccc. fogalommeghatározás);

intelligens kijelölt berendezés (IDE)*:* az e melléklet 7. függelékében meghatározott, adatletöltéshez használt berendezés.

2. ÁLTALÁNOS ELŐÍRÁSOK

2.1. **A rendszerek közötti váltás áttekintése**

E melléklet bevezetése az első és második generációs menetíró rendszerek közötti váltásról nyújt áttekintést.

A bevezetésben foglalt előírások mellett a következők is érvényesek:

— az első generációs mozgásérzékelők nem lesznek interoperábilisak a második generációs járműegységekkel;

— a második generációs mozgásérzékelőket a második generációs járműegységekkel egy időben kezdik majd beszerelni a járműegységekbe;

▼B

— az adatletöltésre és kalibrálásra szolgáló berendezéseket tovább kell fejleszteni, hogy támogatni tudják az adatrögzítő készülékek és tachográfkártyák mindkét generációjának használatát.

2.2. **A járműegység és a kártyák közötti interoperabilitás**

Ismeretes, hogy az első generációs tachográfkártyák interoperábilisak az első generációs járműegységekkel (e rendelet 1B. mellékletének megfelelően), a második generációs tachográfkártyák pedig interoperábilisak a második generációs járműegységekkel (e rendelet 1C. mellékletének megfelelően). Ezenkívül az alábbi követelményeket kell alkalmazni.

MIG_001 A MIG_004 és MIG_005 követelményben előírtak kivételével az első generációs tachográfkártyák érvényességi idejük végéig továbbra is használhatók a második generációs járműegységekben. Azonban amint rendelkezésre állnak a második generációs tachográfkártyák, az első generációs tachográfkártyák birtokosai kérhetik ezek második generációsra való kicserélését.

MIG_002 A második generációs járműegységeknek alkalmasnak kell lenniük bármely érvényes első generációs járművezetői, ellenőrző- és vállalkozáskártya használatára.

MIG_003 A műhelyek végleg megszüntethetik az ilyen járműegységek e képességét annak érdekében, hogy a járműegységek első generációs tachográfkártyákkal ne legyenek használhatók. Ezt csak azután lehet elvégezni, hogy az Európai Bizottság eljárást indított, melyben felkéri a műhelyeket e művelet elvégzésére, például a menetíró készülékek időszakos vizsgálata keretében.

MIG_004 A második generációs járműegységek csak második generációs műhelykártyák használatára lehetnek alkalmasak.

MIG_005 Az üzemeltetési mód meghatározása céljából a második generációs járműegységek csak az érvényes kártyák típusát vehetik figyelembe, függetlenül a kártyák generációjától.

MIG_006 Bármely érvényes második generációs tachográfkártyának ugyanolyan módon alkalmasnak kell lennie az első generációs járműegységekben való használatra, mint az ugyanolyan típusú első generációs tachográfkártyának.

2.3. **A járműegység és a mozgásérzékelő közötti interoperabilitás**

Ismeretes, hogy az első generációs mozgásérzékelők interoperábilisak az első generációs járműegységekkel, a második generációs mozgásérzékelők pedig interoperábilisak a második generációs járműegységekkel. Ezenkívül az alábbi követelményeket kell alkalmazni.

MIG_007 A második generációs járműegységek nem lesznek alkalmasak az első generációs mozgásérzékelőkkel való összekapcsolásra és használatra.

MIG_008 A második generációs mozgásérzékelőket úgy kell kialakítani, hogy vagy csak második generációs járműegységekkel, vagy első és második generációs járműegységekkel is párosíthatók és használhatók legyenek.

2.4. **A járműegységek, tachográfkártyák és adatletöltésre szolgáló berendezések közötti interoperabilitás**

MIG_009 Az adatletöltésre szolgáló berendezés használható a járműegységek és tachográfkártyák csak egyik vagy mindkét generációjával is.

▼B

2.4.1 *Az IDE általi közvetlen kártyaletöltés*

MIG_010 Az IDE-nek a kártyaolvasóba helyezett tachográfkártyák egyik generációjának adatait kell letöltenie az adott generációra vonatkozó biztonsági eljárások és adatletöltési protokollok segítségével, a letöltött adatoknak pedig az adott generációra előírt formátumúnak kell lenniük.

MIG_011 Annak érdekében, hogy nem uniós ellenőrző hatóságok is ellenőrizhessék a járművezetőket, lehetővé kell tenni, hogy a második generációs járművezetői kártyákat (és műhelykártyákat) ugyanolyan módon lehessen letölteni, mint az első generációs járművezetői kártyákat (és műhelykártyákat). Az ilyen letöltésnek ki kell terjednie a következőkre:

— a következő alá nem írt EF-ek: `IC` és `ICC`;

— a következő alá nem írt (első generációs) EF-ek: `Card_Certificate` és `CA_Certificate`;

— az első generációs adatletöltési protokoll szerint előírt egyéb alkalmazási adatokat tartalmazó EF-ek (a `TACHO` DF-en belül). Ezeket az információkat digitális aláírással kell ellátni az első generációs biztonsági eljárásoknak megfelelően.

Az ilyen letöltésnek nem kell kiterjednie a csak a második generációs járművezetői kártyákon (és műhelykártyákon) szereplő alkalmazási adatokat tartalmazó EF-ekre (a `TACHO_G2` DF-en belüli, alkalmazási adatokat tartalmazó EF-ekre).

2.4.2 *Járműegységen keresztül történő kártyaletöltés*

MIG_012 Ha egy első generációs járműegységbe második generációs kártyát helyeznek be, az adatletöltésnek az első generációs adatletöltési protokollnak megfelelően kell történnie. A kártyának ugyanúgy kell válaszolnia a járműegység parancsaira, mint egy első generációs kártyának, a letöltött adatok formátumának pedig meg kell egyeznie az első generációs kártyákról letöltött adatok formátumával.

MIG_013 Ha egy második generációs járműegységbe első generációs kártyát helyeznek be, az adatletöltésnek az e melléklet 7. függelékében meghatározott adatletöltési protokoll szerint kell történnie. A járműegységnek ugyanolyan módon kell parancsokat küldenie a kártyának, mintha első generációs járműegység lenne, a letöltött adatok formátumának pedig meg kell felelnie az első generációs kártyákra vonatkozóan előírt formátumnak.

2.4.3 *Járműegység adatainak letöltése*

MIG_014 A második generációs járműegységekből való adatletöltés során a második generációs biztonsági eljárásokat és az e melléklet 7. függelékében meghatározott adatletöltési protokollt kell alkalmazni.

MIG_015 Annak érdekében, hogy nem uniós ellenőrző hatóságok is ellenőrizhessék a járművezetőket és nem uniós műhelyek is letölthessék a járműegységek adatait, opcionálisan lehetséges a második generációs járműegységek adatainak az első generációs biztonsági eljárásokkal és az első generációs adatletöltési protokollal való letöltése is. A letöltött adatok formátumának meg kell egyeznie az első generációs járműegységekből letöltött adatok formátumával. Ezt a funkciót a menü parancsai segítségével lehet kiválasztani.

▼B

2.5. **A járműegység és a kalibrálóberendezés közötti interoperabilitás**

MIG_016 A kalibrálóberendezésnek alkalmasnak kell lennie arra, hogy a menetíró készülékek mindkét generációját kalibrálja az adott generációra vonatkozó kalibrálási protokoll szerint. A kalibrálóberendezés használható a menetíró készülékek csak egyik vagy mindkét generációjával is.

3. A BEVEZETÉS IDŐPONTJA ELŐTTI IDŐSZAKBAN ELVÉGZENDŐ FŐBB INTÉZKEDÉSEK

MIG_017 A tesztkulcsokat és -tanúsítványokat a bevezetés időpontja előtt legalább **30 hónappal** a gyártók rendelkezésére kell bocsátani.

MIG_018 Az interoperabilitási teszteknek legkésőbb **15 hónappal** a bevezetés időpontja előtt készen kell állniuk a gyártók kérésére történő elindításra.

MIG_019 A hivatalos kulcsokat és tanúsítványokat a bevezetés időpontja előtt legalább **12 hónappal** a gyártók rendelkezésére kell bocsátani.

MIG_020 A tagállamoknak legkésőbb a bevezetés időpontja előtt **3 hónappal** készen kell állniuk a második generációs műhelykártyák kibocsátására.

MIG_021 A tagállamoknak legkésőbb **a bevezetés időpontja előtt 1 hónappal** készen kell állniuk valamennyi típusú második generációs tachográfkártya kibocsátására.

4. A BEVEZETÉS IDŐPONTJA UTÁNI IDŐSZAKRA VONATKOZÓ RENDELKEZÉSEK

MIG_022 A bevezetés időpontja után a tagállamok csak második generációs tachográfkártyákat bocsáthatnak ki.

MIG_023 Amíg az első generációs járműegységek/mozgásérzékelők használatban vannak, a járműegységek/mozgásérzékelők gyártói továbbra is gyárthatnak ilyen eszközöket a hibás alkatrészek cseréje céljából.

MIG_024 A járműegységek/mozgásérzékelők gyártói számára lehetővé kell tenni, hogy a már jóváhagyott típusú első generációs járműegységekre/mozgásérzékelőkre vonatkozóan a típusjóváhagyás fenntartását kérelmezzék és megkapják.

▼B

16. Függelék

AZ M1 ÉS N1 KATEGÓRIÁJÚ JÁRMŰVEKBE ÉPÍTENDŐ ADAPTER

TARTALOMJEGYZÉK

1. RÖVIDÍTÉSEK ÉS REFERENCIADOKUMENTUMOK

1.1. Rövidítések

1.2. Szabványhivatkozások

2. AZ ADAPTER ÁLTALÁNOS JELLEMZŐI ÉS FUNKCIÓI

2.1. Az adapter általános leírása

2.2. Funkciók

2.3. Biztonság

3. AZ ADATRÖGZÍTŐ KÉSZÜLÉKRE VONATKOZÓ KÖVETELMÉNYEK ADAPTER ALKALMAZÁSA ESETÉN

4. AZ ADAPTER KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

4.1. A bejövő sebességimpulzusok közvetítése és átalakítása

4.2. A bejövő impulzusok továbbítása a beépített mozgásérzékelő felé

4.3. A beépített mozgásérzékelő

4.4. Biztonsági követelmények

4.5. Teljesítményjellemzők

4.6. Anyagok

4.7. Jelölések

5. AZ ADATRÖGZÍTŐ KÉSZÜLÉK BEÉPÍTÉSE ADAPTER ALKALMAZÁSA ESETÉN

5.1. Beépítés

5.2. Plombálás

6. ELLENŐRZÉS, FELÜLVIZSGÁLAT ÉS JAVÍTÁSOK

6.1. Időszakos felülvizsgálatok

7. AZ ADATRÖGZÍTŐ KÉSZÜLÉK TÍPUSJÓVÁHAGYÁSA ADAPTER ALKALMAZÁSA ESETÉN

7.1. Általános szempontok

7.2. Működési tanúsítvány

1. RÖVIDÍTÉSEK ÉS REFERENCIADOKUMENTUMOK

1.1. **Rövidítések**

TBD meghatározandó

VU járműegység

1.2. **Szabványhivatkozások**

ISO16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

2. AZ ADAPTER ÁLTALÁNOS JELLEMZŐI ÉS FUNKCIÓI

2.1. **Az adapter általános leírása**

ADA_001 Az adapter feladata, hogy folyamatosan biztonságos mozgásadatokat szolgáltasson a vele összeköttetésben álló járműegységnek (VU) a jármű sebességéről és a megtett távolságról.

Az adapter csak azon járművek esetében alkalmazandó, amelyeket e rendelet értelmében adatrögzítő készülékkel kell felszerelni.

▼B

Csak az IC. melléklet yy) pontja szerinti „adapter” fogalommeghatározásban meghatározott azon járműkategóriák esetében építik be és alkalmazzák, amelyekbe mechanikai okokból nem építhető be olyan egyéb típusú meglévő mozgásérzékelő, amely egyébként megfelel az e mellékletben és e melléklet 1–16. függelékében foglalt előírásoknak.

Az adapter nem csatlakozik mechanikusan a jármű valamely mozgó alkatrészéhez, hanem az integrált érzékelők vagy alternatív interfészek által a sebességre/megtett útra vonatkozóan generált impulzusokat fogadja.

ADA_002 A típusjóváhagyással rendelkező mozgásérzékelőt (megfelelően az IC melléklet 8. szakaszának: Az adatrögzítő készülék és a tachográfkártyák típusjóváhagyása) az adapter burkolatán belülre kell beépíteni, ahol egy, a beépített mozgásérzékelő számára továbbítandó impulzusokat előállító impulzusátalakító is helyet foglal. A beépített mozgásérzékelő a járműegységhez (VU) kapcsolódik, így a járműegység és az adapter közötti interfésznek meg kell felelnie az ISO 16844-3 szabványban foglalt előírásoknak.

2.2. **Funkciók**

ADA_003 Az adapter a következő funkciókat látja el:

— a bejövő sebességimpulzusok közvetítése és átalakítása,

— a bejövő impulzusok továbbítása a beépített mozgásérzékelő felé,

— a mozgásérzékelő valamennyi funkciója, valamint a járműegység (VU) biztonságos mozgásadatokkal történő ellátása.

2.3. **Biztonság**

ADA_004 Az adapter biztonsági tanúsítása nem a mozgásérzékelőkre vonatkozó, az e melléklet 10. függelékében meghatározott általános biztonsági célok alapján történik. E helyett az e függelék 4.4. pontjában meghatározott biztonsági vonatkozású követelményeket kell alkalmazni.

3. AZ ADATRÖGZÍTŐ KÉSZÜLÉKRE VONATKOZÓ KÖVETELMÉNYEK ADAPTER ALKALMAZÁSA ESETÉN

A következő fejezetekben foglalt követelmények arra vonatkoznak, hogy adapter alkalmazása esetén miként kell az e mellékletben foglalt előírásokat értelmezni. Az IC melléklet érintett előírásának száma zárójelben szerepel.

ADA_005 Ha e függelék másként nem írja elő, az adapterrel felszerelt járművekben használt adatrögzítő készüléknek meg kell felelnie e melléklet valamennyi előírásának.

ADA_006 Adapter alkalmazása esetén az adatrögzítő készülék magában foglalja a kábeleket, az adaptert (a mozgásérzékelőt is beleértve) és egy járműegységet (VU) [01].

ADA_007 Az adatrögzítő készülék esemény- és/vagy hibafelderítő funkciója az alábbiak szerint módosul:

— az „áramellátás megszakadása” eseményt a járműegység (VU) abban az esetben váltja ki, amikor a berendezés nincs a kalibrálási üzemmódban, és a beépített mozgásérzékelő bármely áramkimaradása meghaladja a 200 milliszekundumot [79],

▼B

— „a mozgásra vonatkozó adatok hibája” eseményt a járműegység (VU) abban az esetben váltja ki, ha megszakad a normál adatfolyam a beépített mozgásérzékelő és a járműegység között és/vagy ha hiba lép fel az adatintegritásban vagy adathitelesítésben a beépített mozgásérzékelő és a járműegység közötti adatcsere folyamán [83],

— „a biztonsági rendszer megsértésére irányuló kísérlet” eseményt a járműegység (VU) minden más, a beépített mozgásérzékelő biztonságát érintő eseménykor kiváltja, amikor a berendezés nincs a kalibrálási üzemmódban [85],

— „az adatrögzítő készülék hibája” eseményt a járműegység (VU) a beépített mozgásérzékelő bármely hibája esetén kiváltja, amikor a berendezés nincs a kalibrálási üzemmódban [88].

ADA_008 Az adatrögzítő készülék az adapternek a beépített mozgásérzékelővel kapcsolatos hibáit érzékeli [88].

ADA_009 A VU-kalibrálási funkció lehetővé teszi a beépített mozgásérzékelő automatikus összekapcsolását a járműegységgel [202, 204].

4. AZ ADAPTER KIALAKÍTÁSÁRA ÉS MŰKÖDÉSÉRE VONATKOZÓ KÖVETELMÉNYEK

4.1. **A bejövő sebességimpulzusok közvetítése és átalakítása**

ADA_011 Az adapter bemeneti interfésze a jármű sebességét és a megtett távolságot jelző impulzusokat képes fogadni. A bejövő impulzusok elektromos jellemzői: *a gyártó által meghatározandó*. A csak az adapter gyártója és az adapter beépítését végző elismert műhely számára ismert beállításoknak adott esetben lehetővé kell tenniük az adapter bemeneti oldalának megfelelő összekötését a járművel.

ADA_012 Az adapter bemeneti interfészének adott esetben képesnek kell lennie a bejövő sebességimpulzusok impulzusszámának egy rögzített tényezővel történő szorzására, illetve osztására, a jelet az e mellékletben meghatározott k-tényező tartományhoz (4 000–25 000 imp/km) igazítva. Ezt a rögzített tényezőt csak az adapter gyártója vagy az adapter beépítését végző elismert műhely táplálhatja be.

4.2. **A bejövő impulzusok továbbítása a beépített mozgásérzékelő felé**

ADA_013 A bejövő, adott esetben a fentiek szerint átalakított impulzusokat olyan módon kell a beépített mozgásérzékelőnek továbbítani, hogy az minden bejövő impulzust érzékeljen.

4.3. **A beépített mozgásérzékelő**

ADA_014 A beérkező jelek stimulálják a beépített mozgásérzékelőt, amely a jármű mozgását olyan pontosan leíró mozgásadatokat hoz létre, mintha mechanikus kapcsolatban állna a jármű valamely mozgó alkatrészével.

ADA_015 A járműegység (VU) a beépített mozgásérzékelő azonosító adatait használja az adapter azonosítására [95].

▼B

ADA_016 A beépített mozgásérzékelőben tárolt beépítési adatok minősülnek az adapter beépítési adatainak [122].

4.4. **Biztonsági követelmények**

ADA_017 Az adapter burkolatát úgy kell kialakítani, hogy azt ne lehessen felnyitni. Annak érdekében, hogy a fizikai manipulálási kísérletek könnyen észrevehetők legyenek (pl. szemrevételezéssel, ld. ADA_035), az adapter burkolatát le kell plombálni. A plombákra a mozgásérzékelő plombáira vonatkozó követelmények érvényesek [398–406].

ADA_018 A beépített mozgásérzékelőt kizárólag az adapter burkolatán lévő plomba (plombák) vagy az érzékelőt és az adapter burkolatát összekötő plomba feltörésével lehet eltávolítani (ld. ADA_034).

ADA_019 Az adapter biztosítja, hogy a mozgási adatokat kizárólag az adapter bemenetén keresztül lehessen lehívni és feldolgozni.

4.5. **Teljesítményjellemzők**

ADA_020 Az adapter a gyártó által meghatározott hőmérséklet-tartományban teljes mértékben működőképes.

ADA_021 Az adapter 10–90 %-os páratartalom mellett teljes mértékben működőképes [214].

ADA_022 Az adaptert óvni kell a túlfeszültségtől, az energiaellátás polaritásának felcserélésétől és a rövidzárlatoktól [216].

ADA_023 Az adapter:

— vagy reagál a jármű mozgásának érzékelését zavaró mágneses térre – ilyen körülmények esetén a járműegység (VU) érzékelőhibát jegyez fel és tárol [88], vagy

— olyan érzékelő elemmel rendelkezik, amely védett vagy ellenállóképes a mágneses térrel szemben [217].

ADA_024 Az adapter az elektromágneses kompatibilitás tekintetében megfelel az ENSZ-EGB 10. sz. előírásának, valamint az adaptert védeni kell az elektrosztatikus kisülésektől és tranziens áramoktól [218].

4.6. **Anyagok**

ADA_025 Az adapter megfelel a(z) (*a gyártó által meghatározandó, a beépítés helyének függvényében*) érintésvédelmi osztálynak [220, 221].

ADA_026 Az adapter burkolatának színe sárga.

4.7. **Jelölések**

ADA_027 Az adapterre ismertető címkét kell erősíteni, amelyen a következő adatok szerepelnek:

— az adapter gyártójának neve és címe,

— a gyártói alkatrészek száma és az adapter gyártási éve,

— az adapter vagy azt tartalmazó adatrögzítő készülék típusjóváhagyási jele,

— az adapter beépítésének időpontja,

▼B

— azon jármű alvázszáma, amelybe az adaptert beépítették.

ADA_028 Az ismertető címkén szerepelnek továbbá a következő adatok (amennyiben azok nem olvashatók le közvetlenül a beépített mozgásérzékelő burkolatáról):

— a beépített mozgásérzékelő gyártójának neve,

— a gyártói alkatrészek száma és a beépített mozgásérzékelő gyártási éve,

— a beépített mozgásérzékelő jóváhagyási jele.

5. AZ ADATRÖGZÍTŐ KÉSZÜLÉK BEÉPÍTÉSE ADAPTER ALKALMAZÁSA ESETÉN

5.1. **Beépítés**

ADA_029 A járművekbe szerelendő adaptereket csak járműgyártók, vagy jóváhagyott, digitális és intelligens menetíró készülékek beépítésére, aktiválására, illetve kalibrálására feljogosított műhelyek szerelhetik be.

ADA_030 Az adaptert beépítő jóváhagyott műhely beállítja a bemeneti interfészt és – adott esetben – kiválasztja a bemeneti jel konverziójának arányát.

ADA_031 Az adaptert beépítő jóváhagyott műhely leplombálja az adapter burkolatát.

ADA_032 Az adaptert a lehető legközelebb kell beszerelni a járműnek az adapter bejövő impulzusait küldő részéhez.

ADA_033 Az adapter tápkábele piros (pozitív) és fekete (föld).

5.2. **Plombálás**

ADA_034 A plombálásra az alábbi követelmények vonatkoznak:

— az adapter burkolatát plombával látják el (ld. ADA_017),

— a beépített érzékelő burkolatát plombával kell az adapter burkolatához kötni, kivéve, ha az érzékelő egyébként sem távolítható el az adapterburkolat plombájának (plombáinak) feltörése nélkül (ld. ADA_018),

— az adapter burkolatát plombával kell a járműhöz kötni,

— az adapter és az adapter bejövő impulzusait küldő berendezés közötti összekötő elemet – az ésszerűség határain belül – mindkét végén plombával kell ellátni.

6. ELLENŐRZÉS, FELÜLVIZSGÁLAT ÉS JAVÍTÁSOK

6.1. **Időszakos felülvizsgálatok**

ADA_035 Adapter alkalmazása esetén az adatrögzítő készülék minden egyes időszakos felülvizsgálata alkalmával az 1C. melléklet VI. fejezete 409–413. követelményeinek megfelelően az alábbiakat kell ellenőrizni:

— szerepel-e megfelelő típus-jóváhagyási jel az adapteren,

— sértetlenek-e az adapteren lévő plombák és csatlakozások,

▼B

— az adapter a beépítési címkén szereplő adatoknak megfelelően került-e beépítésre,

— az adapter a gyártója és/vagy a járműgyártó által meghatározott módon került-e beépítésre,

— jóváhagyták-e a vizsgált járműre vonatkozóan adapter beépítését.

ADA_036 Ezek a felülvizsgálatok kiterjednek az összes plomba kalibrálására és cseréjére, függetlenül azok állapotától.

7. AZ ADATRÖGZÍTŐ KÉSZÜLÉK TÍPUSJÓVÁHAGYÁSA ADAPTER ALKALMAZÁSA ESETÉN

7.1. **Általános szempontok**

ADA_037 Az adatrögzítő készüléket az adapterrel együtt kell jóváhagyásra benyújtani [425].

ADA_038 Az adapterek benyújthatók saját típusjóváhagyásuk vagy az adatrögzítő készülék részeként történő típusjóváhagyás céljából.

ADA_039 Az ilyen típusjóváhagyás keretében elvégzésre kerülnek az adaptert érintő működési tesztek is. Az egyes vizsgálatok kedvező eredményeit megfelelő tanúsítvány állapítja meg [426].

7.2. **Működési tanúsítvány**

ADA_040 Az adapterre, illetve adaptert tartalmazó adatrögzítő készülékre vonatkozó működési tanúsítványt az adapter gyártója részére csak akkor lehet kiadni, ha az adott készülék az alábbi alapvető működési tesztek közül valamennyinek megfelelt.

Szám	Teszt	Leírás	Kapcsolódó követelmények
1.	**Adminisztratív vizsgálat**		
1.1.	Dokumentáció	Az adapter dokumentációjának helyessége	
2.	**Szemrevételezés**		
2.1.	Az adapter megfelelése a dokumentációnak		
2.2.	Az adapter azonosítói/jelzései		ADA_027, ADA_028
2.3.	Az adapterhez felhasznált anyagok		[219]–[223] ADA_026
2.4.	Plombálás		ADA_017, ADA_018, ADA_034
3.	**Működési tesztek**		
3.1.	A sebességimpulzusok továbbítása a beépített mozgásérzékelő felé		ADA_013

▼B

Szám	Teszt	Leírás	Kapcsolódó követelmények
3.2.	A bejövő sebességimpulzusok közvetítése és átalakítása		ADA_011, ADA_012
3.3.	A mozgás mérésének pontossága		[30]–[35], [217]
4.	**Környezeti tesztek**		
4.1.	A gyártó tesztjeinek eredményei	A gyártó környezeti tesztjeinek eredményei	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromágneses összeférhetőség**		
5.1.	Sugárzás-kibocsátás és érzékenység	A 2006/28/EK irányelvnek való megfelelés ellenőrzése	ADA_024
5.2.	A gyártó tesztjeinek eredményei	A gyártó környezeti tesztjeinek eredményei	ADA_024

▼C1

II. MELLÉKLET

JÓVÁHAGYÁSI JEL ÉS TÍPUSBIZONYÍTVÁNY

I. JÓVÁHAGYÁSI JEL

1. A jóváhagyási jel a következőkből áll:

a) egy téglalap, amelyben egy „e” betű szerepel, ezt a jóváhagyást megadó ország megkülönböztető száma vagy betűje követi, a következő hagyományos jelöléseknek megfelelően:

Belgium	6
Bulgária	34
Cseh Köztársaság	8
Dánia	18
Németország	1
Észtország	29
Írország	24
Görögország	23
Spanyolország	9
Franciaország	2
Horvátország	25
Olaszország	3
Ciprus	CY
Lettország	32
Litvánia	36
Luxemburg	13
Magyarország	7
Málta	MT
Hollandia	4
Ausztria	12
Lengyelország	20
Portugália	21
Románia	19
Szlovénia	26
Szlovákia	27
Finnország	17
Svédország	5
Egyesült Királyság	11

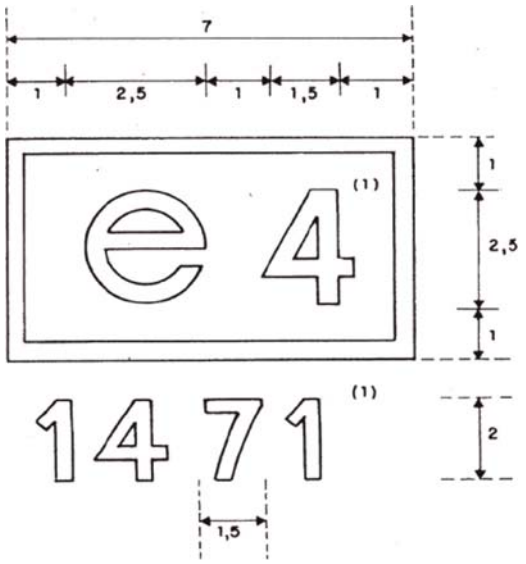
valamint

b) egy jóváhagyási szám, amely az adatrögzítő készülék vagy az adatrögzítő lap prototípusára kiadott típusbizonyítvány számának vagy a tachográf-kártya számának felel meg, és a téglalap közvetlen közelében tetszőleges helyen helyezkedik el.

▼C1

2. A jóváhagyási jelet fel kell tüntetni minden egyes készülék ismertető címkéjén, minden egyes adatrögzítő lapon és minden egyes tachográfkártyán. A jóváhagyási jelnek eltávolíthatatlannak és mindig jól olvashatónak kell lennie.

3. A jóváhagyási jel alábbi méretei ([1]) milliméterekben vannak megadva és a legkisebb méreteket jelentik. A méretek közötti arányokat meg kell tartani.



([1]) Ezek a számok csak tájékoztatásul szolgálnak.

▼C1

II. AZ ANALÓG MENETÍRÓ KÉSZÜLÉKEK TÍPUSBIZONYÍTVÁNYA

A jóváhagyást megadó tagállam a kérelmező számára típusbizonyítványt állít ki az alábbi minta alapján. A tagállam e típusbizonyítvány másolatának felhasználásával értesíti a többi tagállamot a kiadott jóváhagyásokról vagy adott esetben a jóváhagyások visszavonásáról.

TÍPUSBIZONYÍTVÁNY

Az illetékes hatóság neve .....

Értesítés ([1]):

— menetíró készülék típusának jóváhagyásáról

— menetíró készülék típusára vonatkozó jóváhagyás visszavonásáról

— adatrögzítő lap mintájának jóváhagyásáról

— adatrögzítő lap mintájára vonatkozó jóváhagyás visszavonásáról

Jóváhagyási szám:

.....

1. Védjegy vagy márkanév: .....

2. A típus vagy modell neve .....

3. A gyártó neve .....

4. A gyártó címe .....

5. Jóváhagyásra benyújtva (dátum) .....

6. Vizsgálat helye .....

7. A vizsgálat(ok) időpontja és száma .....

8. Jóváhagyás dátuma .....

9. Jóváhagyás visszavonásának dátuma .....

10. A menetíró készülékek típusa vagy típusai, amely(ek)ben az adatrögzítő lap használatát tervezik

11. Hely .....

12. Dátum .....

13. Csatolt leíró dokumentumok .....

14. Megjegyzések (ideértve adott esetben a plombák helyzetét)

(aláírás)

([1]) A nem megfelelő rész törlendő.

▼C1

III. A DIGITÁLIS MENETÍRÓ KÉSZÜLÉKEK TÍPUSBIZONYÍTVÁNYA

A jóváhagyást megadó tagállam a kérelmező számára típusbizonyítványt állít ki az alábbi minta alapján. A tagállam e típusbizonyítvány másolatának felhasználásával értesíti a többi tagállamot a kiadott jóváhagyásokról vagy adott esetben a jóváhagyások visszavonásáról.

A DIGITÁLIS MENETÍRÓ KÉSZÜLÉKEK TÍPUSBIZONYÍTVÁNYA

Az illetékes hatóság neve .....

Értesítés ([1]):

☐ a következő jóváhagyásáról: ☐ a következő jóváhagyásának visszavonásáról:

☐ adatrögzítő készülék modellje

☐ menetíró készülék alkatrésze ([2])

☐ járművezetői kártya

☐ műhelykártya

☐ vállalkozáskártya

☐ ellenőrzőkártya

Jóváhagyási szám:

.....

1. Márkanév vagy védjegy .....
2. A modell neve .....
3. A gyártó neve .....
4. A gyártó címe .....
5. Jóváhagyásra benyújtva .....
6. Laboratórium(ok) .....
7. Vizsgálati jelentés kelte és száma .....
8. Jóváhagyás dátuma .....
9. Jóváhagyás visszavonásának dátuma .....
10. A menetíró készülék(ek) azon modelljei, amelyekkel való használatra az alkatrészt tervezték
11. Hely .....
12. Dátum .....
13. Csatolt leíró dokumentumok .....
14. Megjegyzések (ideértve adott esetben a plombák helyzetét)

(aláírás)

([1]) Jelölje be a megfelelő négyzetet.
([2]) Adja meg, hogy az értesítés melyik alkatrészre vonatkozik.

▼C1

IV. AZ INTELLIGENS MENETÍRÓ KÉSZÜLÉKEK TÍPUSBIZONYÍTVÁNYA

A jóváhagyást megadó tagállam a kérelmező számára típusbizonyítványt állít ki az alábbi minta alapján. A tagállam e típusbizonyítvány másolatának felhasználásával értesíti a többi tagállamot a kiadott jóváhagyásokról vagy adott esetben a jóváhagyások visszavonásáról.

AZ INTELLIGENS MENETÍRÓ KÉSZÜLÉKEK TÍPUSBIZONYÍTVÁNYA

Az illetékes hatóság neve .....

Értesítés ([1]):

☐ a következő jóváhagyásáról: ☐ a következő jóváhagyásának visszavonásáról:

☐ adatrögzítő készülék modellje

☐ menetíró készülék alkatrésze ([2])

☐ járművezetői kártya

☐ műhelykártya

☐ vállalkozáskártya

☐ ellenőrzőkártya

Jóváhagyási szám:

.....

1. Márkanév vagy védjegy .....
2. A modell neve .....
3. A gyártó neve .....
4. A gyártó címe .....
5. Jóváhagyásra benyújtva .....
6. a) A működési tanúsítást végző vizsgálólaboratórium .....
   b) A biztonsági tanúsítást végző vizsgálólaboratórium .....
   c) Az interoperabilitási tanúsítást végző vizsgálólaboratórium .....
7. a) A működési tanúsítvány dátuma és száma .....
   b) A biztonsági tanúsítvány dátuma és száma .....
   c) Az interoperabilitási tanúsítvány dátuma és száma .....
8. Jóváhagyás dátuma .....
9. Jóváhagyás visszavonásának dátuma .....
10. A menetíró készülék(ek) azon modelljei, amelyekkel való használatra az alkatrészt tervezték
11. Hely .....
12. Dátum .....
13. Csatolt leíró dokumentumok .....
14. Megjegyzések (ideértve adott esetben a plombák helyzetét)

(aláírás)

([1]) Jelölje be a megfelelő négyzetet.
([2]) Adja meg, hogy az értesítés melyik alkatrészre vonatkozik.