2025/2462

9.12.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/2462 AL COMISIEI

din 8 decembrie 2025

de modificare a Regulamentului de punere în aplicare (UE) 2024/482 în ceea ce privește definițiile, certificarea seriilor de produse TIC, continuitatea asigurării și documentele ce reflectă stadiul actual al tehnologiei

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) ([1]), în special articolul 49 alineatul (7),

întrucât:

(1) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([2]) precizează rolurile, normele și obligațiile, precum și structura sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) în conformitate cu cadrul european de certificare a securității cibernetice prevăzut în Regulamentul (UE) 2019/881.

(2) Metodologia comună de evaluare care însoțește criteriile comune (CC), un standard internațional pentru evaluarea securității informațiilor, permite evaluarea securității produselor TIC în scopul certificării. În acest context, unele produse TIC, denumite și serii de produse, pot fi construite pe aceeași bază funcțională pentru a oferi funcționalități de securitate similare pe platforme sau aparate diferite. Cu toate acestea, proiectarea, hardware-ul, firmware-ul sau software-ul pot varia de la un produs TIC la altul. Este de competența organismului de certificare să decidă, de la caz la caz, dacă este posibilă certificarea unei serii de produse. Condițiile pentru certificarea seriilor de produse ar putea fi ilustrate mai în detaliu în orientările EUCC aferente.

(3) Pentru a menține fiabilitatea produselor certificate, este esențial să se definească ceea ce constituie o modificare majoră și minoră a obiectivului evaluării sau a mediului său, inclusiv a mediilor sale operaționale sau de dezvoltare. Prin urmare, este necesar să se specifice noțiunile respective, luând în considerare specificațiile tehnice existente și utilizate pe scară largă ale Grupul înalților funcționari pentru securitatea sistemelor informatice (SOG-IS) și ale participanților la Acordurile privind recunoașterea certificatelor privind criteriile comune în domeniul securității informatice (CCRA).

(4) Modificările minore sunt adesea caracterizate de efectul lor limitat asupra declarației de asigurare a produsului furnizate de certificatul EUCC emis. Astfel, modificările minore ar trebui gestionate în cadrul procedurilor de întreținere și nu necesită o reevaluare a funcționalităților de securitate ale produsului. Printre exemplele de modificări minore care ar trebui abordate prin întreținere se numără, fără a se limita la acestea, modificările de redactare, modificările aduse țintei mediului de evaluare care nu modifică ținta certificată a evaluării și modificările aduse țintei certificate de evaluare care nu afectează dovezile de asigurare. Modificările aduse mediului de dezvoltare pot fi, de asemenea, considerate minore, cu condiția ca acestea să nu aibă niciun impact ulterior asupra măsurilor de asigurare existente. Cu toate acestea, în unele cazuri, acestea pot necesita o evaluare parțială a măsurilor relevante.

([1]) JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) O modificare majoră este orice modificare a obiectivului certificat de evaluare sau a mediului său care ar putea avea un impact negativ asupra asigurării exprimate în certificatul EUCC și, prin urmare, ar trebui să necesite o reevaluare. Printre exemplele de modificări majore se numără, fără a se limita la acestea, modificările aduse setului de cerințe de asigurare declarate, cu excepția cerințelor de asigurare ale familiei CC ALC_FLR (remedierea deficiențelor), modificările controalelor privind confidențialitatea sau integritatea mediului de dezvoltare, în cazul în care astfel de modificări ar putea afecta dezvoltarea sau producerea în condiții de siguranță a țintei de evaluare sau modificările țintei de evaluare pentru a soluționa o vulnerabilitate exploatabilă. În plus, o serie de modificări minore care exercită în mod colectiv un impact semnificativ asupra securității pot fi, de asemenea, calificate drept modificări majore. De asemenea, este important să se recunoască faptul că, deși o soluție greșită poate afecta doar un anumit aspect al obiectivului evaluării, imprevizibilitatea și impactul potențial asupra asigurării pot face ca aceasta să fie o modificare majoră în cazul în care compromite asigurările securității oferite de certificare.

(6) Evoluțiile amenințărilor din mediul unui produs TIC certificat nemodificat ar putea necesita o reevaluare. Ar trebui să fie clar stabilite rezultatele posibile ale unui astfel de proces de reevaluare, în special impactul său asupra certificatului EUCC. În cazul în care o reevaluare este finalizată cu succes, organismul de certificare ar trebui să confirme certificatul sau să elibereze un nou certificat cu o dată de expirare prelungită. În cazul în care un proces de reevaluare nu este finalizat cu succes, organismul de certificare ar trebui să retragă certificatul și, eventual, să elibereze un nou certificat cu un domeniu diferit de aplicare. Aceste dispoziții ar trebui să se aplice *mutatis mutandis* reevaluării profilurilor de protecție.

(7) Anexa I la Regulamentul de punere în aplicare (UE) 2024/482 enumeră documentele aplicabile ce reflectă stadiul actual al tehnologiei pentru evaluarea produselor TIC și a profilurilor de protecție. Aceste documente ce reflectă stadiul actual al tehnologiei ar trebui actualizate pentru a reflecta cele mai recente evoluții, cum ar fi cele legate de evoluțiile tehnologice, de peisajul amenințărilor cibernetice, de practicile industriale sau de standardele internaționale. O astfel de actualizare este oportună pentru documentele ce reflectă stadiul actual al tehnologiei referitoare la cerințele minime de securitate a site-ului, aplicarea potențialelor de atac la cardurile inteligente, aplicarea potențialelor de atac asupra dispozitivelor hardware cu casete de securitate, aplicarea unor criterii comune pentru circuitele integrate și evaluarea produselor compozite pentru cardurile inteligente și dispozitivele similare. În plus, nu sunt incluse documentele ce reflectă stadiul actual al tehnologiei referitoare la evaluarea și certificarea produselor compozite care utilizează cea mai recentă versiune a standardelor bazate pe criteriile comune, reutilizarea rezultatelor evaluării auditurilor la fața locului și clarificări cu privire la interpretarea profilurilor de protecție referitoare la dispozitivele de creare a semnăturilor electronice calificate, tahografe și modulele de securitate hardware. Pentru a asigura o evaluare uniformă a produselor TIC în cadrul EUCC, anexa I ar trebui modificată pentru a include aceste noi documente ce reflectă stadiul actual al tehnologiei, în urma aprobării lor de către Grupul european pentru certificarea securității cibernetice (ECCG).

(8) În plus, documentul ce reflectă stadiul actual al tehnologiei intitulat „ADV_SPM.1 interpretation for CC:2022 transition” ar trebui adăugat la sistem pentru a se asigura că procesele de certificare care se bazează pe profiluri de protecție specifice pot continua să utilizeze modelarea formală (ADV_SPM.1) până la actualizarea profilurilor de protecție corespunzătoare, de exemplu prin adăugarea unei configurații conforme a profilului de protecție multiasigurare CC: 2022 care sprijină ADV_SPM.1. Pentru a oferi pieței suficient timp pentru a trece la standardele actualizate bazate pe criteriile comune, trebuie prevăzute norme de tranziție specifice pentru profilurile de protecție Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, sau Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020. Pentru a evita orice perturbare a pieței, este oportun să se stabilească faptul că documentul ce reflectă stadiul actual al tehnologiei privind interpretarea „ADV_SPM.1 interpretation for CC: 2022 transition” se aplică proceselor de certificare care au fost inițiate înainte de adoptarea prezentului regulament. Cu toate acestea, aplicarea acestui document ar trebui să fie strict limitată la ceea ce este necesar, având în vedere timpul necesar pentru finalizarea actualizării profilurilor de protecție corespunzătoare. Mai precis, pentru procesele de certificare care utilizează profilurile de protecție Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, sau Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, documentul ce reflectă stadiul actual al tehnologiei ar trebui să se aplice proceselor care au fost inițiate înainte de 1 octombrie 2026. Pentru procesele de certificare care utilizează profilul de protecție Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, documentul ce reflectă stadiul actual al tehnologiei ar trebui să se aplice numai proceselor inițiate înainte de data intrării în vigoare a prezentului regulament, având în vedere că este deja disponibilă o nouă versiune a profilului de protecție Java Card System – Open Configuration.

(9) O modificare a documentelor ce reflectă stadiul actual al tehnologiei în cursul unui proces de certificare ar putea perturba evaluarea produsului și ar putea întârzia eliberarea certificatului. Prin urmare, sunt necesare norme de tranziție adecvate pentru documentele noi sau actualizate ce reflectă stadiul actual al tehnologiei, pentru a permite vânzătorilor, ITSEF, organismelor de certificare și altor părți interesate să efectueze ajustările necesare. Documentele noi și actualizate ce reflectă stadiul actual al tehnologiei aplicabile ar trebui să vizeze cererile de certificare, inclusiv cererile de reevaluare și reevaluare, în timp ce procesele de certificare în curs ar trebui să poată utiliza în continuare versiuni anterioare ale documentelor ce reflectă stadiul actual al tehnologiei.

(10) Anexele II și III la Regulamentul de punere în aplicare (UE) 2024/482 enumeră profilurile de protecție certificate la nivelul AVA_VAN 4 sau 5 și, respectiv, profilurile de protecție recomandate. Mai multe referințe sunt incomplete sau caduce, din cauza unei actualizări a profilurilor de protecție. Aceste referințe ar trebui completate și, în plus, ar trebui incluse noi referințe pentru a asigura o acoperire mai cuprinzătoare a circuitelor integrate securizate, a cardurilor inteligente și a dispozitivelor conexe, precum și a sistemelor informatice de încredere.

(11) Este necesar să se aducă modificări articolului 19 din Regulamentul de punere în aplicare (UE) 2024/482 pentru a clarifica faptul că anexa IV se aplică, cu modificările necesare, revizuirii certificatelor EUCC pentru profilurile de protecție.

(12) Având în vedere că obiectivul de securitate este un element-cheie pentru înțelegerea domeniului de aplicare al unui proces de certificare, este, de asemenea, necesar ca ENISA să publice obiectivul de securitate corespunzător fiecărui certificat EUCC pe site-ul său web.

(13) În plus, organismele de certificare ar trebui să furnizeze ENISA o versiune în limba engleză a obiectivului de securitate și a raportului de certificare pentru a permite agenției să pună la dispoziție informațiile respective în limba engleză pe site-ul corespunzător, în temeiul articolului 42 alineatul (2) din Regulamentul de punere în aplicare (UE) 2024/482. Din acest motiv, solicitanții de certificare ar trebui să furnizeze organismelor de certificare o versiune în limba engleză a obiectivului de securitate, ori de câte ori li se solicită acest lucru.

(14) Nu este necesar ca trimiterea la denumirea organismului de certificare să apară în identificarea unică a certificatului, deoarece numărul de identificare al organismului de certificare este suficient pentru a identifica acest organism într-un mod unic. Nici luna eliberării nu trebuie să apară, deoarece numărarea certificatelor se face anual. Prin urmare, această cerință ar trebui eliminată, din motive de simplificare. Întrucât anul eliberării certificatului corespunde eliberării primului certificat, aceeași dată ar trebui să figureze în identificarea unică de pe certificatele eliberate după o revizuire, pentru a se asigura trasabilitatea.

(15) Prin urmare, Regulamentul de punere în aplicare (UE) 2024/482 trebuie modificat în consecință.

(16) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit în temeiul articolului 66 din Regulamentul (UE) 2019/881,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Regulamentul de punere în aplicare (UE) 2024/482 se modifică după cum urmează:

1. la articolul 2, se adaugă următoarele puncte 16, 17 și 18:

„16. «serie de produse» înseamnă un set de produse TIC ale unui solicitant, construit pe aceeași bază funcțională pentru a răspunde acelorași nevoi în materie de securitate, având un proiect, un hardware, un firmware sau un software care poate varia de la un produs TIC la altul;

17. «modificare minoră» înseamnă orice modificare a obiectivului certificat de evaluare sau a mediului său care nu are un impact negativ asupra asigurării exprimate în certificatul EUCC;

18. «modificare majoră» înseamnă orice modificare a obiectivului certificat de evaluare sau a mediului său care poate avea un impact negativ asupra asigurării exprimate în certificatul EUCC.”;

2. la articolul 5, se adaugă următorul alineat (3):

„(3) Un organism de certificare poate permite certificarea unei serii de produse.”;

3. la articolul 9 alineatul (2), litera (a) se înlocuiește cu următorul text:

„(a) să furnizeze organismului de certificare și unității ITSEF toate informațiile necesare, complete și corecte și să furnizeze informații suplimentare necesare, la cerere, inclusiv o versiune în limba engleză a obiectivului de securitate;”;

4. la articolul 11 alineatul (3), litera (b) se înlocuiește cu următorul text:

„(b) identificarea unică a certificatului, constând în:

1. denumirea sistemului;
2. numărul de identificare, în conformitate cu articolul 3 din Regulamentul de punere în aplicare (UE) 2024/3143, al organismului de certificare care a eliberat certificatul;
3. anul eliberării certificatului inițial;
4. numărul de identificare atribuit de organismul de certificare care a eliberat certificatul.";

5. la articolul 19, alineatul (1) se înlocuiește cu următorul text:

„(1) La cererea titularului certificatului sau din alte motive justificate, organismul de certificare poate decide să revizuiască un certificat EUCC pentru un profil de protecție. Revizuirea se efectuează în conformitate cu anexa IV. Organismul de certificare stabilește amploarea revizuirii. În cazul în care acest lucru este necesar pentru revizuire, organismul de certificare solicită unității ITSEF să efectueze o reevaluare a profilului de protecție certificat.";

6. articolul 42 se modifică după cum urmează:

(a) la alineatul (1) se adaugă următoarea literă (i):

„(i) obiectivul de securitate corespunzător fiecărui certificat EUCC;";

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) Informațiile menționate la alineatul (1) trebuie să fie puse la dispoziție cel puțin în limba engleză. În acest scop, organismele de certificare furnizează ENISA versiunile în limba originală ale rapoartelor de certificare și ale obiectivelor de securitate și, în plus, furnizează, de asemenea, versiunea în limba engleză a acestor documente, fără întârzieri nejustificate.";

7. la articolul 48, alineatul (4) se înlocuiește cu următorul text:

„(4) Cu excepția cazului în care se prevede altfel în anexa I sau II, documentele ce reflectă stadiul actual al tehnologiei se aplică proceselor de certificare, inclusiv reevaluării, lansate de la data aplicării actului de modificare prin care au fost încorporate documentele ce reflectă stadiul actual al tehnologiei în anexa I sau II.";

8. anexa I se înlocuiește cu textul anexei I la prezentul regulament;

9. anexa II se înlocuiește cu textul anexei II la prezentul regulament;

10. anexa III se înlocuiește cu textul anexei III la prezentul regulament;

11. anexa IV se modifică în conformitate cu anexa IV la prezentul regulament;

12. anexa V se modifică în conformitate cu anexa V la prezentul regulament;

13. anexa IX se înlocuiește cu textul din anexa VI la prezentul regulament.

Articolul 2

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

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

Adoptat la Bruxelles, 8 decembrie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

„ANEXA I

Documente ce reflectă stadiul actual al tehnologiei și sprijină domeniile tehnice și alte documente ce reflectă stadiul actual al tehnologiei

1. Documente ce reflectă stadiul actual al tehnologiei și sprijină domeniile tehnice la nivelul 4 sau 5 al AVA_VAN:

   (a) următoarele documente referitoare la evaluarea armonizată a domeniului tehnic «carduri inteligente și dispozitive similare»:

      1. «Minimum ITSEF requirements for security evaluations of smart cards and similar devices», versiunea 1.1;
      2. «Minimum Site Security Requirements», versiunea 2;
      3. «Reusing evaluation results of site audits (STAR)», versiunea 1;
      4. «Application of Common Criteria to integrated circuits», versiunea 2;
      5. «Security Architecture requirements (ADV_ARC) for smart cards and similar devices», versiunea 1.1;
      6. «Certification of 'open' smart card products», versiunea 1.1;
      7. «Composite product evaluation for smart cards and similar devices for CC3.1», versiunea 2;
      8. «Composite product evaluation and certification for CC:2022», versiunea 1;
      9. «Application of Attack Potential to Smartcards and Similar Devices», versiunea 2;
      10. «Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices», versiunea 1;
      11. «ADV_SPM.1 interpretation for CC:2022 transition», versiunea 1.1, aplicabilă proceselor de certificare care utilizează profiluri de protecție după cum urmează:

         (a) profiluri de protecție Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014 sau Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, inițiate înainte de 1 octombrie 2026;

         (b) profilul de protecție Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, inițiat înainte de 29 decembrie 2025;

   (b) următoarele documente referitoare la evaluarea armonizată a domeniului tehnic «dispozitive hardware cu casete de securitate»:

      1. «Minimum ITSEF requirements for security evaluations of hardware devices with security boxes», versiunea 1.1;
      2. «Minimum Site Security Requirements», versiunea 2;
      3. «Reusing evaluation results of site audits (STAR)», versiunea 1;
      4. «Application of Attack Potential to hardware devices with security boxes», versiunea 2;
      5. «Hardware assessment in EN 419221-5 (HSM PP)», versiunea 1;
      6. «JIL Tachograph MS PP Clarification», versiunea 1.

2. Documente ce reflectă stadiul actual al tehnologiei referitoare la acreditarea armonizată a organismelor de evaluare a conformității:

   (a) «Accreditation of ITSEFs for the EUCC», versiunea 1.1, pentru acreditările emise înainte de 8 iulie 2025;

   (b) «Accreditation of ITSEFs for the EUCC», versiunea 1.6c, pentru acreditările nou emise sau revizuite după 8 iulie 2025;

   (c) «Accreditation of CBs for the EUCC», versiunea 1.6b."

ANEXA II

„ANEXA II

Profiluri de protecție certificate la nivelul AVA_VAN 4 sau 5

1. Pentru dispozitivele calificate de creare a semnăturii și a sigiliului la distanță:

   (a) EN 419241-2: 2019 – Sisteme fiabile de susținere a semnăturii prin server – Partea 2: profilul de protecție pentru QSCD pentru semnătura prin server (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 – Profiluri de protecție pentru modulele criptografice ale prestatorilor de servicii de încredere – Partea 5: modulul criptografic pentru serviciile de încredere (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Profilurile de protecție care au fost adoptate ca documente ce reflectă stadiul actual al tehnologiei:

   [NECOMPLETAT]."

ANEXA III

„ANEXA III

Profiluri de protecție recomandate

Profiluri de protecție utilizate în certificarea produselor TIC, inclusiv a produselor din domeniile tehnice:

1. Carduri inteligente și dispozitive similare

   (a) pașaport:

      1. PP Machine Readable Travel Document with «ICAO Application» Basic Access Control (v1.10), BSI-CC-PP-0055-2009;

      2. PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3. PP Machine Readable Travel Document with «ICAO Application» Extended Access Control with PACE (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   (b) dispozitive securizate de creare a semnăturii (SSCD):

      1. EN 419211-2:2013 – Profiluri de protecție pentru dispozitive securizate de creare a semnăturii – Partea 2: dispozitiv cu generare de cheie (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2. EN 419211-3:2013 – Profiluri de protecție pentru dispozitive securizate de creare a semnăturii – Partea 3: dispozitiv cu import de cheie (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3. EN 419211-4:2013 – Profiluri de protecție pentru dispozitive securizate de creare a semnăturii – Partea 4: extensie pentru dispozitive cu generare de cheie și comunicație securizată cu aplicația de generare de certificate (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4. EN 419211-5:2013 – Profiluri de protecție pentru dispozitive securizate de creare a semnăturii – Partea 5: extensie pentru dispozitive cu generare de cheie și comunicație securizată cu aplicația de creare a semnăturii (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5. EN 419211-6:2014 – Profiluri de protecție pentru dispozitive securizate de creare a semnăturii – Partea 6: extensie pentru dispozitive cu import de cheie și comunicație securizată cu aplicația de creare a semnăturii (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   (c) tahograf: Digital Tachograph – Tachograph Card (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   (d) CI securizat, platforma Java Card și eUICC:

      1. Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic and SCWS);

      2. Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014;

      3. Embedded UICC (eUICC) for Machine-to-Machine Devices (v1.1), BSI-CC-PP-0089-2015;

      4. Cryptographic Service Provider – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5. Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019;

      6. Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) Version 0.9.4, BSI-CC-PP-0108-2019;

      7. Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020;

      8. Secure Element Protection Profile – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9. Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (v1.8), BSI-CC-PP-0117-V2-2023;

      10. Java Card System – Open Configuration (v3.2), BSI-CC-PP-0099-V3-2024;

      11. Embedded UICC for Consumer Devices Protection Profile (v2.1), BSI-CC-PP-0100-V2-2025;

   (e) Trusted Platform Module: Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Dispozitive hardware cu casete de securitate

(a) puncte de interacțiune (de plată) și terminale de plăți (POI):

1. Punctul de interacțiune «POI-CHIP-ONLY» (v4.0), ANSSI-CC-PP-2015/01;
2. Punctul de interacțiune «POI-CHIP-ONLY and Open Protocol Package» (v4.0), ANSSI-CC-PP-2015/02;
3. Punctul de interacțiune «POI-COMPREHENSIVE» (v4.0), ANSSI-CC-PP-2015/03;
4. Punctul de interacțiune «POI-COMPREHENSIVE and Open Protocol Package» (v4.0), ANSSI-CC-PP-2015/04;
5. Punctul de interacțiune «POI-PED-ONLY» (v4.0), ANSSI-CC-PP-2015/05;
6. Punctul de interacțiune «POI-PED-ONLY and Open Protocol Package» (v4.0), ANSSI-CC-PP-2015/06;

(b) modulul de securitate hardware:

1. Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;
2. Cryptographic Module for CSP Key Generation Services – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;
3. Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

(c) tahograf:

1. Digital Tachograph – Motion Sensor (MS PP) (v1.0), BSI-CC-PP-0093-2017;
2. Digital Tachograph – Vehicle Unit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;
3. Digital Tachograph – External GNSS Facility (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021.

3. Altele: Trusted Execution Environment Protection Profile – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”

ANEXA IV

Anexa IV la Regulamentul de punere în aplicare (UE) 2024/482 se modifică după cum urmează:

1. la punctul IV.2, subpunctul 4 se înlocuiește cu următorul text:

„4. Organismul de certificare examinează raportul tehnic de evaluare actualizat și întocmește un raport de reevaluare. Statutul certificatului inițial se modifică apoi în conformitate cu articolul 13 sau cu articolul 19. În cazul în care procesul de reevaluare este realizat cu succes, articolul 13 alineatul (2) literele (a) sau (c) se aplică în cazul certificării unui produs, iar articolul 19 alineatul (2) litera (a) sau (c) se aplică în cazul certificării unui profil de protecție. În cazul în care procesul de reevaluare nu este realizat cu succes, articolul 13 alineatul (2) literele (b) sau (d) se aplică în cazul certificării unui produs, iar articolul 19 alineatul (2) litera (b) sau (d) se aplică în cazul certificării unui profil de protecție.";

2. punctul IV.3 se modifică după cum urmează:

(a) titlul IV.3 se înlocuiește cu următorul text:

„IV.3 **Modificări ale unui produs TIC certificat – întreținere și reevaluare**";

(b) punctele 4 și 5 se înlocuiesc cu următorul text:

„4. În urma examinării, organismul de certificare stabilește amploarea unei modificări ca fiind minoră sau majoră, în funcție de impactul acesteia asupra asigurării prevăzute în certificatul EUCC.

5. În cazul în care modificările au fost confirmate de organismul de certificare ca fiind minore, nu se eliberează niciun nou certificat pentru produsul TIC modificat în conformitate cu articolul 13 alineatul (2) litera (a) sau cu articolul 19 alineatul (2) litera (a) și se întocmește un raport de menținere a raportului de certificare inițial.";

(c) se inserează următorul punct 5a:

„5a. În cazul oricăror modificări ale măsurilor de asigurare în mediul de dezvoltare, inclusiv adăugarea unor cerințe de asigurare ale familiei CC ALC_FLR (remedierea deficiențelor), organismul de certificare poate solicita ITSEF să efectueze o evaluare a unui subansamblu al măsurilor de asigurare afectate. ITSEF emite un raport tehnic de evaluare parțială, pe baza căruia organismul de certificare confirmă că modificările sunt minore sau majore. În cazul în care modificările au fost confirmate de organismul de certificare ca fiind minore, se aplică anexa IV.3 punctul 5. În cazul în care modificările au fost confirmate de organismul de certificare ca fiind majore, se aplică anexa IV.3 punctul 7."

ANEXA V

Punctul V.1 din anexa V la Regulamentul de punere în aplicare (UE) 2024/482 se înlocuiește cu următorul text:

„V.1 **Raportul de certificare**

1. Pe baza rapoartelor tehnice de evaluare furnizate de ITSEF, organismul de certificare întocmește un raport de certificare care urmează să fie publicat împreună cu certificatul EUCC și cu obiectivul de securitate aferente.

2. Raportul de certificare este sursa de informații detaliate și practice cu privire la produsul TIC și la implementarea în condiții de siguranță a produsului TIC. Prin urmare, acesta include toate informațiile care sunt publice și pot fi comunicate relevante pentru utilizatori și părțile interesate. Informațiile care sunt publice și pot fi comunicate pot fi menționate în raportul de certificare.

3. Raportul de certificare conține cel puțin următoarele informații:
   (a) rezumatul;
   (b) identificarea produsului TIC;
   (c) datele de contact referitoare la evaluarea produsului TIC;
   (d) politici de securitate;
   (e) ipotezele și clarificarea sferei de aplicare;
   (f) informații privind arhitectura informatică;
   (g) informații suplimentare în materie de securitate cibernetică, dacă este cazul;
   (h) rezumatul evaluării produselor TIC și configurația evaluată;
   (i) rezultatele evaluării și informații privind certificatul;
   (j) observații și recomandări, dacă este cazul;
   (k) anexe, dacă este cazul;
   (l) o trimitere la obiectivul de securitate al produsului TIC supus certificării;
   (m) atunci când este disponibilă, marca sau eticheta asociată sistemului;
   (n) glosarul, dacă este cazul;
   (o) bibliografia.

4. Rezumatul menționat la punctul 3 litera (a) este un rezumat succint al întregului raport de certificare. Acesta oferă o imagine de ansamblu clară și concisă a rezultatelor evaluării și include următoarele informații:
   (a) denumirea produsului TIC evaluat;
   (b) denumirea ITSEF care a efectuat evaluarea;
   (c) data finalizării evaluării;
   (d) data eliberării certificatului;
   (e) dacă este cazul, data eliberării certificatului inițial;
   (f) perioada de valabilitate;
   (g) identificarea unică a certificatului, astfel cum se descrie la articolul 11;
   (h) scurtă descriere a rezultatelor raportului de certificare, inclusiv:
      (i) versiunea și, dacă este cazul, ediția criteriilor comune aplicate evaluării;
      (ii) pachetul aferent asigurării sau lista componentelor asigurării securității din criteriile comune, inclusiv nivelul AVA_VAN aplicat în timpul evaluării și nivelul de asigurare corespunzător, astfel cum se prevede la articolul 52 din Regulamentul (UE) 2019/881, la care se referă certificatul EUCC;
      (iii) după caz, profilul (profilurile) de protecție cu care produsul TIC declară conformitatea;
      (iv) trimiterea la politica de securitate a produsului TIC evaluat;
      (v) declarație (declarații) de declinare a responsabilității, dacă este cazul.

5. Identificarea menționată la punctul 3 litera (b) identifică în mod clar produsul TIC evaluat și conține inclusiv următoarele informații:

   (a) identificatorul unic al produsului TIC evaluat;

   (b) enumerarea componentelor produsului TIC care fac parte din evaluare cu numărul versiunii fiecărei componente;

   (c) trimiterea la cerințele suplimentare pentru mediul operarațional al produsului TIC certificat;

6. Datele de contact menționate la punctul 3 litera (c) includ cel puțin următoarele informații:

   (a) denumirea dezvoltatorului;

   (b) denumirea și datele de contact ale titularului certificatului EUCC;

   (c) denumirea organismului de certificare care a eliberat certificatul;

   (d) autoritatea națională competentă de certificare a securității cibernetice;

   (e) denumirea unității ITSEF care a efectuat evaluarea și, după caz, lista subcontractanților;

7. Secțiunea privind politica de securitate menționată la punctul 3 litera (d) conține descrierea politicii de securitate a produsului TIC ca ansamblu de servicii de securitate și a politicilor sau normelor pe care produsul TIC evaluat trebuie să le aplice sau să le respecte. Aceasta trebuie să conțină următoarele informații:

   (a) o descriere a procedurilor de gestionare a vulnerabilităților și de divulgare a vulnerabilităților ale titularului certificatului, care trebuie completată exclusiv cu informații care pot fi făcute publice;

   (b) politica de continuitate a asigurării a titularului certificatului, inclusiv, după caz, descrierea proceselor de gestionare a ciclului de viață sau de producție ale titularului certificatului, în conformitate cu secțiunea IV.1 din anexa IV;

   (c) dacă este cazul, prezența procedurii de gestionare a corecțiilor și rezultatul evaluării sale în conformitate cu secțiunea IV.4 din anexa IV.

8. Ipotezele și clarificarea domeniului de aplicare menționate la punctul 3 litera (e) conțin informații privind circumstanțele și obiectivele legate de utilizarea preconizată a produsului, astfel cum se menționează la articolul 7 alineatul (1) litera (c), și includ următoarele:

   (a) ipoteze privind utilizarea și implementarea produsului TIC sub forma unor cerințe minime, cum ar fi cerințele de instalare și configurare corespunzătoare și cerințele de hardware care sunt îndeplinite;

   (b) ipoteze privind mediul necesar pentru funcționarea conformă a produsului TIC;

   (c) descrierea oricăror amenințări la adresa produsului TIC care nu sunt contracarate de funcțiile de securitate evaluate ale produsului în funcție de utilizarea preconizată, dacă se consideră că sunt relevante pentru un potențial utilizator al produsului TIC.

   Informațiile menționate la primul paragraf trebuie să fie cât mai clare și mai ușor de înțeles pentru, a permite potențialilor utilizatori ai produsului TIC certificat să ia decizii în cunoștință de cauză cu privire la riscurile asociate utilizării acestuia.

9. Informațiile arhitecturale menționate la punctul 3 litera (f) includ o descriere de nivel înalt a produsului TIC și a principalelor sale componente, pe baza rezultatelor definite în familia de asigurare a criteriilor comune: Development – TOE Design (ADV_TDS).

10. Informațiile suplimentare privind securitatea cibernetică menționate la punctul 3 litera (g) includ linkul către site-ul web al titularului certificatului EUCC menționat la articolul 55 din Regulamentul (UE) 2019/881.

11. Evaluarea și configurația produselor TIC menționate la punctul 3 litera (h) descriu efortul de testare atât al dezvoltatorului, cât și al evaluatorului, subliniind abordarea, configurația și amploarea testării. Acestea includ cel puțin următoarele informații:

    (a) o identificare a componentelor de asigurare utilizate în standardele menționate la articolul 3;

    (b) versiunea documentelor ce reflectă stadiul actual al tehnologiei și criteriile suplimentare de evaluare a securității utilizate în evaluare;

    (c) setările și configurația obiectivului de evaluare utilizat pentru testare și analiza vulnerabilității;

    (d) orice profil de protecție care a fost utilizat, inclusiv următoarele informații: denumirea, versiunea, data și certificatul profilului de protecție.

12. Rezultatele evaluării și informațiile privind certificatul menționat la punctul 3 litera (i) includ informații privind nivelul de asigurare atins, astfel cum se menționează la articolul 4 din prezentul regulament și la articolul 52 din Regulamentul (UE) 2019/881.

13. Observațiile și recomandările menționate la punctul 3 litera (j) sunt utilizate pentru a furniza informații suplimentare cu privire la rezultatele evaluării. Aceste observații și recomandări pot consta în deficiențe ale produsului TIC descoperite în timpul evaluării sau în mențiuni ale unor caracteristici deosebit de utile.

14. Anexele menționate la punctul 3 litera (k) sunt utilizate pentru a evidenția orice informații suplimentare care ar putea fi utile publicului raportului, dar care nu se încadrează din punct de vedere logic în secțiunile prevăzute ale raportului, inclusiv în cazul unei descrieri complete a politicii de securitate.

15. Obiectivul de securitate menționat la punctul 3 litera (l) menționează obiectivul de securitate evaluat. Obiectivul de securitate evaluat este însoțit de raportul de certificare în scopul publicării pe site-ul web menționat la articolul 50 alineatul (1) din Regulamentul (UE) 2019/881. În cazul în care este necesară sanitizarea obiectivului de securitate evaluat înainte de publicare, aceasta se realizează în conformitate cu punctul V.2 din anexa V la prezentul regulament.

16. Mărcile sau etichetele asociate sistemului EUCC menționate la punctul 3 litera (m) se încorporează în raportul de certificare în conformitate cu normele și procedurile prevăzute la articolul 11.

17. Glosarul menționat la punctul 3 litera (n) este utilizat pentru a spori lizibilitatea raportului prin furnizarea unor definiții ale acronimelor sau termenilor ale căror semnificații ar putea să nu fie ușor vizibile.

18. Secțiunea bibliografică menționată la punctul 3 litera (o) include trimiteri la toate documentele utilizate pentru întocmirea raportului de certificare. Informațiile respective includ cel puțin următoarele:

    (a) criteriile de evaluare a securității, documentele ce reflectă stadiul actual al tehnologiei și specificațiile relevante suplimentare utilizate;

    (b) raportul tehnic de evaluare;

    (c) raportul tehnic de evaluare pentru evaluarea compozită, dacă este cazul;

    (d) documentația tehnică de referință;

    (e) orientări în materie de securitate ale dezvoltatorului;

    (f) lista de configurație pentru dezvoltatori.

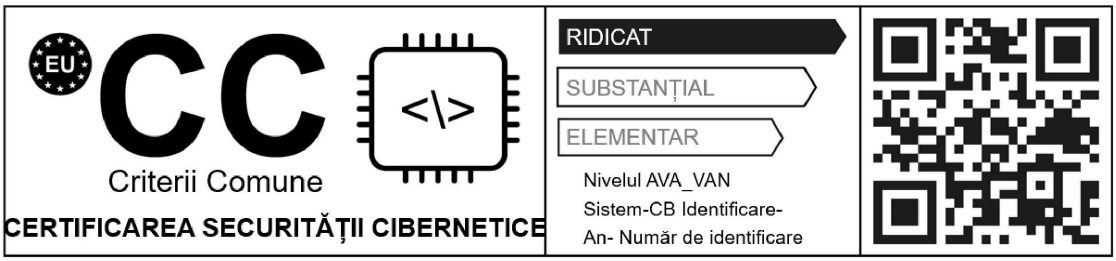
    Pentru a garanta reproductibilitatea evaluării, toate documentele la care se face referire trebuie să fie identificate în mod unic cu ajutorul datei exacte a publicării și al numărului exact al versiunii.”

ANEXA VI

„ANEXA IX

Marca și eticheta

1. Forma mărcii și a etichetei:



2. În caz de micșorare sau de mărire a mărcii și a etichetei, trebuie respectate proporțiile menționate la punctul 1.

3. În cazul în care sunt prezente fizic, marca și eticheta trebuie să aibă o înălțime de cel puțin 5 mm.”