2025/2462

2025.12.9.

A BIZOTTSÁG (EU) 2025/2462 VÉGREHAJTÁSI RENDELETE

(2025. december 8.)

az (EU) 2024/482 végrehajtási rendeletnek a fogalommeghatározások, az IKT-terméksorozatok tanúsítása, a megbízhatóság folytonossága és a technika állásának megfelelő dokumentumok tekintetében történő módosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletre (kiberbiztonsági jogszabály) ([1]) és különösen annak 49. cikke (7) bekezdésére,

mivel:

(1) Az (EU) 2024/482 bizottsági végrehajtási rendelet ([2]) az (EU) 2019/881 rendelettel létrehozott európai kiberbiztonsági tanúsítási keretrendszerrel összhangban meghatározza a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) szerepét, szabályait és kötelezettségeit, valamint felépítését.

(2) A közös kritériumokhoz kapcsolódó közös értékelési módszertan – az informatikai biztonságértékelés nemzetközi szabványa – lehetővé teszi az IKT-termékek biztonságának tanúsítási célú értékelését. Ebben az összefüggésben egyes IKT-termékek azonos funkcionális alapokra épülhetnek annak érdekében, hogy hasonló biztonsági funkciókat kínáljanak különböző platformokon vagy készülékeken; az ilyen IKT-termékek alkotják az úgynevezett terméksorozatokat. A tervezés, a hardver, a belső vezérlőprogram vagy a szoftver azonban IKT-termékenként eltérő lehet. A tanúsító szerv feladata eseti alapon eldönteni, hogy elvégezhető-e egy adott terméksorozat tanúsítása. A terméksorozatok tanúsítására vonatkozó feltételeket részletesebben be lehetne mutatni az EUCC-t támogató iránymutatásokban.

(3) A tanúsított termékek megbízhatóságának fenntartása érdekében alapvető fontosságú annak meghatározása, hogy mi minősül jelentős, illetve kisebb jelentőségű változtatásnak az értékelés tárgya vagy környezete tekintetében, az üzemeltetési és a fejlesztési környezetet egyaránt beleértve. Ezért szükség van az említett fogalmak meghatározására, figyelembe véve a vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportjának (SOG-IS), valamint az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás (CCRA) résztvevőinek már meglévő és széles körben használt műszaki előírásait.

(4) A kisebb jelentőségű változtatásokat gyakran a kibocsátott EUCC-tanúsítványban szereplő, a termékek megbízhatóságára vonatkozó nyilatkozatra gyakorolt korlátozott hatásuk jellemzi. Ezért a kisebb jelentőségű változtatások esetében nincs szükség a termék biztonsági funkcióinak újraértékelésére, ehelyett az ilyen változtatásokat célszerű karbantartási eljárások keretében kezelni. A karbantartás révén kezelendő, kisebb jelentőségű változtatások közé tartoznak többek között a szerkesztési változtatások, az értékelés tárgyának környezetét érintő olyan változtatások, amelyek nem módosítják az értékelés tanúsításon átesett tárgyát, valamint az értékelés tanúsításon átesett tárgya tekintetében végrehajtott olyan változtatások, amelyek nem befolyásolják a megbízhatóság bizonyítékait. A fejlesztési környezet vonatkozásában végrehajtott változtatások is minősülhetnek kisebb jelentőségű változtatásnak, feltéve, hogy nem váltanak ki a megbízhatósággal kapcsolatos meglévő intézkedéseket érintő hatásokat. Egyes esetekben azonban szükségessé tehetik a vonatkozó intézkedések részleges értékelését.

([1]) HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Jelentős változtatásnak minősül az értékelés tanúsításon átesett tárgyát vagy az értékelés tárgyának környezetét érintő bármely olyan változtatás, amely hátrányosan befolyásolhatja az EUCC-tanúsítványban kifejezett megbízhatóságot, és amely ebből kifolyólag szükségessé teszi az újraértékelést. A jelentős változtatások közé tartoznak például az állítólagosan teljesített megbízhatósági követelmények együttesében végrehajtott változások a CC ALC_FLR család (A hiányosságok orvoslása) bizonyossági követelményeihez kapcsolódó változtatások kivételével; a fejlesztési környezetnek a bizalmas kezelés vagy az integritás szempontjából történő ellenőrzését érintő változtatások, amennyiben az ilyen módosítások befolyásolhatják az értékelés tárgyának biztonságos fejlesztését vagy előállítását, vagy az értékelés tárgyát illetően a kihasználható sebezhetőség felszámolása érdekében végrehajtott változtatások. Emellett jelentős változtatásnak minősülhet a kisebb jelentőségű változtatások olyan együttese is, amely jelentős hatást gyakorol a biztonságra. Azt is fontos elismerni, hogy még ha a hibajavítás csak az értékelés tárgyának egy konkrét aspektusát érinti is, kiszámíthatatlansága és a megbízhatóságra gyakorolt lehetséges hatása miatt jelentős változtatásnak minősülhet, ha veszélyezteti a tanúsítás által nyújtott biztonsági garanciákat.

(6) A változatlan tanúsított IKT-termék fenyegetettségi környezetét érintő változtatások szükségessé tehetik az újbóli értékelést. Indokolt egyértelműen meghatározni az ilyen újbóli értékelésre irányuló folyamat lehetséges eredményeit, különösen az EUCC-tanúsítványra gyakorolt hatását. Indokolt előírni a tanúsító szerv számára, hogy az újbóli értékelés sikeres elvégzése esetén erősítse meg a tanúsítványt, vagy állítson ki egy új, meghosszabbított érvényességi idejű tanúsítványt. Ha az újbóli értékelésre irányuló folyamat sikertelen, a tanúsító szervnek vissza kell vonnia a tanúsítványt, és – amennyiben lehetséges – ki kell állítania egy eltérő hatályú új tanúsítványt. Ezeket a rendelkezéseket értelemszerűen alkalmazni kell a védelmi profilok újbóli értékelésére is.

(7) Az (EU) 2024/482 végrehajtási rendelet I. melléklete felsorolja az IKT-termékek és védelmi profilok értékeléséhez alkalmazandó, a technika állásának megfelelő dokumentumokat. Ezeket a technika állásának megfelelő dokumentumokat aktualizálni kell annak érdekében, hogy tükrözzék a legújabb fejleményeket, például a technológiai fejlődéssel, a kiberfenyegetettségi helyzettel, az ipari gyakorlatokkal vagy a nemzetközi szabványokkal kapcsolatos újdonságokat. Időszerű ilyen aktualizálást elvégezni a helyszíni biztonsági minimumkövetelményekkel, a támadási potenciálok intelligens kártyákra történő alkalmazásával, a támadási potenciálok biztonsági dobozokkal ellátott hardvereszközökre való alkalmazásával, a közös kritériumok integrált áramkörökre történő alkalmazásával, valamint az összetett termékek intelligens kártyák és hasonló eszközök vonatkozásában történő értékelésével kapcsolatos, a technika állásának megfelelő dokumentumok esetében. Ezenkívül jelenleg nem szerepelnek a felsorolásban az összetett termékeknek a közös kritériumokra vonatkozó szabványok legújabb változata alapján történő értékelésével és tanúsításával, a helyszíni ellenőrzések értékelési eredményeinek újrafelhasználásával, valamint a minősített elektronikus aláírást létrehozó eszközökhöz, menetíró készülékekhez és biztonsági hardvermodulokhoz kapcsolódó védelmi profilok értelmezésére vonatkozó pontosításokkal kapcsolatos, a technika állásának megfelelő dokumentumok. Az IKT-termékek EUCC keretében történő egységes értékelésének biztosítása érdekében az I. mellékletet módosítani kell oly módon, hogy abba az európai kiberbiztonsági tanúsítási csoport (ECCG) általi jóváhagyásukat követően bekerüljenek az említett aktualizált vagy új, a technika állásának megfelelő dokumentumok.

(8) Emellett a rendszert ki kell egészíteni az „ADV_SPM.1 interpretation for CC:2022 transition” (ADV_SPM.1 értelmezés a közös kritériumok CC:2022. verziójára való átálláshoz) című, a technika állásának megfelelő dokumentummal annak biztosítására, hogy a konkrét védelmi profilokon alapuló tanúsítási folyamatok a megfelelő védelmi profilok frissítéséig továbbra is formális modellezést (ADV_SPM.1) alkalmazzanak, például egy, a CC:2022. verziónak megfelelő, az ADV_SPM.1-et támogató, többszintű megbízhatósági követelményekkel rendelkező védelmi profil konfigurációjának hozzáadásával. Annak érdekében, hogy a piac számára elegendő idő álljon rendelkezésre a közös kritériumok aktualizált szabványaira való átálláshoz, egyedi átmeneti szabályok bevezetését kell előirányozni a következő védelmi profilok tekintetében: Security IC Platform PP with Augmentation Packages (Biztonsági IC platform védelmi profil kiegészítő csomagokkal) (1.0. verzió), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (Java Card rendszer – Zárt konfiguráció) (3.1. verzió), BSI-CC-PP-0101-V2–2020, illetve Java Card System – Open Configuration (Java Card rendszer – Nyitott konfiguráció) (3.1. verzió), BSI-CC-PP-0099-V2-2020. A piaci zavarok elkerülése érdekében helyénvaló megállapítani, hogy az „ADV_SPM.1 interpretation for CC:2022 transition” (ADV_SPM.1 értelmezés a közös kritériumok CC:2022. verziójára való átálláshoz) című, a technika állásának megfelelő dokumentum alkalmazandó az e rendelet elfogadása előtt kezdeményezett tanúsítási folyamatokra. E dokumentum alkalmazását azonban szigorúan a szükséges mértékűre kell korlátozni, figyelembe véve a megfelelő védelmi profilok frissítésének véglegesítéséhez szükséges időt. Konkrétabban: a Security IC Platform PP with Augmentation Packages (Biztonsági IC platform védelmi profil kiegészítő csomagokkal) (1.0. verzió), BSI-CC-PP-0084-2014, illetve a Java Card System – Closed Configuration (Java Card rendszer – Zárt konfiguráció) (3.1. verzió), BSI-CC-PP-0101-V2–2020 védelmi profilt alkalmazó tanúsítási folyamatok esetében indokolt úgy rendelkezni, hogy a technika állásának megfelelő dokumentum a 2026. október 1. előtt kezdeményezett folyamatokra legyen alkalmazandó. A Java Card System – Open Configuration (Java Card rendszer – Nyitott konfiguráció) (3.1. verzió), BSI-CC-PP-0099-V2-2020 védelmi profilt alkalmazó tanúsítási folyamatok esetében a technika állásának megfelelő dokumentum használatát indokolt az e rendelet hatálybalépése előtt kezdeményezett folyamatokra korlátozni, tekintettel arra, hogy már rendelkezésre áll a Java Card System – Open Configuration (Java Card rendszer – Nyitott konfiguráció) védelmi profil új verziója.

(9) A technika állásának megfelelő dokumentumban a tanúsítási folyamat során végrehajtott változtatás megzavarhatja a termék értékelését és késleltetheti a tanúsítvány kiállítását. Ezért megfelelő átmeneti szabályokat kell megállapítani a technika állásának megfelelő, új vagy aktualizált dokumentumok tekintetében azért, hogy az értékesítők, az információtechnológiai biztonságértékelő intézetek (ITSEF-ek), a tanúsító szervek és más érdekelt felek elvégezhessék a szükséges kiigazításokat. Indokolt úgy rendelkezni, hogy az alkalmazandó aktualizált és új, a technika állásának megfelelő dokumentumok vonatkozzanak a tanúsítás iránti kérelmekre, beleértve az újbóli értékelésre és újraértékelésre irányuló kérelmeket is, ugyanakkor lehetővé kell tenni, hogy a már megindított tanúsítási folyamatok lebonyolítására továbbra is a technika állásának megfelelő dokumentumok korábbi változatainak használatával kerüljön sor.

(10) Az (EU) 2024/482 végrehajtási rendelet II. és III. melléklete felsorolja az AVA_VAN 4. vagy 5. szinten tanúsított védelmi profilokat és az ajánlott védelmi profilokat. A védelmi profilok aktualizálásának következtében számos hivatkozás hiányos vagy elavult. A szóban forgó hivatkozásokat ki kell egészíteni, és emellett új hivatkozásokat kell beilleszteni a biztonságos integrált áramkörök, az intelligens kártyák és a kapcsolódó eszközök, valamint a megbízható számítástechnika szélesebb körű lefedettségének biztosítására.

(11) Módosítani kell az (EU) 2024/482 végrehajtási rendelet 19. cikkét annak egyértelművé tétele érdekében, hogy a IV. melléklet – a szükséges változtatásokkal – alkalmazandó a védelmi profilokra kiadott EUCC-tanúsítványok felülvizsgálatára.

(12) Tekintettel arra, hogy a biztonsági előirányzat kulcsfontosságú tényező a tanúsítási folyamat hatályának megértése szempontjából, indokolt előírni azt is, hogy az ENISA tegye közzé weboldalán az egyes EUCC-tanúsítványoknak megfelelő biztonsági előirányzatot.

(13) A tanúsító szerveknek továbbá az ENISA rendelkezésére kell bocsátaniuk a biztonsági előirányzat és a tanúsítási jelentés angol nyelvű változatát annak érdekében, hogy az ügynökség az (EU) 2024/482 végrehajtási rendelet 42. cikkének (2) bekezdésével összhangban angol nyelven közzétehesse ezeket az információkat a megfelelő weboldalon. Ezért a tanúsítást kérelmezőknek kérésre a tanúsító szervek rendelkezésére kell bocsátaniuk a biztonsági előirányzat angol nyelvű változatát.

(14) A tanúsítvány egyedi azonosítójában nem szükséges feltüntetni a tanúsító szerv nevét, mivel a tanúsító szerv azonosító száma elegendő e szervezet egyedi azonosításához. A kiállítás hónapját sem kell feltüntetni, mivel a tanúsítványok számbavétele éves alapon történik. Ezért ezt a követelményt az egyszerűsítés érdekében törölni kell. Mivel a tanúsítvány kiállításának éve annak az évnek felel meg, amelyben az első tanúsítvány kiállítására sor került, a nyomonkövethetőség biztosítására ugyanezt az időpontot kell feltüntetni a felülvizsgálatot követően kiállított tanúsítványok egyedi azonosítójában.

(15) Az (EU) 2024/482 végrehajtási rendeletet ezért ennek megfelelően módosítani kell.

(16) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2019/881 rendelet 66. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Az (EU) 2024/482 végrehajtási rendelet a következőképpen módosul:

1. A 2. cikk a következő 16., 17. és 18. ponttal egészül ki:

„16. »terméksorozat«: egy adott kérelmező olyan IKT-termékeinek együttese, amelyek azonos funkcionális alapra épülnek ugyanazon biztonsági igények kielégítése érdekében, ám amelyek tervezése, hardvere, belső vezérlőprogramja vagy szoftvere IKT-termékenként eltérő lehet;

17. »kisebb jelentőségű változtatás«: az értékelés tanúsításon átesett tárgyát vagy annak környezetét érintő bármely olyan változtatás, amely nem befolyásolja hátrányosan az EUCC-tanúsítványban kifejezett megbízhatóságot;

18. »jelentős változtatás«: az értékelés tanúsításon átesett tárgyát vagy annak környezetét érintő bármely olyan változtatás, amely hátrányosan befolyásolhatja az EUCC-tanúsítványban kifejezett megbízhatóságot.”

2. Az 5. cikk a következő (3) bekezdéssel egészül ki:

„(3) Egy tanúsító szerv terméksorozat tanúsítását is engedélyezheti.”

3. A 9. cikk (2) bekezdésének a) pontja helyébe a következő szöveg lép:

„a) a tanúsító szerv és az ITSEF rendelkezésére bocsátja az összes szükséges, teljes körű és helyes információt, és kérésre további szükséges információkat szolgáltat, beleértve a biztonsági előirányzat angol nyelvű változatát;”.

4. A 11. cikk (3) bekezdésének b) pontja helyébe a következő szöveg lép:

„b) a tanúsítvány egyedi azonosítója, amely a következőkből áll:

1. a rendszer neve;

2. a tanúsítványt kiállító tanúsító szervnek az (EU) 2024/3143 végrehajtási rendelet 3. cikke szerinti azonosító száma;

3. az első tanúsítvány kiállításának éve;

4. a tanúsítványt kiállító tanúsító szerv által kiadott azonosító szám.”

5. A 19. cikk (1) bekezdésének helyébe a következő szöveg lép:

„(1) A tanúsítvány jogosultjának kérésére vagy más indokolt esetben a tanúsító szerv dönthet úgy, hogy felülvizsgálja egy adott védelmi profil EUCC-tanúsítványát. A felülvizsgálatot a IV. melléklettel összhangban kell elvégezni. A tanúsító szerv meghatározza a felülvizsgálat terjedelmét. Amennyiben a felülvizsgálathoz szükséges, a tanúsító szerv felkéri az ITSEF-et, hogy értékelje újra a tanúsított védelmi profilt.”

6. A 42. cikk a következőképpen módosul:

a) az (1) bekezdés a következő i) ponttal egészül ki:

„i) az egyes EUCC-tanúsítványoknak megfelelő biztonsági előirányzat;”

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) Az (1) bekezdésben említett információkat legalább angol nyelven rendelkezésre kell bocsátani. E célból a tanúsító szervek eljuttatják az ENISA-hoz a tanúsítási jelentések és a biztonsági előirányzatok eredeti nyelvi változatait, továbbá indokolatlan késedelem nélkül rendelkezésére bocsátják az említett dokumentumok angol nyelvű változatát is.”

7. A 48. cikk (4) bekezdésének helyébe a következő szöveg lép:

„(4) Amennyiben az I. vagy a II. melléklet másként nem rendelkezik, a technika állásának megfelelő dokumentumokat azokra – az újbóli értékelést és az újraértékelést is magukban foglaló – tanúsítási folyamatokra kell alkalmazni, amelyek kezdeményezésére azon módosító jogi aktus alkalmazásának kezdőnapján vagy azt követően került sor, amely a technika állásának megfelelő dokumentumokat beillesztette az I. vagy a II. mellékletbe.”

8. Az I. melléklet helyébe e rendelet I. mellékletének szövege lép.

9. A II. melléklet helyébe e rendelet II. mellékletének szövege lép.

10. A III. melléklet helyébe e rendelet III. mellékletének szövege lép.

11. A IV. melléklet e rendelet IV. mellékletének megfelelően módosul.

12. Az V. melléklet e rendelet V. mellékletének megfelelően módosul.

13. A IX. melléklet helyébe e rendelet VI. mellékletének szövege lép.

2. cikk

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

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

Kelt Brüsszelben, 2025. december 8-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

„I. MELLÉKLET

A műszaki területeket támogató, a technika állásának megfelelő dokumentumok és a technika állásának megfelelő egyéb dokumentumok

1. Az AVA_VAN 4. vagy 5. szintű műszaki területeket támogató, a technika állásának megfelelő dokumentumok:
   a) az »intelligens kártyák és hasonló eszközök« műszaki terület harmonizált értékelésével kapcsolatos következő dokumentumok:
      1. »Minimum ITSEF requirements for security evaluations of smart cards and similar devices« (Az intelligens kártyák és hasonló eszközök biztonsági értékelésére vonatkozó ITSEF minimumkövetelmények), 1.1. verzió;
      2. »Minimum Site Security Requirements« (Helyszíni biztonsági minimumkövetelmények), 2. verzió;
      3. »Reusing evaluation results of site audits (STAR)« (Helyszíni ellenőrzések értékelési eredményeinek újbóli felhasználása [STAR]), 1. verzió;
      4. »Application of Common Criteria to integrated circuits« (A közös kritériumok alkalmazása integrált áramkörökre), 2. verzió;
      5. »Security Architecture requirements (ADV_ARC) for smart cards and similar devices« (Az intelligens kártyákra és hasonló eszközökre vonatkozó biztonsági architektúra-követelmények [ADV_ARC]), 1.1. verzió;
      6. »Certification of 'open' smart card products« (»Nyílt« intelligenskártya-termékek tanúsítása), 1.1. verzió;
      7. »Composite product evaluation for smart cards and similar devices for CC3.1« (Összetett termékek intelligens kártyák és hasonló eszközök vonatkozásában történő értékelése a CC3.1. verzió használata esetén), 2. verzió;
      8. »Composite product evaluation and certification for CC:2022« (Összetett termékek értékelése és tanúsítása a CC:2022. verzió használata esetén), 1. verzió;
      9. »Application of Attack Potential to Smartcards and Similar Devices« (A támadási potenciál alkalmazása az intelligens kártyákra és hasonló eszközökre), 2. verzió;
      10. »Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices« (Minősített elektronikus aláírást/bélyegzőt létrehozó eszközök biztonsági értékelése és tanúsítása), 1. verzió;
      11. »ADV_SPM.1 interpretation for CC:2022 transition« (ADV_SPM.1 értelmezés a közös kritériumok CC:2022. verziójára való átálláshoz), 1.1. verzió, amely a következő védelmi profilokat használó tanúsítási folyamatok tekintetében alkalmazandó:
         a) Security IC Platform PP with Augmentation Packages (Biztonsági IC platform védelmi profil kiegészítő csomagokkal) (1.0. verzió), BSI-CC-PP-0084-2014, illetve Java Card System – Closed Configuration (Java Card rendszer – Zárt konfiguráció) (3.1. verzió), BSI-CC-PP-0101-V2-2020 védelmi profilok a 2026. október 1-je előtt kezdeményezett folyamatok esetében;
         b) Java Card System – Open Configuration (Java Card rendszer – Nyitott konfiguráció) (3.1. verzió), BSI-CC-PP-0099-V2-2020 védelmi profil a 2025. december 29. előtt kezdeményezett folyamatok esetében;
   b) a »biztonsági dobozzal ellátott hardvereszközök« műszaki terület harmonizált értékelésével kapcsolatos következő dokumentumok:
      1. »Minimum ITSEF requirements for security evaluations of hardware devices with security boxes« (A biztonsági dobozzal ellátott hardvereszközök biztonsági értékelésére vonatkozó ITSEF minimumkövetelmények), 1.1. verzió;
      2. »Minimum Site Security Requirements« (Helyszíni biztonsági minimumkövetelmények), 2. verzió;
      3. »Reusing evaluation results of site audits (STAR)« (Helyszíni ellenőrzések értékelési eredményeinek újbóli felhasználása [STAR]), 1. verzió;
      4. »Application of Attack Potential to hardware devices with security boxes« (A támadási potenciál alkalmazása a biztonsági dobozzal ellátott hardvereszközökre), 2. verzió;
      5. »Hardver assessment in EN 419221–5 (HSM PP)« (Hardverértékelés az EN 419221–5 szabvány keretében [HSM PP]), 1. verzió;
      6. »JIL Tachograph MS PP Clarification« (Joint Interpretation Library [JIL] – A menetíró készülékek mozgásérzékelő szerkezetére vonatkozó védelmi profil [MS PP] egyértelműsítése), 1. verzió.
2. A megfelelőségértékelő szervezetek harmonizált akkreditációjával kapcsolatos, a technika állásának megfelelő dokumentumok:
   a) »Accreditation of ITSEFs for the EUCC« (Az ITSEF akkreditálása az EUCC alkalmazása céljából), 1.1. verzió a 2025. július 8. előtt kiadott akkreditációk esetében;
   b) »Accreditation of ITSEFs for the EUCC« (Az ITSEF akkreditálása az EUCC alkalmazása céljából), 1.6c. verzió az újonnan kiadott vagy 2025. július 8. után felülvizsgált akkreditációk esetében;
   c) »Accreditation of CBs for the EUCC« (A tanúsító szervek akkreditálása az EUCC alkalmazása céljából), 1.6b. verzió."

II. MELLÉKLET

„II. MELLÉKLET

AVA_VAN 4. vagy 5. szinten tanúsított védelmi profilok

1. A távoli minősített aláírást és bélyegzőt létrehozó eszközök esetében:

   a) EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing (A kiszolgáló aláírását támogató megbízható rendszerek. 2. rész: QSCD védelmi profil a kiszolgáló aláírásához) (0.16. verzió), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services (Védelmi profilok a TSP kriptográfiai modulokhoz. 5. rész: Kriptográfiai modul a bizalmi szolgáltatásokhoz) (0.15. verzió), ANSSI-CC-PP-2016/05-M01.

2. A technika állásának megfelelő dokumentumokként elfogadott védelmi profilok:

   [ÜRES].”

III. MELLÉKLET

„III. MELLÉKLET

Ajánlott védelmi profilok

Az IKT-termékek tanúsítása során használt védelmi profilok, beleértve a műszaki területekhez tartozó termékeket is:

1. Intelligens kártyák és hasonló eszközök
   a) útlevél:
      1. PP Machine Readable Travel Document with "ICAO Application" Basic Access Control (Az »ICAO-alkalmazás« alapszintű hozzáférés-ellenőrzési mechanizmusával védett, géppel olvasható úti okmányra vonatkozó védelmi profil), (1.10. verzió), BSI-CC-PP-0055-2009;
      2. PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (A jelszóval hitelesített összeköttetés-létesítéssel (PACE) működő standard vizsgálati eljárást alkalmazó, géppel olvasható úti okmányra vonatkozó védelmi profil) (PACE_PP) (1. verzió), BSI-CC-PP-0068-V2-2011-MA-01;
      3. PP Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE (Az »ICAO-alkalmazás« kiterjesztett hozzáférés-ellenőrzési mechanizmusa és PACE által védett, géppel olvasható úti okmányra vonatkozó védelmi profil) (1.3. verzió), BSI-CC-PP-0056-V2-2012-MA-02;
   b) biztonságos aláírás-létrehozó eszközök (SSCD):
      1. EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation (Biztonságos aláírás-létrehozó eszköz védelmi profilja. 2. rész: Kulcsgeneráló eszközök) (1.03. verzió), BSI-CC-PP-0059-2009-MA-02;
      2. EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import (Biztonságos aláírás-létrehozó eszköz védelmi profilja. 3. rész: Kulcsimportáló eszközök) (1.0.2. verzió), BSI-CC-PP-0075-2012-MA-01;
      3. EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application (Biztonságos aláírás-létrehozó eszköz védelmi profilja. 4. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna tanúsítványgeneráló alkalmazáshoz) (1.0.1. verzió), BSI-CC-PP-0071-2012-MA-01;
      4. EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application (Biztonságos aláírás-létrehozó eszköz védelmi profilja. 5. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna aláírás-létrehozó alkalmazáshoz) (1.0.1. verzió), BSI-CC-PP-0072-2012-MA-01;
      5. EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application (Biztonságos aláírás-létrehozó eszköz védelmi profilja. 6. rész: Tartozék kulcsimportáló eszközökhöz és megbízható csatorna aláírás-létrehozó alkalmazáshoz) (1.0.4. verzió), BSI-CC-PP-0076-2013-MA-01;
   c) menetíró készülék: Digital Tachograph – Tachograph Card (Digitális menetíró készülék – Tachográfkártya) (TC PP) (1.0. verzió), BSI-CC-PP-0091-2017;
   d) biztonságos integrált áramkörök, Java Card platform és eUICC:
      1. Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (Univerzális védelmi profil SIM- és Java-kártyák platformjaihoz – alapszintű és SCWS-konfigurációk) (2.0.2. verzió), ANSSI-CC-PP-2010/04 (alapszintű), ANSSI-CC-PP-2010/05 (alapszintű és SCWS);
      2. Security IC Platform PP with Augmentation Packages (Biztonsági IC platform védelmi profil kiegészítő csomagokkal) (1.0. verzió), BSI-CC-PP-0084-2014;
      3. Embedded UICC (eUICC) for Machine-to-Machine Devices (Beágyazott UICC [EUICC] gépek közötti eszközökhöz) (1.1. verzió), BSI-CC-PP-0089-2015;
      4. Cryptographic Service Provider – CSP (Kriptográfiai szolgáltató – CSP) (0.9.8. verzió), BSI-CC-PP-0104-2019;
      5. Cryptographic Service Provider – Time Stamp Service and Audit (Kriptográfiai szolgáltató – Időbélyegző-szolgáltatás és ellenőrzés) (PPC-CSP-TS-Au), 0.9.5. verzió, BSI-CC-PP-0107-2019;
      6. Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (Kriptográfiai szolgáltatói konfiguráció – Időbélyegző-szolgáltatás, ellenőrzés és klaszterezés) (PPC-CSP-TS-Au-Cl) 0.9.4. verzió, BSI-CC-PP-0108-2019;
      7. Java Card System – Closed Configuration (Java Card rendszer – Zárt konfiguráció) (3.1. verzió), BSI-CC-PP-0101-V2-2020;
      8. Secure Element Protection Profile (Biztonsági elemekre vonatkozó védelmi profil) – GPC_SPE_174 (1.0. verzió), CCN-CC-PP-5-2021;
      9. Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (Az egylapkás rendszeren belüli biztonságos alrendszerre [3S in SoC] vonatkozó védelmi profil) (1.8. verzió), BSI-CC-PP-0117-V2-2023;
      10. Java Card System – Open Configuration (Java Card rendszer – Nyitott konfiguráció) (3.2. verzió), BSI-CC-PP-0099-V3-2024;
      11. Embedded UICC for Consumer Devices Protection Profile (A fogyasztói eszközökbe beágyazott univerzális integrált áramköri kártyákra [UICC] vonatkozó védelmi profil) (2.1. verzió), BSI-CC-PP-0100-V2-2025;
   e) megbízható platform modul: Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0 (Védelmi profil a PC kliensspecifikus megbízható platform moduljának 2.0 családja esetében); 0. szint; 1.59. felülvizsgálat (1.3. verzió), ANSSI-CC-PP-2021/02.

2. Biztonsági dobozzal ellátott hardvereszközök

   a) (fizetési) interakciós pontok és fizetési terminálok (POI);

      1. »POI-CHIP-ONLY« interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/01;

      2. »POI-CHIP-ONLY and Open Protocol Package« (POI-CHIP-ONLY és nyitott protokollcsomag) interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/02;

      3. »POI-COMPREHENSIVE« interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/03;

      4. »POI-COMPREHENSIVE and Open Protocol Package« (POI-COMPREHENSIVE és nyitott protokollcsomag) interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/04;

      5. »POI-PED-ONLY« interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/05;

      6. »POI-PED-ONLY and Open Protocol Package« (POI-PED-ONLY és nyitott protokollcsomag) interakciós pont (4.0. verzió), ANSSI-CC-PP-2015/06;

   b) biztonsági hardvermodul:

      1. Cryptographic Module for CSP Signing Operations with Backup (Kriptográfiai modul backup funkcióval kriptográfiai szolgáltató aláírási műveleteihez) – PP CMCSOB 14167-2 (0.35. verzió), ANSSI-CC-PP-2015/08;

      2. Cryptographic Module for CSP Key Generation Services (Kriptográfiai modul kriptográfiai szolgáltató kulcsgenerálási szolgáltatásaihoz) – PP CMCKG 14167-3 (0.20. verzió), ANSSI-CC-PP-2015/09;

      3. Cryptographic Module for CSP Signing Operations without Backup (Kriptográfiai modul backup funkció nélkül kriptográfiai szolgáltató aláírási műveleteihez) – PP CMCSO 14167-4 (0.32. verzió), ANSSI-CC-PP-2015/10;

   c) menetíró készülék:

      1. Digital Tachograph – Motion Sensor (Digitális menetíró készülék – Mozgásérzékelő) (MS PP) (1.0. verzió), BSI-CC-PP-0093-2017;

      2. Digital Tachograph – Vehicle Unit (Digitális menetíró készülék – Járműegység) (VU PP) (1.15. verzió), BSI-CC-PP-0094-V2-2021;

      3. Digital Tachograph – External GNSS Facility (Digitális menetíró készülék – Külső GNSS-eszköz) (EGF PP) (1.10. verzió), BSI-CC-PP-0092-V2-2021.

3. Egyebek: Trusted Execution Environment Protection Profile (A megbízható végrehajtási környezetre vonatkozó védelmi profil) – GPD_SPE_021 (1.3. verzió), ANSSI-CC-PP-2014/01-M02.”

IV. MELLÉKLET

Az (EU) 2024/482 végrehajtási rendelet IV. melléklete a következőképpen módosul:

1. A IV.2. szakasz 4. pontja helyébe a következő szöveg lép:

„4. A tanúsító szerv felülvizsgálja az aktualizált értékelési technikai jelentést, és jelentést készít az újbóli értékelésről. Az eredeti tanúsítvány státuszát ezt követően a 13. vagy a 19. cikknek megfelelően módosítani kell. Ha az újbóli értékelésre irányuló folyamat sikeres, terméktanúsítás esetén a 13. cikk (2) bekezdésének a) vagy c) pontja, védelmi profil tanúsítása esetén pedig a 19. cikk (2) bekezdésének a) vagy c) pontja alkalmazandó. Ha az újbóli értékelésre irányuló folyamat sikertelen, terméktanúsítás esetén a 13. cikk (2) bekezdésének b) vagy d) pontja, védelmi profil tanúsítása esetén pedig a 19. cikk (2) bekezdésének b) vagy d) pontja alkalmazandó.”

2. A IV.3. szakasz a következőképpen módosul:

a) A IV.3. szakasz címének helyébe a következő szöveg lép:

„IV.3. **Tanúsított IKT-termék tekintetében végrehajtott változtatások – Karbantartás és újraértékelés”;**

b) a 4. és az 5. pont helyébe a következő szöveg lép:

„4. A vizsgálatot követően a tanúsító szerv a változtatás mértékét az EUCC-tanúsítványban kifejezett megbízhatóságra gyakorolt hatásnak megfelelően kisebb jelentőségűként vagy jelentősként határozza meg.

5. Amennyiben a tanúsító szerv megerősítette, hogy a változtatások kisebb jelentőségűek, nem kell új tanúsítványt kiadni a módosított IKT-termékre vonatkozóan a 13. cikk (2) bekezdésének a) pontjával vagy a 19. cikk (2) bekezdésének a) pontjával összhangban, hanem karbantartási jelentést kell készíteni az eredeti tanúsítási jelentéshez.”;

c) a szakasz a következő 5a. ponttal egészül ki.

„5a. A fejlesztési környezetben a megbízhatósággal kapcsolatban végrehajtandó intézkedéseket érintő bármilyen változtatás – például a CC ALC_FLR családba (A hiányosságok orvoslása) tartozó megbízhatósági követelményekkel való kiegészítés – esetén a tanúsító szerv felkérheti az ITSEF-et, hogy végezze el a megbízhatósággal kapcsolatos érintett intézkedések egy részének az értékelését. Az ITSEF részleges értékelési technikai jelentést ad ki, amelynek alapján a tanúsító szerv megerősíti, hogy a változtatások kisebb jelentőségűek vagy jelentősek-e. Amennyiben a tanúsító szerv megerősíti, hogy a változtatások kisebb jelentőségűek, a IV. melléklet IV.3. szakaszának 5. pontját kell alkalmazni. Amennyiben a tanúsító szerv megerősíti, hogy a változtatások jelentősek, a IV. melléklet IV.3. szakaszának 7. pontját kell alkalmazni.”

V. MELLÉKLET

Az (EU) 2024/482 végrehajtási rendelet V. mellékletének V.1. szakasza helyébe a következő szöveg lép:

„V.1. **Tanúsítási jelentés**

1. A tanúsító szerv az ITSEF által benyújtott értékelési technikai jelentések alapján tanúsítási jelentést készít, amelyet a megfelelő EUCC-tanúsítvánnyal és biztonsági előirányzattal együtt közzé kell tenni.

2. A tanúsítási jelentés az IKT-termékre és az IKT-termék biztonságos telepítésére vonatkozó részletes és gyakorlati információk forrása. Ezért magában kell foglalnia minden nyilvánosan hozzáférhető és megosztható, a felhasználók és az érdekelt felek számára releváns információt. A tanúsítási jelentés hivatkozhat nyilvánosan hozzáférhető és megosztható információkra.

3. A tanúsítási jelentésnek legalább az alábbi információkat kell tartalmaznia:

   a) vezetői összefoglaló;

   b) az IKT-termék azonosítása;

   c) az IKT-termék értékelésével kapcsolatos kapcsolattartási adatok;

   d) biztonsági szabályzatok;

   e) feltételezések és a hatály egyértelműsítése;

   f) az architektúrára vonatkozó információk;

   g) adott esetben kiegészítő kiberbiztonsági információk;

   h) az IKT-termék értékelésének összefoglalása és az értékelt konfiguráció;

   i) az értékelés eredményei és a tanúsítványra vonatkozó információk;

   j) adott esetben megjegyzések és ajánlások;

   k) adott esetben mellékletek;

   l) hivatkozás a tanúsításra benyújtott IKT-termék biztonsági előirányzatára;

   m) amennyiben rendelkezésre áll, a rendszerhez kapcsolódó jelölés vagy címke;

   n) adott esetben glosszárium;

   o) bibliográfia.

4. A 3. a) pontban említett vezetői összefoglaló a teljes tanúsítási jelentés rövid összefoglalása. Világos és tömör áttekintést kell nyújtania az értékelés eredményeiről, és magában kell foglalnia a következő információkat:

   a) az értékelt IKT-termék megnevezése;

   b) az értékelést végző ITSEF neve;

   c) az értékelés lezárásának dátuma;

   d) a tanúsítvány kiállításának dátuma;

   e) adott esetben az első tanúsítvány kiállításának dátuma;

   f) az érvényesség időtartama;

   g) a tanúsítvány egyedi azonosítója a 11. cikkben leírtak szerint;

   h) a tanúsítási jelentés eredményeinek rövid leírása, beleértve a következőket:

      i. a közös kritériumoknak az értékelés során alkalmazott verziója és adott esetben kiadása;

      ii. a közös kritériumok szerinti megbízhatósági dokumentumok vagy a biztonsági megbízhatósági komponensek jegyzéke, az értékelés során alkalmazott AVA_VAN-szint és az (EU) 2019/881 rendelet 52. cikkében meghatározott megfelelő megbízhatósági szint, amelyre az EUCC-tanúsítvány hivatkozik;

      iii. adott esetben az(ok) a védelmi profil(ok), amely(ek)nek az IKT-termék állítólagosan megfelel;

      iv. az értékelt IKT-termékre alkalmazandó biztonsági szabályzatra vonatkozó hivatkozás;

      v. adott esetben felelősségkizáró nyilatkozat(ok).

5. A 3. b) pontban említett azonosításnak egyértelműen azonosítania kell az értékelt IKT-terméket, többek között a következő információk megadásával:

   a) az értékelt IKT-termék egyedi azonosítója;

   b) az IKT-termék azon összetevőinek felsorolása, amelyek részét képezik az értékelésnek, az egyes összetevők verziószámát is feltüntetve;

   c) a tanúsított IKT-termék üzemeltetési környezetére alkalmazandó további követelményekre vonatkozó hivatkozás.

6. A 3. c) pontban említett kapcsolattartási információknak legalább a következőket kell magukban foglalniuk:

   a) a fejlesztő neve;

   b) az EUCC-tanúsítvány jogosultjának neve és elérhetőségei;

   c) a tanúsítványt kiállító tanúsító szerv neve;

   d) a felelős nemzeti kiberbiztonsági tanúsító hatóság;

   e) az értékelést elvégző ITSEF neve és adott esetben az alvállalkozók jegyzéke.

7. A 3. d) pontban említett biztonsági szabályzatnak tartalmaznia kell az IKT-termékre alkalmazandó biztonsági szabályzat biztonsági szolgáltatások gyűjteményeként megadott leírását, valamint azokat a szabályzatokat vagy szabályokat, amelyeket az értékelt IKT-terméknek érvényesítenie kell, illetve amelyeknek meg kell felelnie. Magában kell foglalnia továbbá a következő információkat is:

   a) a tanúsítvány jogosultja által alkalmazott sebezhetőségkezelési és sebezhetőségfeltárási eljárások leírása, amelyben kizárólag nyilvánosan hozzáférhetővé tehető információk tüntethetők fel;

   b) a tanúsítvány jogosultjának a megbízhatóság folytonosságára vonatkozó szabályzata, beleértve adott esetben a tanúsítvány jogosultja által alkalmazott életciklus-menedzsment vagy gyártási folyamatok leírását a IV. melléklet IV.1. szakaszával összhangban;

   c) adott esetben a javításkezelési eljárás megléte és értékelésének eredménye a IV. melléklet IV.4. szakaszával összhangban.

8. A 3. e) pontban említett feltételezéseknek és a hatály ugyanazon pontban említett egyértelműsítésének információkat kell tartalmazniuk a terméknek a 7. cikk (1) bekezdésének c) pontjában említett rendeltetésszerű használatához kapcsolódó körülményekről és célkitűzésekről, és magukban kell foglalniuk a következőket:

   a) az IKT-termék használatára és telepítésére vonatkozó feltételezések minimumkövetelmények formájában, például a megfelelő telepítési, valamint konfigurációs és hardverkövetelmények teljesítése;

   b) az IKT-termék megfelelő működéséhez szükséges környezetre vonatkozó feltételezések;

   c) az IKT-terméket fenyegető minden olyan veszély leírása, amelyet a termék értékelt biztonsági funkciói nem ellensúlyoznak a rendeltetésszerű használat során, amennyiben ez az IKT-termék potenciális felhasználója szempontjából relevánsnak minősül.

   Az első albekezdésben említett információknak a lehető legegyértelműbbnek és legérthetőbbnek kell lenniük annak érdekében, hogy a tanúsított IKT-termék potenciális felhasználói megalapozott döntéseket hozhassanak a termék használatával kapcsolatos kockázatokról.

9. A 3. f) pontban említett, az architektúrára vonatkozó információknak magukban kell foglalniuk az IKT-termék és fő összetevői magas szintű leírását, amelynek a közös kritériumok szerinti Development – TOE Design (ADV_TDS) megbízhatósági család vonatkozásában meghatározott eredményeken kell alapulnia.

10. A 3. g) pontban említett kiegészítő kiberbiztonsági információknak magukban kell foglalniuk az EUCC-tanúsítvány jogosultjának az (EU) 2019/881 rendelet 55. cikke szerinti honlapjára mutató hivatkozást.

11. A 3. h) pontban említett, az IKT-termék értékelésére és konfigurációjára vonatkozó információknak be kell mutatniuk mind a fejlesztő, mind az értékelő tesztelési tevékenységeit, ismertetve a teszteléshez alkalmazott megközelítést és konfigurációt, valamint a tesztelés mélységét. Ezen belül közölni kell legalább a következőket:

    a) a 3. cikkben említett szabványokból származó alkalmazott megbízhatósági komponensek azonosítása;

    b) a technika állásának megfelelő dokumentum verziója és az értékelés során használt további biztonsági értékelési kritériumok;

    c) az értékelés tárgyának a teszteléshez és a sebezhetőségi elemzéshez használt beállításai és konfigurációja;

    d) az esetlegesen alkalmazott védelmi profil, beleértve a következő információkat: a védelmi profil neve, verziója, dátuma és tanúsítványa.

12. A 3. i) pontban említett, az értékelés eredményeire és a tanúsítványra vonatkozó információknak magukban kell foglalniuk az elért biztonsági szintre vonatkozó információkat az e rendelet 4. cikkében és az (EU) 2019/881 rendelet 52. cikkében foglaltak szerint.

13. A 3. j) pontban említett megjegyzések és ajánlások az értékelés eredményeire vonatkozó további információk közlésére szolgálnak. A szóban forgó megjegyzések és ajánlások megtehetők például az IKT-termék tekintetében az értékelés során felfedezett hiányosságok jelzésének vagy a különösen hasznos jellemzők megemlítésének formájában.

14. A 3. k) pontban említett mellékletek olyan további információk megadására szolgálnak, amelyek hasznosak lehetnek a jelentés közönsége számára, de logikusan nem illeszthetők be a jelentés előírt szakaszaiba; ez a helyzet például a biztonsági szabályzat teljes körű leírásával.

15. A 3. l) pontban említett hivatkozásnak az értékelt biztonsági előirányzatra kell vonatkoznia. Az értékelt biztonsági előirányzathoz az (EU) 2019/881 rendelet 50. cikkének (1) bekezdésében említett honlapon való közzététel céljából mellékelni kell a tanúsítási jelentést. Amennyiben az értékelt biztonsági előirányzatot a közzététel előtt szanitizálni kell, azt e rendelet V. mellékletének V.2. szakaszával összhangban kell elvégezni.

16. A 3. m) pontban említett, az EUCC-rendszerhez kapcsolódó jelöléseket vagy címkéket a 11. cikkben megállapított szabályoknak és eljárásoknak megfelelően kell feltüntetni a tanúsítási jelentésben.

17. A 3. n) pontban említett glosszárium a jelentés könnyebb olvashatóságát szolgálja azáltal, hogy meghatározást ad azokhoz a betűszavakhoz vagy kifejezésekhez, amelyek jelentése nem nyilvánvaló.

18. A 3. o) pontban említett bibliográfia hivatkozásokat tartalmaz a tanúsítási jelentés összeállításához felhasznált valamennyi dokumentumra. A szóban forgó információknak magukban kell foglalniuk legalább a következőket:

    a) a biztonsági értékelési kritériumok, a technika állásának megfelelő dokumentumok és a további felhasznált releváns előírások;

    b) az értékelési technikai jelentés;

    c) adott esetben az összetett értékelésre vonatkozó értékelési technikai jelentés;

    d) műszaki referenciadokumentáció;

    e) fejlesztői biztonsági iránymutatás;

    f) fejlesztői konfigurációs lista.

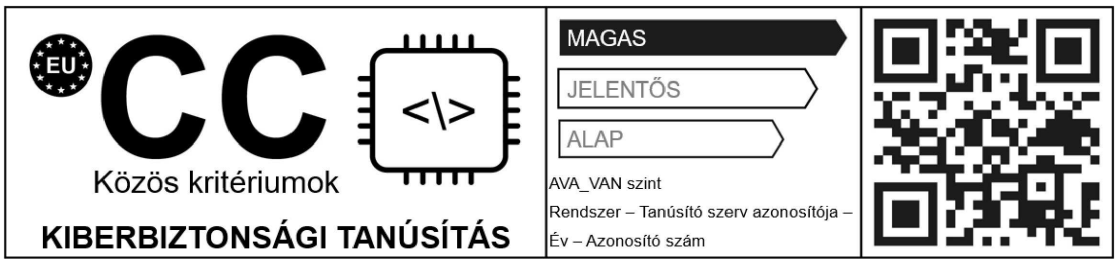
    Az értékelés reprodukálhatóságának biztosítása érdekében minden említett dokumentációt egyedileg azonosítani kell a kiadás megfelelő dátumával és a megfelelő verziószámmal.”

VI. MELLÉKLET

„IX. MELLÉKLET

Jelölés és címke

1. A jelölés és a címke formátuma a következő:



2. A jelölés és a címke kicsinyítése vagy nagyítása esetén be kell tartani az 1. pontban megadott arányokat.

3. Fizikai megjelenítés esetén a jelölésnek és a címkének legalább 5 mm magasnak kell lennie.”