Úradný vestník
Európskej únie

SK
Séria L

2025/2462

9.12.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/2462

z 8. decembra 2025,

ktorým sa mení vykonávacie nariadenie (EÚ) 2024/482, pokiaľ ide o vymedzenie pojmov, certifikáciu sérií produktov IKT, zachovanie záruky a dokumenty na základe aktuálneho stavu

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) ([1]), a najmä na jeho článok 49 ods. 7,

keďže:

(1) Vo vykonávacom nariadení Komisie (EÚ) 2024/482 ([2]) sa v súlade s európskym rámcom certifikácie kybernetickej bezpečnosti stanoveným v nariadení (EÚ) 2019/881 špecifikujú úlohy, pravidlá a povinnosti, ako aj štruktúra európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (ďalej len „EUCC“).

(2) Spoločná metodika hodnotenia, ktorá je pripojená k spoločným kritériám (CC), je medzinárodná norma pre hodnotenie informačnej bezpečnosti a umožňuje hodnotenie bezpečnosti produktov IKT na účely certifikácie. V tejto súvislosti môžu niektoré produkty IKT stavať na rovnakom funkčnom základe s cieľom ponúkať podobné bezpečnostné funkcie na rôznych platformách alebo zariadeniach, čo sa označuje aj ako produktová séria. Návrh, hardvér, firmvér alebo softvér sa však môžu produkt od produktu IKT líšiť. Je však na certifikačnom orgáne, aby v jednotlivých prípadoch rozhodol, či sa môže vykonať certifikácia produktovej série. Podmienky certifikácie produktových sérií by sa mohli bližšie ilustrovať na podporu usmernení EUCC.

(3) S cieľom zachovať spoľahlivosť certifikovaných produktov je nevyhnutné určiť, čo predstavuje závažnú a menej závažnú zmenu objektu hodnotenia alebo jeho prostredia vrátane jeho prevádzkového alebo vývojového prostredia. Preto je potrebné špecifikovať tieto pojmy vzhľadom na existujúce a široko používané technické špecifikácie skupiny vysokých úradníkov pre bezpečnosť informačných systémov (SOG-IS) a účastníkov Dohody o uznávaní certifikátov spoločných kritérií v oblasti informačnej bezpečnosti (CCRA).

(4) Menej závažné zmeny sa často vyznačujú obmedzeným vplyvom na vyhlásenie o záruke bezpečnosti produktu, ktoré poskytuje vydaný certifikát EUCC. Menej závažné zmeny by preto mali byť upravené v postupoch údržby a nevyžadujú si prehodnotenie bezpečnostných funkcií produktu. Medzi príklady menej závažných zmien, ktoré by sa mali riešiť prostredníctvom údržby, patria okrem iného redakčné zmeny, zmeny objektu hodnotiaceho prostredia, ktorými sa nemení certifikovaný objekt hodnotenia, a zmeny certifikovaného objektu hodnotenia, ktoré nemajú vplyv na dôkazy o záruke. Aj zmeny vývojového prostredia možno považovať za menej závažné za predpokladu, že nemajú žiadny následný vplyv na existujúce opatrenia záruky. V niektorých prípadoch si však môžu vyžadovať čiastočné hodnotenie príslušných opatrení.

([1]) Ú. v. EÚ L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Závažná zmena je akákoľvek zmena certifikovaného objektu hodnotenia alebo jeho prostredia, ktorá môže mať nepriaznivý vplyv na záruku vyjadrenú v certifikáte EUCC, a preto by si mala vyžadovať prehodnotenie. Medzi príklady závažných zmien patria okrem iného zmeny súboru požiadaviek na deklarovanú záruku, s výnimkou požiadaviek na záruku skupiny CC ALC_FLR (náprava chyby); zmeny v kontrolách dôvernosti alebo integrity vývojového prostredia, ak by takéto úpravy mohli ovplyvniť bezpečný vývoj alebo výrobu objektu hodnotenia alebo zmeny objektu hodnotenia s cieľom vyriešiť zneužiteľnú zraniteľnosť. Okrem toho možno za závažnú zmenu považovať aj súbor menej závažných zmien, ktoré majú spoločne významný vplyv na bezpečnosť. Je tiež dôležité uznať, že hoci oprava chyby môže ovplyvniť len konkrétny aspekt objektu hodnotenia, jej nepredvídateľnosť a potenciálny vplyv na záruku môžu spôsobiť, že sa stane závažnou zmenou, ak sa tým ohrozia bezpečnostné záruky poskytnuté certifikáciou.

(6) Zmeny v prostredí hrozieb nezmeneného certifikovaného produktu IKT by si mohli vyžadovať opätovné posúdenie. Mali by sa jasne stanoviť možné výsledky takéhoto procesu opätovného posúdenia, najmä jeho vplyv na certifikát EUCC. Ak sa opätovné posúdenie úspešne dokončí, certifikačný orgán by mal certifikát potvrdiť alebo vydať nový certifikát s predĺženým dátumom uplynutia platnosti. Ak proces opätovného posúdenia nie je úspešný, certifikačný orgán by mal certifikát odňať a prípadne vydať nový certifikát s odlišným rozsahom pôsobnosti. Takéto ustanovenia by sa mali uplatňovať *mutatis mutandis* na opätovné posúdenie profilov ochrany.

(7) V prílohe I k vykonávaciemu nariadeniu (EÚ) 2024/482 sa uvádzajú uplatniteľné dokumenty na základe aktuálneho stavu na hodnotenie produktov IKT a profilov ochrany. Tieto dokumenty na základe aktuálneho stavu by sa mali aktualizovať tak, aby odrážali najnovší vývoj, napríklad technologický vývoj, vývoj prostredia kybernetických hrozieb, priemyselných postupov alebo medzinárodných noriem. Takáto aktualizácia je vhodná pre dokumenty na základe aktuálneho stavu týkajúce sa minimálnych požiadaviek na bezpečnosť lokality, použitia potenciálu útoku na inteligentné karty, použitia potenciálu útoku na hardvérové zariadenia s bezpečnostnými skrinkami, uplatňovania spoločných kritérií na integrované obvody a hodnotenia zložených produktov pre inteligentné karty a podobné zariadenia. Okrem toho nie sú zahrnuté dokumenty na základe aktuálneho stavu týkajúce sa hodnotenia a certifikácie zložených produktov s použitím najnovšej verzie noriem spoločných kritérií, opätovné použitie výsledkov hodnotenia auditov na mieste a objasnenia týkajúce sa výkladu profilov ochrany týkajúcich sa zariadení na vyhotovenie kvalifikovaného elektronického podpisu, tachografov a hardvérových bezpečnostných modulov. S cieľom zabezpečiť jednotné hodnotenie produktov IKT v rámci EUCC by sa príloha I mala zmeniť tak, aby zahŕňala tieto aktualizované a nové dokumenty na základe aktuálneho stavu po ich schválení európskou skupinou pre certifikáciu kybernetickej bezpečnosti (ECCG).

(8) Okrem toho by sa do schémy mal doplniť dokument na základe aktuálneho stavu *ADV_SPM.1 interpretation for CC:2022 transition* (Výklad ADV_SPM.1 pre prechod CC:2022) s cieľom zabezpečiť, aby procesy certifikácie využívajúce špecifické profily ochrany mohli pokračovať v používaní formálneho modelovania (ADV_SPM.1), kým sa neaktualizujú zodpovedajúce profily ochrany, napríklad pridaním konfigurácie profilu ochrany s viacerými zárukami v súlade s CC:2022, ktorá podporuje ADV_SPM.1. S cieľom poskytnúť trhu dostatočný čas na prechod na aktualizované normy spoločných kritérií je potrebné stanoviť osobitné prechodné pravidlá pre profily ochrany *Security IC Platform PP with Augmentation Packages (v1.0)* [Profil ochrany pre platformu bezpečnostného integrovaného obvodu s rozširujúcimi balíkmi (v1.0)], BSI-CC-PP-0084-2014, *Java Card System – Closed Configuration (v3.1)* [Systém Java Card – uzavretá konfigurácia (v3.1)], BSI-CC-PP-0101-V2-2020, alebo *Java Card System – Open Configuration (v3.1)* [Systém Java Card – otvorená konfigurácia (v3.1)], BSI-CC-PP-0099-V2-2020. S cieľom zabrániť akýmkoľvek narušeniam trhu je vhodné stanoviť, že na procesy certifikácie, ktoré sa začali pred prijatím tohto nariadenia, sa vzťahuje dokument na základe aktuálneho stavu *ADV_SPM.1 interpretation for CC:2022 transition* (Výklad ADV_SPM.1 pre prechod CC:2022) Uplatňovanie tohto dokumentu by sa však malo prísne obmedziť na to, čo je nevyhnutné, vzhľadom na čas potrebný na dokončenie aktualizácie zodpovedajúcich profilov ochrany. Presnejšie v prípade procesov certifikácie využívajúcich profily ochrany *Security IC Platform PP with Augmentation Packages (v1.0)* [Profil ochrany pre platformu bezpečnostného integrovaného obvodu s rozširujúcimi balíkmi (v1.0)], BSI-CC-PP-0084-2014, alebo *Java Card System – Closed Configuration (v3.1)* [Systém Java Card – uzavretá konfigurácia (v3.1)], BSI-CC-PP-0101-V2-2020 by sa na tie procesy, ktoré sa začali pred 1. októbrom 2026, mal uplatňovať dokument na základe aktuálneho stavu. V prípade procesov certifikácie využívajúcich profil ochrany *Java Card System – Open Configuration (v3.1)* [Systém Java Card – otvorená konfigurácia (v3.1)], BSI-CC-PP-0099-V2-2020 by sa mal dokument na základe aktuálneho stavu uplatňovať len na tie procesy, ktoré sa začali pred dátumom nadobudnutia účinnosti tohto nariadenia, keďže je už k dispozícii nová verzia profilu ochrany *Java Card System – Open Configuration* (Systém Java Card – otvorená konfigurácia).

(9) Zmena dokumentov na základe aktuálneho stavu počas procesu certifikácie by mohla narušiť hodnotenie produktu a oddialiť vydanie certifikátu. Pre nové alebo aktualizované dokumenty na základe aktuálneho stavu sú potrebné príslušné prechodné pravidlá, aby predajcovia, zariadenia ITSEF, certifikačné orgány a iné zainteresované strany mohli vykonať potrebné úpravy. Uplatniteľné aktualizované a nové dokumenty na základe aktuálneho stavu by sa mali týkať žiadostí o certifikáciu vrátane žiadostí o opätovné posúdenie a prehodnotenie, pričom by počas prebiehajúcich procesov certifikácie malo byť možné naďalej používať predchádzajúce verzie dokumentov na základe aktuálneho stavu.

(10) V prílohe II a prílohe III k vykonávaciemu nariadeniu (EÚ) 2024/482 sa uvádzajú príslušné profily ochrany certifikované na úrovni AVA_VAN 4 alebo 5 a odporúčané profily ochrany. Viacero odkazov je neúplných alebo zastaraných z dôvodu aktualizácie profilov ochrany. Tieto odkazy by sa mali doplniť a okrem toho by sa mali uviesť nové odkazy, aby sa zabezpečilo komplexnejšie pokrytie zabezpečených integrovaných obvodov, inteligentných kariet a súvisiacich zariadení a dôveryhodnej výpočtovej techniky.

(11) Je potrebné zmeniť článok 19 vykonávacieho nariadenia (EÚ) 2024/482 s cieľom objasniť, že príloha IV sa s potrebnými zmenami uplatňuje na preskúmanie certifikátov EUCC pre profily ochrany.

(12) Vzhľadom na to, že kľúčovým prvkom na pochopenie rozsahu pôsobnosti procesu certifikácie je bezpečnostný zámer, je takisto potrebné, aby agentúra ENISA na svojom webovom sídle zverejnila bezpečnostný zámer zodpovedajúci každému certifikátu EUCC.

(13) Certifikačné orgány by okrem toho mali agentúre ENISA poskytnúť anglické znenie bezpečnostného zámeru a správy o certifikácii, aby agentúra mohla tieto informácie sprístupniť v angličtine na príslušnom webovom sídle podľa článku 42 ods. 2 vykonávacieho nariadenia (EÚ) 2024/482. Z tohto dôvodu by žiadatelia o certifikáciu mali certifikačným orgánom poskytnúť vždy, keď o to požiadajú, anglickú verziu bezpečnostného zámeru.

(14) Nie je potrebné, aby sa v jedinečnej identifikácii certifikátu uvádzala zmienka názvu certifikačného orgánu, keďže identifikačné číslo certifikačného orgánu postačuje na jedinečnú identifikáciu tohto orgánu. Nie je potrebné uvádzať ani mesiac vydania, keďže počítanie certifikátov sa vykonáva na ročnom základe. Táto požiadavka by sa preto na účely zjednodušenia mala vypustiť. Keďže rok vydania certifikátu zodpovedá vydaniu prvého certifikátu, ten istý dátum by sa mal uviesť v jedinečnej identifikácii na certifikátoch vydaných po preskúmaní, aby sa zabezpečila vysledovateľnosť.

(15) Vykonávacie nariadenie (EÚ) 2024/482 by sa preto malo zodpovedajúcim spôsobom zmeniť.

(16) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 66 nariadenia (EÚ) 2019/881,

PRIJALA TOTO NARIADENIE:

Článok 1

Vykonávacie nariadenie (EÚ) 2024/482 sa mení takto:

1. V článku 2 sa dopĺňajú tieto body 16, 17 a 18:

„16. ‚produktová séria‘ je súbor produktov IKT žiadateľa postavený na rovnakom funkčnom základe s cieľom riešiť rovnaké bezpečnostné potreby, ktorých návrh, hardvér, firmvér alebo softvér sa môžu od produktu IKT k produktu IKT líšiť;

17. ‚menej závažná zmena‘ je akákoľvek zmena certifikovaného objektu hodnotenia alebo jeho prostredia, ktorá nemá nepriaznivý vplyv na záruku vyjadrenú v certifikáte EUCC;

18. ‚závažná zmena‘ je akákoľvek zmena certifikovaného objektu hodnotenia alebo jeho prostredia, ktorá môže mať nepriaznivý vplyv na záruku vyjadrenú v certifikáte EUCC.“

2. V článku 5 sa dopĺňa tento odsek 3:

„3. Certifikačný orgán môže povoliť certifikáciu produktovej série.“;

3. V článku 9 ods. 2 sa písmeno a) nahrádza takto:

„a) poskytnúť certifikačnému orgánu a zariadeniu ITSEF všetky potrebné úplné a správne informácie a na požiadanie poskytnúť ďalšie potrebné informácie vrátane anglického znenia bezpečnostného zámeru;“;

4. V článku 11 ods. 3 sa písmeno b) nahrádza takto:

„b) jedinečnú identifikáciu certifikátu, ktorá pozostáva z:

1. názvu schémy;

2. identifikačného čísla certifikačného orgánu, ktorý certifikát vydal, v súlade s článkom 3 vykonávacieho nariadenia (EÚ) 2024/3143;

3. roku vydania počiatočného certifikátu;

4. identifikačného čísla prideleného certifikačným orgánom, ktorý certifikát vydal.“;

5. V článku 19 sa odsek 1 nahrádza takto:

„1. Na žiadosť držiteľa certifikátu alebo z iných opodstatnených dôvodov môže certifikačný orgán rozhodnúť o preskúmaní certifikátu EUCC pre profil ochrany. Preskúmanie prebieha v súlade s prílohou IV. Rozsah preskúmania určí certifikačný orgán. Ak je to potrebné na účely preskúmania, certifikačný orgán požiada zariadenie ITSEF o vykonanie opätovného hodnotenia certifikovaného profilu ochrany.“

6. Článok 42 sa mení takto:

a) V odseku 1 sa dopĺňa toto písmeno i):

„i) bezpečnostný zámer zodpovedajúci každému certifikátu EUCC;“;

b) Odsek 2 sa nahrádza takto:

„2. Informácie uvedené v odseku 1 sa sprístupnia aspoň v anglickom jazyku. Na tento účel certifikačné orgány poskytnú agentúre ENISA pôvodné jazykové znenia správ o certifikácii a bezpečnostných zámerov a okrem toho bez zbytočného odkladu poskytnú aj anglické znenie takýchto dokumentov.“;

7. V článku 48 sa odsek 4 nahrádza takto:

„4. Pokiaľ nie je v prílohe I alebo II stanovené inak, dokumenty na základe aktuálneho stavu sa uplatňujú na procesy certifikácie vrátane opätovného posúdenia a opätovného hodnotenia začaté odo dňa začatia uplatňovania pozmeňujúceho aktu, ktorým boli dokumenty na základe aktuálneho stavu začlenené do prílohy I alebo II.“

8. Príloha I sa nahrádza textom uvedeným v prílohe I k tomuto nariadeniu.

9. Príloha II sa nahrádza textom uvedeným v prílohe II k tomuto nariadeniu.

10. Príloha III sa nahrádza textom uvedeným v prílohe III k tomuto nariadeniu.

11. Príloha IV sa mení v súlade s prílohou IV k tomuto nariadeniu.

12. Príloha V sa mení v súlade s prílohou V k tomuto nariadeniu.

13. Príloha IX sa nahrádza textom uvedeným v prílohe VI k tomuto nariadeniu.

Článok 2

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 8. decembra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

„PRÍLOHA I

Dokumenty na základe aktuálneho stavu podporujúce technické domény a iné dokumenty na základe aktuálneho stavu

1. Dokumenty na základe aktuálneho stavu podporujúce technické domény stupňov AVA_VAN 4 alebo 5:
   a) nasledujúce dokumenty týkajúce sa harmonizovaného hodnotenia technickej domény ‚inteligentné karty a podobné zariadenia‘:
      1. *Minimum ITSEF requirements for security evaluations of smart cards and similar devices* (Minimálne požiadavky na zariadenia ITSEF na hodnotenie bezpečnosti inteligentných kariet a podobných zariadení), verzia 1.1;
      2. *Minimum Site Security Requirements* (Minimálne bezpečnostné požiadavky na lokalitu), verzia 2;
      3. *Reusing evaluation results of site audits (STAR)* [Opätovné použitie výsledkov hodnotenia auditov na mieste (STAR)], verzia 1;
      4. *Application of Common Criteria to integrated circuits* (Uplatňovanie spoločných kritérií na integrované obvody), verzia 2;
      5. *Security Architecture requirements (ADV_ARC) for smart cards and similar devices* [Požiadavky na bezpečnostnú architektúru (ADV_ARC) pre inteligentné karty a podobné zariadenia], verzia 1.1;
      6. *Certification of ‚open‘ smart card products* (Certifikácia ‚otvorených‘ inteligentných kariet), verzia 1.1;
      7. *Composite product evaluation for smart cards and similar devices for CC3.1* (Hodnotenie zložených produktov pre inteligentné karty a podobné zariadenia pre CC3.1), verzia 2;
      8. *Composite product evaluation and certification for CC:2022* (Hodnotenie a certifikácia zloženého produktu pre CC:2022), verzia 1;
      9. *Application of Attack Potential to Smartcards and Similar Devices* (Použitie potenciálu útoku na inteligentné karty a podobné zariadenia), verzia 2;
      10. *Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices* (Hodnotenie bezpečnosti a certifikácia zariadení na vyhotovenie kvalifikovaného elektronického podpisu a pečate), verzia 1;
      11. *ADV_SPM.1 interpretation for CC:2022 transition* (Výklad ADV_SPM.1 pre prechod na CC:2022), verzia 1.1, uplatniteľný na procesy certifikácie využívajúce profily ochrany takto:
          a) profily ochrany Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, alebo Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, začaté pred 1. októbrom 2026;
          b) profil ochrany Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, začaté pred 29. decembrom 2025.
   b) nasledujúce dokumenty týkajúce sa harmonizovaného hodnotenia technickej domény ‚hardvérové zariadenia s bezpečnostnými skrinkami‘:
      1. *Minimum ITSEF requirements for security evaluations of hardware devices with security boxes* (Minimálne požiadavky na zariadenia ITSEF na hodnotenie bezpečnosti hardvérových zariadení s bezpečnostnými skrinkami), verzia 1.1;
      2. *Minimum Site Security Requirements* (Minimálne bezpečnostné požiadavky na lokalitu), verzia 2;
      3. *Reusing evaluation results of site audits (STAR)* [Opätovné použitie výsledkov hodnotenia auditov na mieste (STAR)], verzia 1;
      4. *Application of Attack Potential to hardware devices with security boxes* (Použitie potenciálu útoku na hardvérové zariadenia s bezpečnostnými skrinkami), verzia 2;
      5. *Hardware assessment in EN 419221-5 (HSM PP)* [Posúdenie hardvéru v norme EN 419221-5 (HSM PP)], verzia 1;
      6. ‚JIL Tachograph MS PP Clarification‘ (JIL tachograf MS PP objasnenie), verzia 1.
2. Dokumenty na základe aktuálneho stavu týkajúce sa harmonizovanej akreditácie orgánov posudzovania zhody:
   a) *Accreditation of ITSEFs for the EUCC* (Akreditácia zariadení ITSEF pre EUCC), verzia 1.1, v prípade akreditácií vydaných pred 8. júlom 2025;
   b) *Accreditation of ITSEFs for the EUCC* (Akreditácia zariadení ITSEF pre EUCC), verzia 1.6c, v prípade akreditácií, ktoré sú nanovo vydané alebo preskúmané po 8. júli 2025;
   c) *Accreditation of CBs for the EUCC* (Akreditácia certifikačných orgánov pre EUCC), verzia 1.6b.“

PRÍLOHA II

„PRÍLOHA II

Profily ochrany certifikované na stupni AVA_VAN 4 alebo 5

1. Pre zariadenia na vyhotovenie kvalifikovaného podpisu a pečate na diaľku:

   a) EN 419241-2:2019 – Dôveryhodné systémy podporujúce podpisovanie na strane servera – Časť 2: *Protection Profile for QSCD for Server Signing* (v0.16), ANSSI-CC-PP-2018/02-M01 [Profil ochrany pre zariadenie na vyhotovenie kvalifikovaného podpisu pre podpisovanie serverov (v0.16)], ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 – Profily ochrany kryptografických modulov pre poskytovateľov dôveryhodných služieb – Časť 5: *Cryptographic Module for Trust Services* (Kryptografický modul dôveryhodných služieb) (v0.15), ANSSI-CC-PP-2016/05-M01

2. Profily ochrany, ktoré boli prijaté ako dokumenty na základe aktuálneho stavu:

   [PRÁZDNE].“

PRÍLOHA III

„PRÍLOHA III

Odporúčané profily ochrany

Profily ochrany používané pri certifikácii produktov IKT vrátane produktov v technických doménach:

1. Inteligentné karty a podobné zariadenia
   a) Cestovný pas:
      1. *PP Machine Readable Travel Document with „ICAO Application" Basic Access Control* (Profil ochrany pre strojovo čitateľný cestovný doklad so základnou kontrolou prístupu do „aplikácie ICAO") (v1.10), BSI-CC-PP-0055-2009;
      2. *PP Machine Readable Travel Document using Standard Inspection Procedure with PACE* [Profil ochrany pre strojovo čitateľný cestovný doklad s použitím štandardného postupu inšpekcie s 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* (Profil ochrany pre strojovo čitateľný cestovný doklad s rozšírenou kontrolou prístupu do „aplikácie ICAO" s PACE) (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   b) Bezpečné zariadenie na vyhotovenie elektronického podpisu (SSCD):
      1. EN 419211-2:2013 – Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu – Časť 2: Zariadenie s generovaním kľúča (v1.03), BSI-CC-PP-0059-2009-MA-02;
      2. EN 419211-3:2013 – Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu – Časť 3: Zariadenie s importovaním kľúča (v1.0.2), BSI-CC-PP-0075-2012-MA-01;
      3. EN 419211-4:2013 – Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu – Časť 4: Rozšírenie pre zariadenie s generovaním kľúča a dôveryhodným kanálom k aplikácii na generovanie certifikátov (v1.0.1), BSI-CC-PP-0071-2012-MA-01;
      4. EN 419211-5:2013 – Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu – Časť 5: Rozšírenie pre zariadenie s generovaním kľúča a dôveryhodným kanálom k aplikácii na vyhotovovanie podpisov (v1.0.1), BSI-CC-PP-0072-2012-MA-01;
      5. EN 419211-6:2014 – Profily ochrany pre zariadenia na vyhotovenie bezpečného podpisu – Časť 6: Rozšírenie pre zariadenie s importovaním kľúča a dôveryhodným kanálom k aplikácii na vyhotovovanie podpisov (v1.0.4), BSI-CC-PP-0076-2013-MA-01;
   c) Tachograf: Digitálny tachograf – tachografová karta (TC PP) (v1.0), BSI-CC-PP-0091-2017;
   d) Bezpečné integrované obvody, platforma Java Card a eUICC:
      1. *Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations* (Profil ochrany pre platformu Java Card univerzálnej SIM v základnej konfigurácii a SCWS) (v2.0.2), ANSSI-CC-PP-2010/04 (Basic), ANSSI-CC-PP-2010/05 (Basic a SCWS);
      2. *Security IC Platform PP with Augmentation Packages* (Profil ochrany pre platformu zabezpečených integrovaných obvodov s rozšírenými balíkmi) (v1.0), BSI-CC-PP-0084-2014;
      3. *Embedded UICC (eUICC) for Machine-to-Machine Devices* [Zabudovaná karta UICC (eUICC) pre zariadenia stroj-stroj](v1.1), BSI-CC-PP-0089-2015;
      4. *Cryptographic Service Provider – CSP* (Poskytovateľ kryptografických služieb) (v0.9.8), BSI-CC-PP-0104-2019;
      5. *Cryptographic Service Provider – Time Stamp Service and Audit* (Poskytovateľ kryptografických služieb – služba časových pečiatok a audit) (PPC-CSP-TS-Au) verzia 0.9.5, BSI-CC-PP-0107-2019;
      6. *Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering* (PPC-CSP-TS-Au-Cl) (Konfigurácia poskytovateľ kryptografických služieb – služba časových pečiatok, audit a klastrovanie) verzia 0.9.4, BSI-CC-PP-0108-2019;
      7. *Java Card System – Closed Configuration* (Systém Java Card – zatvorená konfigurácia) (v3.1), BSI-CC-PP-0101-V2-2020;
      8. *Secure Element Protection Profile – GPC_SPE_174* (Profil ochrany bezpečných prvkov) (v1.0), CCN-CC-PP-5-2021;
      9. *Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile* (Profil ochrany Zabezpečený subsystém v systéme na čipe) (v1.8), BSI-CC-PP-0117-V2-2023;
      10. *Java Card System – Open Configuration* (Systém Java Card – otvorená konfigurácia) (v3.2), BSI-CC-PP-0099-V3-2024;
      11. *Embedded UICC for Consumer Devices Protection Profile* (Profil ochrany Zabudovaný UICC pre spotrebiteľské zariadenia) (v2.1), BSI-CC-PP-0100-V2-2025;
   e) Modul dôveryhodnej platformy: *Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0* (Profil ochrany pre rodinu špecifikácií 2.0 modulov dôveryhodnej platformy špecifickú pre klienta PC, úroveň 0, revízia 1.59) (v1.3), ANSSI-CC-PP-2021/02;

2. Hardvérové zariadenia s bezpečnostnými schránkami.

   a) miesta (platobnej) interakcie a platobné terminály (POI):

      1. *Point of Interaction* (Miesto interakcie) „POI-CHIP-ONLY“ (v4.0), ANSSI-CC-PP-2015/01;

      2. *Point of Interaction* (Miesto interakcie) „POI-CHIP-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/02;

      3. *Point of Interaction* (Miesto interakcie) „POI-COMPREHENSIVE“ (v4.0), ANSSI-CC-PP-2015/03;

      4. *Point of Interaction* (Miesto interakcie) „POI-COMPREHENSIVE and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/04;

      5. *Point of Interaction* (Miesto interakcie) „POI-PED-ONLY“ (v4.0), ANSSI-CC-PP-2015/05;

      6. *Point of Interaction* (Miesto interakcie) „POI-PED-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/06;

   b) Hardvérový bezpečnostný modul:

      1. *Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB 14167-2* (Kryptografický modul pre operácie podpisovania CSP so zálohovaním – profil ochrany CMCSOB 14167-2) (v0.35), ANSSI-CC-PP-2015/08;

      2. *Cryptographic Module for CSP Key Generation Services* – PP CMCKG 14167-3 (kryptografický modul pre služby generovania kľúčov CSP) (v0.20), ANSSI-CC-PP-2015/09;

      3. *Cryptographic Module for CSP Signing Operations without Backup – PP* CMCSO 14167-4 (Kryptografický modul pre operácie podpisovania CSP bez zálohovania – profil ochrany CMCSO 14167-4)(v0.32), ANSSI-CC-PP-2015/10;

   c) Tachograf:

      1. *Digital Tachograph – Motion Sensor* (Digitálny tachograf – snímač pohybu) (MS PP) (v1.0), BSI-CC-PP-0093-2017;

      2. *Digital Tachograph – Vehicle Unit* (Digitálny tachograf – vozidlová jednotka) (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;

      3. *Digital Tachograph – External GNSS Facility* (Digitálny tachograf – externé zariadenie GNSS) (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021;

3. Iné: *Trusted Execution Environment Protection Profile – GPD_SPE_021* (Profil ochrany dôveryhodného vykonávacieho prostredia – GPD_SPE_021) (v1.3), ANSSI-CC-PP-2014/01-M02.“

PRÍLOHA IV

Príloha IV k vykonávaciemu nariadeniu (EÚ) 2024/482 sa mení takto:

1. V oddiele IV.2 sa bod 4 nahrádza takto:

„4. Certifikačný orgán preskúma túto aktualizovanú technickú správu hodnotenia a vypracuje správu o opätovnom posúdení. Stav počiatočného certifikátu sa následne upraví v súlade s článkom 13 alebo článkom 19. Ak je proces opätovného posúdenia úspešný, v prípade certifikácie produktu sa uplatňuje článok 13 ods. 2 písm. a) alebo c) a v prípade certifikácie profilu ochrany sa uplatňuje článok 19 ods. 2 písm. a) alebo c). Ak proces opätovného posúdenia nie je úspešný, v prípade certifikácie produktu sa uplatňuje článok 13 ods. 2 písm. b) alebo d) a v prípade certifikácie profilu ochrany sa uplatňuje článok 19 ods. 2 písm. b) alebo d).“

2. Oddiel IV.3 sa mení takto:

a) Názov oddielu IV.3 sa nahrádza takto:

„IV.3 **Zmeny certifikovaného produktu IKT – údržba a opätovné hodnotenie**“

b) body 4 a 5 sa nahrádzajú takto:

„4. Po preskúmaní certifikačný orgán určí rozsah zmeny ako menej závažný alebo závažný v súlade s jej vplyvom na dôveryhodnosť vyjadrenú v certifikáte EUCC.

5. Ak certifikačný orgán potvrdil, že zmeny sú menej závažné, nevydá sa pre upravený produkt IKT v súlade s článkom 13 ods. 2 písm. a) alebo článkom 19 ods. 2 písm. a) žiaden nový certifikát a k pôvodnej správe o certifikácii sa vypracuje správa o údržbe.“

c) Vkladá sa tento odsek 5a:

„5a. V prípade akýchkoľvek zmien opatrení dôveryhodnosti vo vývojárskom prostredí vrátane doplnenia požiadaviek na dôveryhodnosť zo skupiny CC ALC_FLR (náprava chyby) môže certifikačný orgán požiadať zariadenie ITSEF o vykonanie čiastkového hodnotenia dotknutých opatrení dôveryhodnosti. Zariadenie ITSEF vydá technickú správu o čiastkovom hodnotení, na základe ktorej certifikačný orgán potvrdí, že zmeny sú buď menej závažné, alebo závažné. Ak certifikačný orgán potvrdí, že zmeny sú menej závažné, uplatňuje sa príloha IV.3 bod 5. Ak certifikačný orgán potvrdí, že zmeny sú závažné, uplatňuje sa príloha IV.3 bod 7.“

PRÍLOHA V

Bod V.1 prílohy VI k vykonávaciemu nariadeniu (EÚ) 2024/482 sa nahrádza takto:

„V.1. **Správa o certifikácii**

1. Certifikačný orgán na základe technických správ hodnotenia, ktoré poskytne zariadenie ITSEF, vypracuje správu o certifikácii, ktorá sa uverejní spolu s príslušným certifikátom EUCC a bezpečnostným zámerom.

2. Správa o certifikácii je zdrojom podrobných a praktických informácií o produkte IKT a o bezpečnom zavádzaní produktu IKT. Preto musí obsahovať všetky verejne dostupné a zdieľateľné informácie, ktoré sú relevantné pre používateľov a zainteresované strany. V správe o certifikácii možno odkazovať na verejne dostupné a zdieľateľné informácie.

3. Správa o certifikácii musí obsahovať aspoň tieto informácie:

   a) zhrnutie;

   b) identifikácia produktu IKT;

   c) kontaktné informácie súvisiace s hodnotením produktu IKT;

   d) bezpečnostné stratégie;

   e) predpoklady a objasnenie rozsahu pôsobnosti;

   f) informácie o architektúre;

   g) prípadné doplnkové informácie o kybernetickej bezpečnosti;

   h) zhrnutie hodnotenia produktu IKT a hodnotená konfigurácia;

   i) výsledky hodnotenia a informácie týkajúce sa certifikátu;

   j) prípadné pripomienky a odporúčania;

   k) prípadné prílohy;

   l) odkaz na bezpečnostný zámer produktu IKT predloženého na certifikáciu;

   m) značka alebo označenie spojené so systémom, ak sú k dispozícii;

   n) glosár, ak existuje;

   o) bibliografia.

4. Zhrnutie uvedené v odseku 3 písm. a) je stručným zhrnutím celej správy o certifikácii. Musí poskytovať jasný a výstižný prehľad výsledkov hodnotenia a musí obsahovať tieto informácie:

   a) názov hodnoteného produktu IKT;

   b) názov zariadenia ITSEF, ktoré vykonalo hodnotenie;

   c) dátum ukončenia hodnotenia;

   d) dátum vydania certifikátu;

   e) dátum vydania počiatočného certifikátu, ak existuje;

   f) obdobie platnosti;

   g) jedinečná identifikácia certifikátu v zmysle článku 11;

   h) stručný opis výsledkov správy o certifikácii, a to aj:

      i) verziu a prípadne vydanie spoločných kritérií použitých na hodnotenie;

      ii) balík dôveryhodnosti spoločných kritérií alebo zoznam zložiek bezpečnostnej dôveryhodnosti, stupeň AVA_VAN použitý počas hodnotenia a jeho zodpovedajúci stupeň dôveryhodnosti stanovený v článku 52 nariadenia (EÚ) 2019/881, na ktorý sa vzťahuje certifikát EUCC;

      iii) prípadne profil(-y) ochrany, súlad s ktorým (ktorými) sa v prípade produktu IKT konštatuje;

      iv) odkaz na bezpečnostnú politiku hodnoteného produktu IKT;

      v) prípadné vyhlásenie (vyhlásenia) o odmietnutí zodpovednosti.

5. V identifikácii uvedenej v odseku 3 písm. b) musí byť jasne určený hodnotený produkt IKT vrátane týchto informácií:

   a) jedinečná identifikácia hodnoteného produktu IKT;

   b) vymenovanie zložiek produktu IKT, ktoré sú súčasťou hodnotenia, s číslom verzie každej zložky;

   c) odkaz na ďalšie požiadavky na operačné prostredie certifikovaného produktu IKT.

6. Kontaktné údaje uvedené v odseku 3 písm. c) musia obsahovať aspoň tieto informácie:

   a) názov vývojára;

   b) meno/názov a kontaktné údaje držiteľa certifikátu EUCC;

   c) názov certifikačného orgánu, ktorý vystavil certifikát;

   d) zodpovedný vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti;

   e) názov zariadenia ITSEF, ktoré vykonalo hodnotenie, a prípadne zoznam subdodávateľov.

7. Bezpečnostná politika uvedená v odseku 3 písm. d) musí obsahovať opis bezpečnostnej politiky produktu IKT ako zbierky bezpečnostných služieb a politík alebo pravidiel, ktoré musí hodnotený produkt IKT presadzovať alebo dodržiavať. Obsahovať musí aj tieto informácie:

   a) opis postupov držiteľa certifikátu týkajúcich sa riadenia zraniteľností a zverejňovania informácií o zraniteľnosti, ktorý má zahŕňať výlučne informácie, ktoré možno sprístupniť verejnosti;

   b) politiku zachovávania dôvernosti držiteľa certifikátu, prípadne vrátane opisu riadenia životného cyklu alebo výrobných procesov držiteľa certifikátu v súlade s oddielom IV.1 prílohy IV;

   c) prípadne prítomnosť postupu riadenia záplat a výsledok jeho posúdenia v súlade s oddielom IV.4 prílohy IV.

8. Predpoklady a objasnenie rozsahu pôsobnosti uvedené v odseku 3 písm. e) musia obsahovať informácie týkajúce sa okolností a cieľov súvisiacich so zamýšľaným použitím produktu, ako sa uvádza v článku 7 ods. 1 písm. c), a musia zahŕňať:

   a) predpoklady týkajúce sa používania a nasadenia produktu IKT vo forme minimálnych požiadaviek, ako je správna inštalácia a konfigurácia a splnenie hardvérových požiadaviek;

   b) predpoklady týkajúce sa prostredia pre prevádzku produktu IKT v súlade s predpismi.

   c) opis akýchkoľvek hrozieb pre produkt IKT, ktorým nezabraňujú hodnotené bezpečnostné funkcie produktu podľa zamýšľaného použitia, ak sa to považuje za relevantné pre potenciálneho používateľa produktu IKT.

   Informácie uvedené v prvom pododseku musia byť čo najjasnejšie a najzrozumiteľnejšie, aby potenciálni používatelia certifikovaného produktu IKT mohli prijímať informované rozhodnutia o rizikách spojených s jeho používaním.

9. Informácie o architektúre uvedené v odseku 3 písm. f) zahŕňajú všeobecný opis produktu IKT a jeho hlavných zložiek na základe požadovaných výsledkov vymedzených v skupine dôveryhodnosti spoločných kritérií: Vývoj – návrh objektu hodnotenia (ADV_TDS).

10. Doplňujúce informácie o kybernetickej bezpečnosti uvedené v odseku 3 písm. g) musia zahŕňať odkaz na webové sídlo držiteľa certifikátu EUCC uvedeného v článku 55 nariadenia (EÚ) 2019/881.

11. V hodnotení a konfigurácii produktu IKT uvedených v odseku 3 písm. h) sa opisujú činnosti skúšania vývojárov aj hodnotiteľov, pričom sa uvádza skúšobný prístup, konfigurácia a hĺbka. Uvádzajú sa v nich minimálne tieto informácie:

    a) identifikácia použitých zložiek dôveryhodnosti z noriem uvedených v článku 3;

    b) verzia dokumentov na základe aktuálneho stavu a ďalšie kritériá hodnotenia bezpečnosti použité v hodnotení;

    c) nastavenia a konfigurácia objektu hodnotenia použité na skúšanie a analýzu zraniteľnosti;

    d) akýkoľvek profil ochrany, ktorý sa použil, vrátane týchto informácií: názov profilu ochrany, verzia, dátum a certifikát.

12. Výsledky hodnotenia a informácie týkajúce sa certifikátu uvedeného v odseku 3 písm. i) musia obsahovať informácie o dosiahnutom stupni dôveryhodnosti v zmysle článku 4 tohto nariadenia a článku 52 nariadenia (EÚ) 2019/881.

13. Pripomienky a odporúčania uvedené v odseku 3 písm. j) sa používajú na poskytnutie dodatočných informácií o výsledkoch hodnotenia. Uvedené pripomienky a odporúčania môžu mať formu nedostatkov produktu IKT zistených počas hodnotenia alebo zmienok o prvkoch, ktoré sú obzvlášť užitočné.

14. Prílohy uvedené v odseku 3 písm. k) sa používajú na opis akýchkoľvek dodatočných informácií, ktoré môžu byť užitočné pre prijímateľov správy, ale logicky nezodpovedajú predpísaným oddielom správy, a to aj v prípadoch úplného opisu bezpečnostnej politiky.

15. Bezpečnostný zámer uvedený v odseku 3 písm. l) musí obsahovať odkaz na zhodnotený bezpečnostný zámer. Zhodnotený bezpečnostný zámer sa poskytne spolu so správou o certifikácii na účely uverejnenia na webovom sídle uvedenom v článku 50 ods. 1 nariadenia (EÚ) 2019/881. Ak je pred uverejnením zhodnoteného bezpečnostného zámeru potrebná úprava, vykoná sa v súlade s oddielom V.2 prílohy V k tomuto nariadeniu.

16. Do správy o certifikácii sa vložia značky alebo označenia spojené so schémou EUCC uvedenou v odseku 3 písm. m), a to v súlade s pravidlami a postupmi stanovenými v článku 11.

17. Glosár uvedený v odseku 3 písm. n) sa používa na zvýšenie čitateľnosti správy prostredníctvom vymedzenia akronymov alebo pojmov, ktorých význam nemusí byť okamžite zrejmý.

18. Bibliografia uvedená v odseku 3 písm. o) musí obsahovať odkazy na všetky dokumenty použité pri zostavovaní správy o certifikácii. Tieto informácie musia zahŕňať aspoň:

    a) kritériá hodnotenia bezpečnosti, dokumenty na základe aktuálneho stavu a ďalšie použité relevantné špecifikácie;

    b) technickú správu hodnotenia;

    c) v prípade potreby technickú správu hodnotenia pre kompozitné hodnotenie;

    d) technickú referenčnú dokumentáciu;

    e) bezpečnostné usmernenia vývojára;

    f) zoznam konfigurácie vývojára.

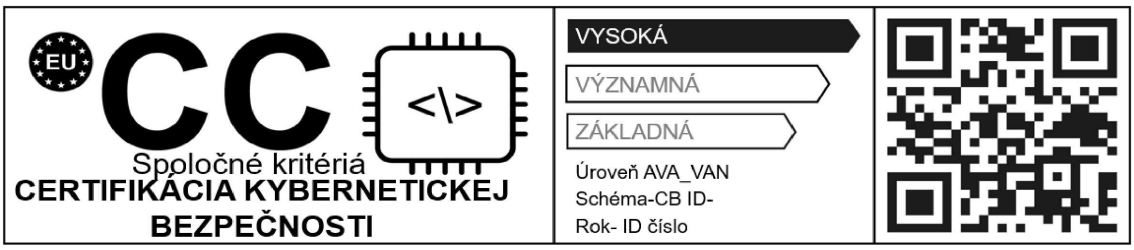
    S cieľom zaručiť reprodukovateľnosť hodnotenia musia byť všetky dokumenty, na ktoré sa odkazuje, jednoznačne identifikované správnym dátumom vydania a správnym číslom verzie.“

PRÍLOHA VI

„PRÍLOHA IX

Značka a označenie

1. Forma značky a označenia:



2. Ak sú značka a označenie zmenšené alebo zväčšené, musia sa dodržať proporcie uvedené v bode 1.

3. Ak sú značka a označenie fyzicky prítomné, musia mať výšku aspoň 5 mm.“