REGULAMENTUL DELEGAT (UE) 2021/1244 AL COMISIEI

din 20 mai 2021

de modificare a anexei X la Regulamentul (UE) 2018/d858 al Parlamentului European și al Consiliului în ceea ce privește accesul standardizat la informațiile privind sistemele de diagnosticare la bord și cele referitoare la repararea și întreținerea vehiculelor, precum și cerințele și procedurile aplicabile accesării informațiilor referitoare la siguranța vehiculelor

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului din 30 mai 2018 privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE ([1]), în special articolul 61 alineatul (11),

întrucât:

(1) Articolul 61 alineatul (2) din Regulamentul (UE) 2018/858 obligă producătorii de vehicule să publice pe site-urile proprii de internet informații privind sistemele de diagnosticare la bord (OBD) ale vehiculelor și informații referitoare la repararea și întreținerea vehiculelor (RMI). Nu există însă criterii armonizate privind modul în care trebuie publicate aceste informații, fapt care presupune ca operatorii independenți să se adapteze unor servicii și terminologii web numeroase și diferite.

(2) Raportul Comisiei către Parlamentul European și Consiliu din 9 decembrie 2016 ([2]) privind funcționarea sistemelor de acces la informațiile privind repararea și întreținerea vehiculelor a concluzionat că standardizarea acestor site-uri de internet și a terminologiei aferente ar putea reduce volumul de muncă al operatorilor independenți.

(3) Întrucât accesul la informațiile referitoare la sistemul de diagnosticare la bord al vehiculului și la cele referitoare la repararea și întreținerea vehiculului ar trebui să fie posibil indiferent de motorizarea unui vehicul, este necesar să se clarifice faptul că accesul nu este obligatoriu doar în cazul cerințelor legate de emisii.

(4) La 15 septembrie 2014, Comitetul European pentru Standardizare (CEN) a publicat părțile 1-5 ale standardului EN ISO 18541 „Vehicule rutiere – Acces standardizat la informațiile referitoare la repararea și întreținerea autovehiculelor (RMI)”. Aceste părți au ca obiectiv facilitarea schimbului de informații între producători și operatori independenți cu privire la sistemul de diagnosticare la bord al vehiculului și la repararea și întreținerea vehiculului, prin stabilirea cerințelor tehnice și procedurilor pentru facilitarea accesului la aceste informații. Este așadar oportun să se facă trimitere în anexa X la Regulamentul (UE) 2018/858 la cerințele părților 1-5 din standardul EN ISO 18541-2014.

(5) Întrucât informațiile referitoare la sistemul de diagnosticare la bord al vehiculului și cele referitoare la repararea și întreținerea vehiculului cuprind date importante pentru securitatea vehiculului, accesul la anumite caracteristici de securitate ale vehiculului ar trebui permis doar operatorilor independenți care îndeplinesc cerințele stabilite în prezenta anexă.

(6) Conform recomandărilor forumului privind accesul la informațiile referitoare la vehicule, la care se face trimitere în articolul 66 alineatul (1) din Regulamentul (UE) 2018/858, aceste cerințe ar trebui să includă aprobarea a operatorilor independenți în cauză și autorizarea angajaților acestora care desfășoară activități relevante de către entități acreditate. Este prin urmare necesar să se instituie o procedură privind aprobarea și autorizarea operatorilor independenți pentru a putea accesa caracteristicile de securitate ale vehiculului, procedură care ar trebui să aibă la bază „Schema de acreditare, aprobare și autorizare în vederea accesării informațiilor privind repararea și întreținerea (RMI) vehiculului legate de securitate”, care a fost validată la 19 mai 2016 de Cooperarea Europeană pentru Acreditare. De asemenea, este necesar să se stabilească dacă astfel de operatori nu sunt implicați în activități economice nelegale.

([1]) JO L 151, 14.6.2018, p. 1.

([2]) Raportul Comisiei către Parlamentul European și Consiliu privind funcționarea sistemelor de acces la informațiile privind repararea și întreținerea vehiculelor prevăzute de Regulamentul (CE) nr. 715/2007 privind omologarea de tip a autovehiculelor în ceea ce privește emisiile provenind de la vehiculele ușoare pentru pasageri și de la vehiculele ușoare comerciale (Euro 5 și Euro 6) și privind accesul la informațiile referitoare la repararea și întreținerea vehiculelor [COM(2016) 782 final].

(7) În plus, este necesar să se prevadă rolul și responsabilitățile organismelor care participă la aprobarea și autorizarea operatorilor independenți și a angajaților acestora pentru a li se permite accesul la informațiile privind repararea și întreținerea vehiculului legate de securitate.

(8) Pentru a permite statelor membre și autorităților naționale, precum și operatorilor economici să se pregătească pentru aplicarea noilor norme introduse prin prezentul regulament, data aplicării ar trebui amânată.

(9) Prin urmare, anexa X la Regulamentul (UE) 2018/858 ar trebui modificată în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa X la Regulamentul (UE) 2018/858 se modifică în conformitate cu anexa la prezentul regulament.

Articolul 2

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la 30 iulie 2023.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 20 mai 2021.

Pentru Comisie,
Președintele
Ursula VON DER LEYEN

ANEXĂ

Anexa X la Regulamentul (UE) 2018/858 se modifică după cum urmează:

1. Punctul 2.1 se înlocuiește cu următorul text:

„2.1. Un producător pune în aplicare dispozițiile și procedurile necesare, în conformitate cu articolul 61 alineatul (2) al doilea paragraf prima teză, pentru a se asigura că accesul la informațiile privind sistemele OBD ale vehiculelor și la cele referitoare la repararea și întreținerea vehiculelor este posibil prin intermediul site-urilor de internet. Conformarea producătorilor cu obligația de a asigura prin intermediul site-urilor proprii de internet și într-un format standardizat acces la informațiile privind sistemele OBD ale vehiculelor și la cele referitoare la repararea și întreținerea vehiculelor se consideră că este în conformitate cu partea 1 «Informații generale și definirea cazurilor de utilizare», partea 2 «Cerințe tehnice», partea 3 «Cerințe funcționale privind interfața cu utilizatorul» din standardul EN ISO 18541 – 2014, partea 4 «Testul de conformitate» din standardul EN ISO 18541 – 2015 și partea 5 «Prevederi specifice privind vehiculele grele» «Vehicule rutiere - Acces standardizat la informațiile referitoare la repararea și întreținerea autovehiculelor (RMI)» din standardul EN ISO 18541 – 2018. Accesul la informațiile privind sistemele OBD ale vehiculelor și la cele referitoare la repararea și întreținerea vehiculelor se asigură într-o manieră ușor accesibilă și rapidă."

2. Punctul 2.5.2 se înlocuiește cu următorul text:

„2.5.2. carnete de întreținere, cuprinzând istoricul lucrărilor de reparații și întreținere, precum și specificații tehnice privind fluidele, inclusiv lubrifianții, lichidele de frână și lichidele de răcire;".

3. La punctul 2.9, primul alineat se înlocuiește cu următorul text:

„În scopul sistemelor OBD, al diagnosticării, reparării și întreținerii, monitorizării și inspecției vehiculelor, fluxul direct de date referitoare la vehicul, inclusiv codurile de eroare și funcțiile de diagnosticare, este pus la dispoziție prin intermediul portului serial de date de pe conectorul standardizat pentru transmisia de date de la punctul 6.5.1.4 și în conformitate cu specificațiile prevăzute în secțiunea 6.5.3. din apendicele 1 al anexei 11 la Regulamentul nr. 83 al Comisiei Economice pentru Europa a Organizației Națiunilor Unite (CEE-ONU) (*) și în conformitate cu punctul 4.7.3 din anexa 9B și cu documentele privind standardul de referință prevăzute în apendicele 6 al anexei respective la Regulamentul ONU nr. 49 Comisiei Economice pentru Europa a Organizației Națiunilor Unite (CEE-ONU) (**)

(*) Regulamentul nr. 83 al Comisiei Economice pentru Europa a Organizației Națiunilor Unite (CEE-ONU) – Dispoziții uniforme privind omologarea vehiculelor în ceea ce privește emisia de gaze poluante în conformitate cu cerințele privind combustibilul (JO L 42, 15.2.2012, p. 1).

(**) Regulamentul nr. 49 al Comisiei Economice pentru Europa a Organizației Națiunilor Unite (CEE-ONU) - Dispoziții uniforme privind măsurile care trebuie luate împotriva emisiilor de gaze și de particule poluante provenite de la motoarele cu aprindere prin compresie utilizate la vehicule și împotriva emisiilor de gaze poluante provenite de la motoarele cu aprindere prin scânteie alimentate cu gaz sau cu gaz petrolier lichefiat utilizate la vehicule (JO L 180, 8.7.2011, p. 53)."

4. La punctul 6.1, primul alineat se înlocuiește cu următorul text:

„Obligația producătorilor de a furniza informațiile privind sistemele OBD și informațiile referitoare la repararea și întreținerea vehiculelor pe site-urilor lor de internet într-un format standard este presupusă a fi respectată dacă aceștia se conformează părților din standardul EN ISO 18541 menționate la punctul 2.1."

5. Punctul 6.2 se înlocuiește cu următorul text:

„Accesul la caracteristicile de securitate ale vehiculului este acordat operatorilor independenți sub protecția unei tehnologii de securitate în conformitate cu următoarele cerințe:".

6. Punctul 6.3 se modifică după cum urmează:

(a) prima teză se înlocuiește cu următorul text:

„Procedura de aprobare și autorizare a operatorilor independenți în vederea accesării caracteristicilor de securitate ale vehiculului în condițiile prevăzute la punctul 6.2 este stabilită în apendicele 3. Rolul și responsabilitățile organismelor implicate în acreditarea, aprobarea și autorizarea operatorilor independenți sunt detaliate în cerințele funcționale constând în exemple și cazuri de utilizare prevăzute în comunicarea Comisiei.";

(b) se adaugă următorul alineat:

„În sensul acestei proceduri, se va considera că operatorii nu desfășoară o activitate economică legală în cazul în care anunță public sau oferă servicii de reparații sau întreținere care ar avea efecte negative asupra performanței privind emisiile generate de vehicul. Acestea cuprind:

(a) dezactivarea sau dezinstalarea dispozitivelor pentru controlul poluării sau a sistemelor de control al emisiilor ori deteriorarea performanțelor sau ascunderea funcționării defectuoase a acestora;

(b) instalarea unor dispozitive de manipulare (*) sau utilizarea unor strategii de invalidare (**);

(c) dezactivarea, dezinstalarea sau modificarea neautorizată a dispozitivelor de monitorizare a consumului de combustibil sau de energie electrică ori modificarea neautorizată a înregistrărilor odometrului;

(d) modificarea neautorizată a unității de comandă a motorului, inclusiv a puterii nominale a motorului.

_____

(*) Astfel cum au fost definite la articolul 3 alineatul (10) din Regulamentul (CE) nr. 715/2007.

(**) Astfel cum au fost definite la articolul 3 alineatul (8) din Regulamentul (CE) nr. 595/2009."

7. Se adaugă următorul apendice 3:

„***Apendicele 3***

Procedura de aprobare și autorizare a operatorilor independenți în vederea accesării caracteristicilor de securitate ale vehiculului (*)

1. Domeniul de aplicare

Prezentul apendice cuprinde cerințele aplicabile aprobării și autorizării operatorilor independenți care solicită acces la informații privind repararea și întreținerea (RMI) vehiculului legate de securitate.

Apendicele specifică detaliat procesul și organismele necesare pentru aprobarea și autorizarea operatorilor independenți pentru accesul la informații legate de securitate privind repararea și întreținerea vehiculelor ușoare de pasageri și comerciale și a vehiculelor grele.

2. Definiții și abrevieri

2.1. Definiții

În sensul prezentului apendice, se aplică următoarele definiții:

2.1.1. «Acreditare»

«acreditare» înseamnă acreditarea astfel cum este definită la articolul 2 alineatul (10) din Regulamentul (CE) nr. 765/2008

2.1.2. «Angajat al unui OI»

«angajat al unui OI» înseamnă angajatul unui operator independent (OI) aprobat care, în urma autorizării de către organismul său de evaluare a conformității (CAB), va avea acces la RMI legate de securitate

2.1.3. «Informații privind repararea și întreținerea vehiculului legate de securitate» sau «RMI legate de securitate»

«informații privind repararea și întreținerea vehiculului legate de securitate» sau «RMI legate de securitate» înseamnă informațiile, programele informatice, funcțiile și serviciile necesare reparării și întreținerii caracteristicilor incluse într-un vehicul de către producător pentru a preveni furtul sau deplasarea acestuia și pentru a permite urmărirea și recuperarea vehiculului.

2.1.4. «Certificat de inspecție de aprobare»

«certificat de inspecție de aprobare» însemnă certificatul emis de CAB operatorilor independenți care îndeplinesc criteriile de aprobare prevăzute în prezentul apendice, certificat care confirmă faptul că respectivii OI sunt aprobați și că angajații lor pot solicita autorizarea în vederea accesului la RMI legate de securitate.

2.1.5. «Certificat de inspecție de autorizare»

«certificat de inspecție de autorizare» înseamnă certificatul emis de CAB angajaților unui OI care îndeplinesc criteriile de autorizare prevăzute în prezentul apendice, certificat care confirmă faptul că respectivii angajații sunt autorizați să acceseze RMI legate de securitate pe site-ul de internet al producătorului vehiculului.

2.1.6. «Centru de încredere» sau «TC»

«centru de încredere» sau «TC» înseamnă organismul desemnat de SERMI și agreat de Comisie cu următoarele atribuții:

(a) gestionează certificatele digitale și stadiul autorizării angajaților unui OI și transmite CAB dispozitivele de securitate de tip token și certificate digitale necesare ale angajaților autorizați ai OI;

(b) transmite unui producător de vehicule informații privind stadiul autorizării unui angajat al unui OI.

2.1.7. «Dispozitiv de securitate de tip token»

«dispozitiv de securitate de tip token» înseamnă dispozitivul care permite autentificarea unui OI în condiții de siguranță.

2.1.8. «Certificat digital»

«certificat digital» însemnă certificatul digital care necesită o semnătură digitală a centrului de încredere emitent pentru a asocia o cheie publică cu identitatea angajatului unui OI, în conformitate cu standardul ISO 9594.

2.1.9. «Bază de date cu autorizații»

«bază de date cu autorizații» înseamnă o bază de date deținută de centrul de încredere și care conține detaliile de autorizare ale angajaților autorizați anonimizați ai OI și detaliile privind înregistrarea OI agreați.

2.1.10. «Bază de date cu certificate»

«bază de date cu certificate» înseamnă o bază de date deținută de centrul de încredere cu scopul de a gestiona validitatea certificatului digital și a codurilor de identificare ale angajaților autorizați ai OI.

2.1.11. «Cooperarea Europeană pentru Acreditare» sau «EA»

«Cooperarea Europeană pentru Acreditare» sau «EA» înseamnă organismul recunoscut de Comisie în temeiul articolului 14 din Regulamentul (CE) nr. 765/2008 și care este responsabil pentru dezvoltarea, menținerea și punerea în aplicare a acreditării în Uniune.

2.1.12. «Forumul privind accesul la RMI legate de securitate» sau «SERMI»

«Forumul privind accesul la RMI legate de securitate» sau «SERMI» înseamnă entitatea cu atribuții de coordonare care acordă consiliere Comisiei cu privire la introducerea procedurilor de „acreditare, aprobare și autorizare în vederea accesării” RMI legate de securitate.

2.1.13. «Autorități relevante»

«autorități relevante» înseamnă autoritățile publice cu atribuții stabilite prin lege în domeniul protecției împotriva infracțiunilor la adresa securității vehiculelor, precum și în domeniul anchetării acestora și trimiterii în judecată.

3. Acreditarea CAB, aprobarea OI și autorizarea angajaților unui OI

Doar CAB acreditate de organismul național de acreditare («NAB»), astfel cum este definit la articolul 2, punctul 11 din Regulamentul (CE) nr. 765/2008, al statului membru în care sunt înregistrate emite certificatele de inspecție de aprobare, prin care atestă acreditarea unui OI, și certificatele de inspecție de autorizare, prin care atestă autorizarea unui angajat al unui OI în vederea accesării RMI legate de securitate.

Aprobarea OI și autorizarea angajatului unui OI se acordă pe o perioadă de 60 de luni de la data emiterii certificatelor de inspecție respective.

OI care doresc să primească RMI legate de securitate trebuie să obțină un certificat de inspecție de aprobare din partea unui CAB acreditat de NAB al statului membru în care sunt înregistrați.

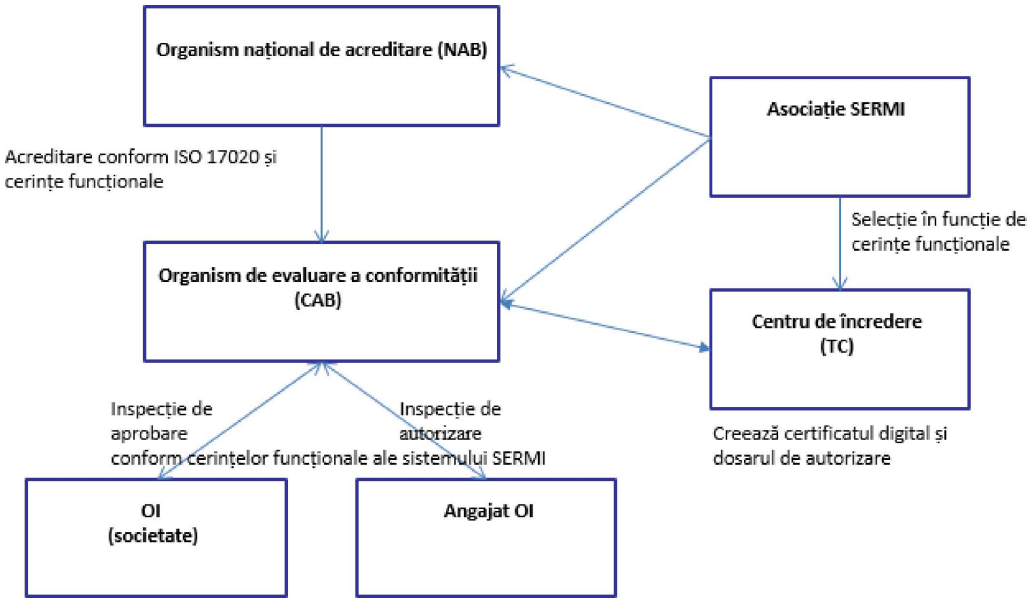
Angajații unui OI care urmează să folosească RMI legate de securitate trebuie să obțină un certificat de inspecție de autorizare din partea unui CAB acreditat de NAB al statului membru în care își au reședința.

CAB informează TC cu privire la toate certificatele de inspecție de aprobare sau certificatele de inspecție de autorizare emise; pe baza acestor informări, TC creează o evidență a autorizațiilor și emite un dispozitiv de securitate de tip token și un certificat digital conținând detalii care permit angajaților unui OI să fie identificați în mod unic pe site-ul de internet cu RMI al producătorului vehiculului. CAB-urile emit fiecărui angajat al unui OI câte un dispozitiv de securitate de tip token și câte un certificat digital.

Producătorii de vehicule pot solicita o taxă pentru înregistrarea angajaților unui OI pe aceste site-uri de internet cu RMI ale producătorilor de vehicule, precum și pentru accesul la RMI legate de securitate. Taxa trebuie să fi proporțională cu costul înregistrării și asigurării accesului. Taxele datorate trebuie specificate pe site-urile de internet cu RMI al producătorilor de vehicule. Toate transferurile de date în format digital între OI, TC și CAB se realizează cu promptitudine, folosind protocoale securizate, prin tranzacții business-to-business (B2B).

Figura 1

Organisme care participă la acreditarea CAB, aprobarea OI și autorizarea angajaților OI, precum și relațiile între aceste organisme



OI care solicită autorizarea de către CAB trebuie să semneze o declarație prin care să arate că desfășoară o activitate economică legală astfel cum se menționează la punctul 6.3 din prezenta anexă. Un OI este aprobat doar în urma unei inspecții în care CAB verifică dacă această declarație a fost semnată și dacă OI și fiecare dintre angajații săi îndeplinesc cerințele prevăzute în prezentul apendice.

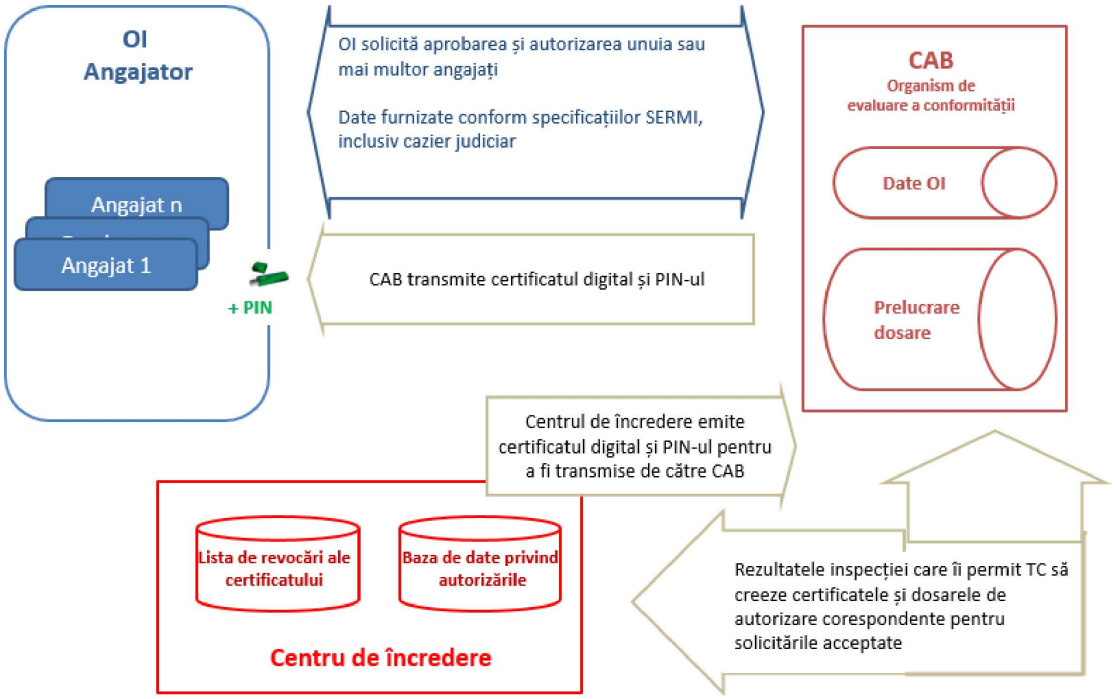
Angajații OI individuali sunt autorizați numai în urma unei inspecții efectuate de un CAB. CAB-urile controlează documentele prezentate și verifică dacă angajatul OI respectiv a mai formulat o cerere de autorizare care a fost respinsă de CAB în cauză sau de orice alt CAB din Uniune.

CAB trimit TC toate datele necesare pentru producerea certificatului digital și a dispozitivului de securitate de tip token pe care CAB le trimite apoi angajaților OI.

Angajații OI care au fost autorizați primesc de la CAB-uri PIN-ul asociat certificatului digital.

Figura 2

Procesul de aprobare a OI și de autorizare a angajaților OI



3.1. Prezentare generală a accesului la RMI legate de securitate

Producătorii de vehicule asigură accesul la RMI legate de securitate prin intermediul site-urilor lor de internet privind RMI, cu condiția ca angajații OI să fie autorizați și să poată prezenta certificatul de inspecție de autorizare, precum și cu condiția ca OI în numele căruia acționează respectivii angajații să dețină un certificat de inspecție de aprobare.

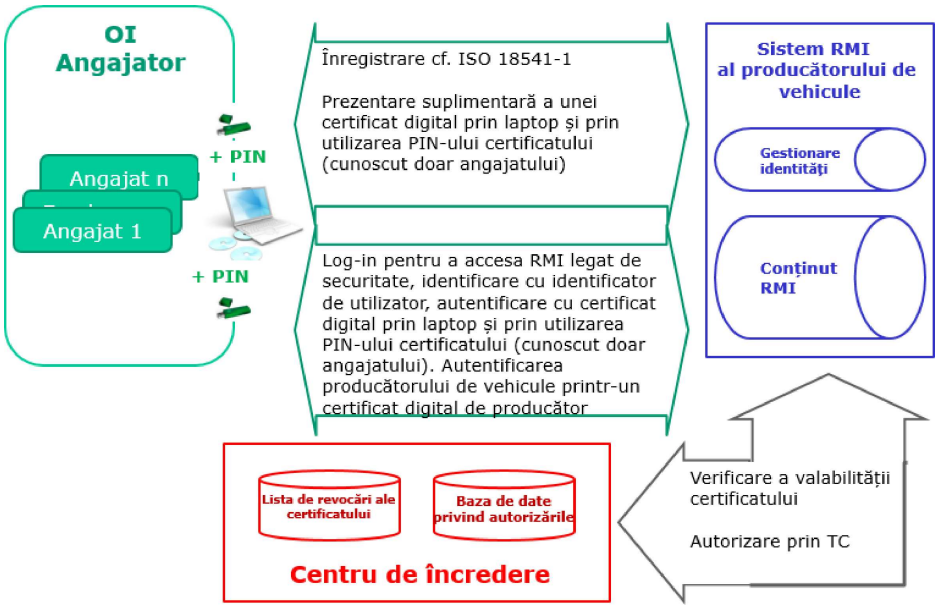
Producătorii pot să ofere angajaților autorizați ai OI aprobate acces la o platformă on-line pentru comanda pieselor legate de securitate folosind o aplicație specializată legată de site-ul de internet cu RMI.

La primirea unei cereri de accesare a unui site de internet cu RMI, site-urile de internet ale producătorilor de vehicule solicită identificarea cu codul unic de identificare a angajatului OI, precum și autentificarea. Angajații OI se autentifică exclusiv folosind certificate digitale. La primirea unui certificat digital, site-urile de internet cu RMI ale producătorului vehiculului verifică codul unic de identificare a angajatului OI și situația actuală a certificatului digital și a autorizării, prin comunicarea cu TC identificat în certificatul digital.

Toate transferurile de date în format digital între OI, producătorii de vehicule, TC și CAB se realizează cu promptitudine, folosind protocoale securizate, prin tranzacții business-to-business (B2B). După verificarea codului unic de identificare și a stadiului autorizării angajatului OI, producătorul vehiculului permite accesul prin intermediul site-ul său de internet la RMI legate de securitate solicitate.

Figura 3

Accesul la RMI legate de securitate



4. Reguli detaliate privind accesul la RMI legate de securitate

4.1. Rolul SERMI

4.1.1. Responsabilități și obligații

SERMI monitorizează aplicarea procesului de acreditare în statele membre și informează Comisia în consecință. SERMI consiliază Comisia cu privire la solicitările de modificare a procesului de acreditare.

(a) SERMI consiliază Comisia cu privire la solicitările de modificare a procesului de acreditare. SERMI monitorizează aplicarea procesului de acreditare în statele membre și informează Comisia în consecință;

(b) SERMI consultă Comisia cu privire la stabilirea criteriilor de selecție a TC;

(c) SERMI consiliază Comisia cu privire la introducerea unor ghiduri de implementare tehnică privind interacțiunea între entitățile participante la proces;

(d) SERMI respectă regulile EA privind titularii schemei;

(e) membrii SERMI sunt reprezentați de părțile interesate implicate în procesul de acreditare, aprobare și autorizare în vederea accesării RMI legate de securitate.

4.1.2. Selecția centrului de încredere

SERMI selectează TC și transmite propunerea Comisiei spre aprobare.

TC selectat trebuie să respecte standardul ETSI TS 319 411-3 și să îndeplinească cerințele privind semnătura electronică stabilite în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului (**) și cerințele prevăzute la punctul 4.6 al prezentului apendice.

În plus, TC trebuie:

— să dețină competențele tehnice și manageriale, viabilitatea financiară și experiența adecvate pentru procesul de acreditare;

— să dispună de personal-cheie cu aptitudinile, experiența și disponibilitatea necesare în procesul de acreditare;

— să poată funcționa în toate statele membre;

— să aplice un proces de asigurare a calității la nivel operațional.

4.2. Rolul NAB

NAB au atribuția de a acredita CAB în scopul agreării OI și al aprobării angajaților acestora în vederea accesării RMI legate de securitate.

4.2.1. Responsabilități și cerințe

Responsabilitățile și cerințele aplicabile NAB sunt cele prevăzute la articolele 8-12 din Regulamentul (CE) nr. 765/2008.

4.2.2. Criterii pentru acreditarea CAB

CAB se acreditează ca organisme de inspecție de tip A, în conformitate cu standardul ISO/IEC 17020:2012. CAB trebuie să îndeplinească cerințele privind cel mai înalt nivel de independență.

În plus, NAB verifică capacitatea CAB de a îndeplini cerințele stabilite la punctele 4.3.1-4.3.4.

Personalul care desfășoară inspecțiile OI trebuie să dețină cunoștințe în domeniul activităților economice de reparare și întreținere a autovehiculelor și al pieței serviciilor post-vânzare pentru autovehicule la un nivel corespunzător sarcinilor pe care le îndeplinesc.

4.3. Rolul CAB

CAB are ca atribuții inspectarea OI și a angajaților acestora, precum și emiterea și revocarea certificatelor de inspecție de aprobare și a certificatelor de inspecție de autorizare în condițiile prezentului apendice.

4.3.1. Responsabilități și cerințe

(a) CAB păstrează datele primite în vederea agreării unui OI;

(b) CAB stabilesc canale de comunicare securizată cu TC căruia îi transmit rezultatele inspecției în vederea emiterii dispozitivului de securitate de tip token însoțit de certificatul digital;

(c) CAB notifică angajații OI cu 6 luni înainte de expirarea autorizației acestora;

(d) CAB mențin o bază de date care conține datele primite în vederea autorizării angajaților OI;

(e) CAB care refuză aprobarea unui OI sau autorizarea unui angajat al unui OI comunică TC rezultatele inspecției privind respectivul OI sau respectivul angajat;

(f) CAB culeg și folosesc doar datele necesare în procesul de agreare sau autorizare;

(g) CAB păstrează confidențialitatea tuturor datelor legate de OI și de angajații acestora și ia măsuri pentru ca doar angajații autorizați să aibă acces la astfel de date;

(h) CAB prezintă anual SERMI și Comisiei situații statistice privind numărul aprobărilor și autorizațiilor emise, precum și privind numărul cererilor refuzate;

(i) CAB păstrează în siguranță evidențe privind inspecțiile de aprobare și de autorizare pe o perioadă de cinci ani;

(j) CAB informează alte CAB din statul membru în care este înregistrat cu privire la rezultatele negative ale inspecției unui OI;

(k) OI și angajații acestora în cazul cărora rezultatul inspecției este negativ pot transmite CAB informații suplimentare prin care corectează deficiențe minore în termen de 15 zile de la primirea rezultatului negativ al inspecției; CAB decid în consecință dacă rezultatul inspecției trebuie modificat;

(l) CAB notifică OI cu 6 luni înainte de expirarea aprobării acestora;

(m) În perioada de 60 de luni de valabilitate a aprobării, CAB desfășoară inspecții aleatorii, inopinate la sediile OI și supune fiecare OI cel puțin unei inspecții aleatorii la fața locului în perioada de 60 de luni de valabilitate a aprobării;

(n) La primirea unei plângeri împotriva unui OI aprobat sau a unui angajat autorizat al unui OI, CAB vor verifica dacă respectivul OI sau angajat îndeplinește criteriile pe baza cărora a fost aprobat, respectiv autorizat. În cadrul investigației, CAB stabilește dacă este necesară o inspecție la fața locului;

(o) În scopul inspecțiilor la fața locului, CAB pot solicita asistența autorităților cu atribuții în domeniul supravegherii pieței din statul membru în care sunt înregistrate;

(p) CAB revocă agreările OI și autorizațiile angajaților OI în cazurile în care aceștia nu mai îndeplinesc criteriile pe baza cărora au fost aprobați, respectiv autorizați. În consecință, CAB solicită TC să suspende și să anuleze certificatele digitale ale angajaților OI vizați.

4.3.2. Reînnoirea aprobării

La cererea unui OI sau cu 6 luni înainte de expirarea validității agreării, CAB desfășoară o inspecție la fața locului și, în cazul unui rezultat pozitiv al inspecției, reînnoiește aprobarea.

CAB emite un nou certificat de inspecție de aprobare OI care îndeplinesc criteriile de aprobare.

CAB evaluează cererile de reînnoirea a autorizațiilor și emite angajaților OI care îndeplinesc criteriile de autorizare un certificat de inspecție de autorizare.

4.3.3. Criterii de aprobare a OI de către CAB

Înainte de aprobarea unui OI și în timpul oricărei inspecții la fața locului efectuate în timpul perioadei de valabilitate a aprobării, CAB verifică următoarele:

(a) dovada dreptului de proprietate asupra OI, numele administratorului;

(b) lista cu angajații propuși spre autorizare prezentată de OI;

(c) informații privind responsabilitatea și atribuțiile angajaților menționați la punctul (a);

(d) dacă OI dispune de o asigurare de răspundere civilă cu o valoare minimă a despăgubirilor de 1 milion de euro pentru vătămări corporale și de 0,5 milioane de euro pentru daune provocate bunurilor;

(e) dacă aprobarea OI a fost revocată din motive de utilizare abuzivă;

(f) dacă OI a prezentat dovezi că își desfășoară activitatea în sectorul autovehiculelor;

(g) dacă OI a semnat declarația prin care se certifică faptul că desfășoară o activitate economică legală astfel cum se menționează la punctul 6.3 și, în timpul inspecției la fața locului, dacă OI desfășoară în realitate o activitate economică legală;

(h) dacă OI sau angajații acestuia nu au cazier judiciar;

(i) dacă reprezentantul legal al OI a semnat o declarație conform căreia respectarea cerințelor procedurale stabilite la punctul 4.3.4 este asigurată pentru toate operațiunile legate de securitatea vehiculului.

4.3.4. Criterii pentru autorizarea angajaților OI de către CAB

Înainte de autorizarea unui angajat al unui OI și în timpul oricărei inspecții la desfășurate la fața locului în perioada de valabilitate a autorizației, CAB verifică următoarele:

(a) dacă angajatul în cauză nu a dispus de o autorizație anterioară care a fost revocată ca urmare a utilizării abuzive a autorizației respective;

(b) dacă angajatul are cazier judiciar;

(c) dacă există un contract de muncă între angajatul în cauză și un OI aprobat;

(d) dacă angajatul în cauză deține o carte de identitate specifică țării sau un document echivalent.

4.4. Rolul OI

4.4.1. Responsabilități și cerințe

(a) OI solicită CAB local să efectueze inspecția în vederea aprobării;

(b) OI informează CAB competent cu privire la modificarea datelor de contact proprii;

(c) OI informează CAB în momentul dizolvării activității proprii;

(d) OI înregistrează fiecare transfer și fiecare operațiune care implică RMI legate de securitate;

(e) OI informează CAB competent cu privire la încetarea contractului de muncă al oricărui angajat autorizat propriu;

(f) OI raportează autorităților relevante orice infracțiune sau abatere săvârșită de angajații lor autorizați și care implică RMI legate de securitate;

(g) OI iau măsuri pentru ca angajații lor autorizați să folosească doar propriile certificate de inspecție de autorizare;

(h) OI iau măsuri pentru plata tuturor taxelor aferente autorizării angajaților lor;

(i) OI iau măsuri pentru ca angajații lor să fie instruiți pentru executarea lucrărilor de reparații privind întreținerea, reprogramarea, precum și funcțiile de securitate și siguranță ale autovehiculelor;

(j) OI solicită CAB competent să efectueze o inspecție la fața locului în perioada de șase luni înainte de expirarea certificatului de inspecție de aprobare.

4.5. Rolul angajaților OI

4.5.1. Responsabilități și cerințe

(a) Angajații OI solicită autorizarea din partea CAB;

(b) Angajații OI se înregistrează în sistemul RMI al producătorului vehiculului;

(c) Angajații OI accesează RMI legate de securitate în conformitate cu standardul EN ISO 18541-2014;

(d) Angajații OI se asigură că toate evidențele privind RMI legate de securitate descărcate din sistemul cu RMI al producătorului vehiculului nu sunt păstrate mai mult decât este necesar pentru executarea operațiunii pentru care sunt necesare;

(e) Atunci când este cazul, angajații OI își anunță angajatorul că certificatul lor digital nu mai este necesar;

(f) Angajații OI nu transmit terților dispozitivul de securitate de tip token, certificatul digital sau PIN-ul;

(g) Angajații OI răspund de utilizarea corectă a dispozitivului de securitate de tip token personal și a PIN-ului;

(h) Angajații OI își informează angajatorul și TC local cu privire la pierderea sau utilizarea abuzivă a dispozitivului de securitate de tip token în termen de 24 de ore de la pierdere sau utilizarea abuzivă;

(i) Angajații OI raportează autorităților relevante orice solicitare sau acțiune a altor angajați ai OI care privește RMI legate de securitate și care nu constituie o activitate economică legală astfel cum este menționat la punctul 6.3 din prezenta anexă.

4.6. Rolul centrului de încredere

TC creează certificate digitale pentru OI și, prin intermediul CAB corespunzătoare, le transmit OI și angajaților acestora. TC mențin o bază de date a certificatelor de inspecție de autorizare emise. TC asigură producătorilor de vehicule accesul la o interfață prin care aceștia pot verifica situația certificatelor digitale și a certificatelor de inspecție de autorizare.

TC păstrează în baza de date a autorizațiilor informațiile privind angajații OI pe o perioadă suplimentară de maximum 60 de luni. Această perioadă nu depășește perioada rămasă de valabilitate a aprobării OI la care lucrează angajatul OI.

4.6.1. Responsabilități și cerințe

(a) TC pot suspenda și anula certificate digitale la cererea CAB;

(b) TC transmit OI și angajaților acestora programele software necesare pentru utilizarea certificatelor digitale;

(c) TC funcționează 24 de ore pe zi, 7 zile pe săptămână.

4.7. Rolul producătorilor de vehicule

Producătorii de vehicule asigură tuturor OI aprobați și angajaților autorizați ai acestora accesul la informații privind repararea și întreținerea vehiculului legate de securitate. Producătorii de vehicule comunică cu TC pentru a verifica situația autorizării și autentificării angajaților OI care doresc să acceseze astfel de informații.

4.7.1. Responsabilități și cerințe

(a) Producătorii de vehicule se asigură că site-urile lor de internet sunt adaptate astfel încât să suporte accesul OI la RMI legate de securitate;

(b) Producătorii de vehicule se asigură că descarcă specificațiile tehnice puse la dispoziție pe site-ul de internet al SERMI.

4.7.2. Cerințe procedurale aplicabile producătorilor de vehicule

Producătorii de vehicule nu acordă acces la RMI legate de securitate decât în condițiile îndeplinirii tuturor cerințelor procedurale de mai jos:

(1) Cerințe procedurale privind vehiculele furate

Producătorii de vehicule păstrează evidența tuturor vehiculelor cu marca proprie raportate de autorități ca fiind furate.

Producătorii de vehicule instituie un proces care asigură trasabilitatea clară și răspunderea și care permite autorităților relevante să urmărească datele transmise de producătorul vehiculului către angajatul OI care a primit acces la informații legate de vehiculul furat.

(2) Cerințe procedurale privind păstrarea informațiilor

Producătorii de vehicule păstrează următoarele date pentru fiecare situație în care acordă acces la informații privind repararea și întreținerea vehiculului legate de securitate:

(a) numărul de identificare al vehiculului (VIN) despre care s-au solicitat informații;

(b) data la care a fost formulată solicitarea;

(c) numărul de înmatriculare al vehiculului despre care s-au solicitat informații, dacă este cunoscut;

(d) tipul, varianta și, după caz, versiunea vehiculului despre care s-au solicitat informații.

Producătorii de vehicule păstrează aceste date timp de 5 ani.

(*) Cerințele stabilite în prezentul apendice au la bază cerințele prevăzute în „Schema de acreditare, aprobare și autorizare în vederea accesării informațiilor privind repararea și întreținerea (RMI) vehiculului legate de securitate”, validată la 19 mai 2016 de Cooperarea Europeană pentru Acreditare (https://www.vehiclesermi.eu/).

(**) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).”