Úřední věstník
Evropské unie

CS
Řada L

2025/2462

9.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2462

ze dne 8. prosince 2025,

kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o definice, certifikaci produktových řad produktů IKT, kontinuitu záruky a přehledy aktuálních certifikačních postupů

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) ([1]), a zejména na čl. 49 odst. 7 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Prováděcí nařízení Komise (EU) 2024/482 ([2]) v souladu s evropským rámcem pro certifikaci kybernetické bezpečnosti stanoveným v nařízení (EU) 2019/881 vymezuje úlohy, pravidla a povinnosti, jakož i strukturu evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC).

(2) Společná metodika hodnocení, která společná kritéria doplňuje a je mezinárodní normou pro hodnocení bezpečnosti informací, umožňuje hodnocení bezpečnosti produktů IKT pro účely certifikace. S tím souvisí skutečnost, že některé produkty IKT mohou být vystavěny na stejném funkčním základě, aby nabízely podobné bezpečnostní funkce na různých platformách nebo zařízeních, a bývají rovněž označovány jako produktové řady. Návrh, hardware, firmware nebo software se však mohou u jednotlivých produktů IKT lišit. Je na certifikačním orgánu, aby v každém konkrétním případě rozhodl, zda lze produktovou řadu certifikovat. Podmínky pro certifikaci produktových řad by mohly být dále objasněny v podpůrných pokynech EUCC.

(3) Aby byla zachována spolehlivost certifikovaných produktů, je nezbytné definovat, co představuje velkou a drobnou změnu cíle hodnocení nebo jeho prostředí, včetně provozního nebo vývojového. S ohledem na stávající a široce používané technické specifikace skupiny vyšších úředníků pro bezpečnost informačních systémů (SOG-IS) a účastníků ujednání o uznávání osvědčení podle společných kritérií v oblasti bezpečnosti IT (CCRA) je proto nezbytné tyto pojmy upřesnit.

(4) Drobné změny se často vyznačují omezeným dopadem na prohlášení o záruce bezpečnosti produktu, kterou poskytuje vydaný certifikát EUCC. Drobné změny by proto měly být řešeny v rámci postupů udržování a nevyžadují přehodnocení bezpečnostních funkcí produktu. Za drobné změny, které by měly být řešeny prostřednictvím postupů udržování, se považují mimo jiné redakční změny, změny cíle hodnotícího prostředí, které nemění certifikovaný cíl hodnocení, a změny certifikovaného cíle hodnocení, které nemají vliv na důkazy o záruce. Za drobné mohou být považovány i změny ve vývojovém prostředí, pokud nemají následný dopad na stávající opatření k zajištění záruky. V některých případech však může být nutné provést částečné hodnocení příslušných opatření.

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

([2]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Velkou změnou je jakákoli změna certifikovaného cíle hodnocení nebo jeho prostředí, která může mít nepříznivý dopad na záruku vyjádřenou certifikátem EUCC, a proto by v případě takové změny mělo být povinné provést přehodnocení. Mezi velké změny patří mimo jiné změny souboru požadavků na konkrétní záruku s výjimkou požadavků na záruku u rodiny CC ALC_FLR (odstranění nedostatků), změny kontrol důvěrnosti nebo integrity ve vývojovém prostředí, pokud by tyto změny mohly ovlivnit bezpečný vývoj nebo produkci cíle hodnocení, nebo změny cíle hodnocení za účelem vyřešení zneužitelné zranitelnosti. Kromě toho může být za velkou změnu považován soubor drobných změn, které mají společně významný dopad na bezpečnost. Je rovněž nutné připustit, že i když oprava chyby může ovlivnit pouze konkrétní aspekt cíle hodnocení, její nepředvídatelnost a potenciální dopad na záruku z ní mohou učinit velkou změnu, pokud ohrožuje bezpečnostní záruky poskytované certifikací.

(6) V případě změn v prostředí hrozeb nezměněného certifikovaného produktu IKT by mohlo být nutné provést přehodnocení. Je třeba jasně stanovit možné výsledky procesu přehodnocení, a zejména jeho dopad na certifikát EUCC. Po úspěšném dokončení přehodnocení by certifikační orgán měl certifikát potvrdit nebo vydat nový certifikát s prodlouženým datem platnosti. Pokud je proces přehodnocení neúspěšný, měl by certifikační orgán certifikát zrušit, případně vydat nový certifikát s jiným rozsahem platnosti. Tato ustanovení by se měla obdobně vztahovat i na přehodnocení profilů ochrany.

(7) Příloha I prováděcího nařízení (EU) 2024/482 uvádí použitelné přehledy aktuálních certifikačních postupů pro hodnocení produktů IKT a profilů ochrany. Tyto přehledy by měly být aktualizovány tak, aby odrážely nejnovější vývoj, například vývoj v oblasti technologií, v prostředí kybernetických hrozeb, vývoj postupů v odvětví nebo vývoj mezinárodních norem. Je vhodné zaktualizovat přehledy aktuálních certifikačních postupů týkající se minimálních bezpečnostních požadavků na lokalitu, uplatnění potenciálu útoku na čipové karty, uplatnění potenciálu útoku na hardwarová zařízení s bezpečnostními schránkami, použití společných kritérií na integrované obvody a hodnocení složených produktů pro čipové karty a podobná zařízení. Kromě toho nejsou na seznamu zahrnuty přehledy aktuálních certifikačních postupů týkající se hodnocení a certifikace složených produktů za použití nejnovější verze standardů společných kritérií, přehledy týkající se opětovného použití výsledků hodnocení z auditů na místě a objasnění výkladu profilů ochrany vztahujících se na prostředky pro vytváření kvalifikovaných elektronických podpisů, tachografy a hardwarové bezpečnostní moduly. V zájmu jednotného hodnocení produktů IKT v rámci EUCC by měla být příloha I změněna tak, aby zahrnovala aktualizované a nové přehledy aktuálních certifikačních postupů po jejich schválení Evropskou skupinou pro certifikaci kybernetické bezpečnosti (ECCG).

(8) Kromě toho by měl být do systému doplněn přehled aktuálních certifikačních postupů *ADV_SPM.1 interpretation for CC:2022 transition* (Výklad ADV_SPM.1 pro přechod na CC:2022), aby se zajistilo, že certifikační procesy založené na konkrétních profilech ochrany mohou pokračovat v používání formálního modelování (ADV_SPM.1) až do aktualizace příslušných profilů ochrany, například přidáním konfigurace profilu ochrany s více zárukami odpovídající verzi CC:2022, která podporuje ADV_SPM.1. Aby měl trh dostatek času na přechod k aktualizovaným standardům společných kritérií, je třeba stanovit zvláštní přechodná pravidla pro profily ochrany *Security IC Platform PP with Augmentation Packages* (profil ochrany pro bezpečnostní platformu IC s rozšiřujícími balíky) (v1.0), BSI-CC-PP-0084–2014, *Java Card System – Closed Configuration* (systém Java Card – uzavřená konfigurace) (v3.1), BSI-CC-PP-0101-V2–2020, či *Java Card System – Open Configuration* (systém Java Card – otevřená konfigurace) (v3.1), BSI-CC-PP-0099-V2–2020. Aby se zabránilo narušení trhu, je vhodné stanovit, že přehled aktuálních certifikačních postupů týkající se výkladu ADV_SPM.1 pro přechod na CC:2022 se vztahuje na certifikační procesy, které byly zahájeny před přijetím tohoto nařízení. Jeho použití by však mělo být přísně omezeno na to, co je nezbytné s ohledem na dobu potřebnou k dokončení aktualizace příslušných profilů ochrany. Přesněji řečeno, v případě certifikačních procesů používajících *Security IC Platform PP with Augmentation Packages* (profil ochrany pro bezpečnostní platformu IC s rozšiřujícími balíky) (v1.0), BSI-CC-PP-0084–2014, nebo *Java Card System – Closed Configuration* (systém Java Card – uzavřená konfigurace) (v3.1), BSI-CC-PP-0101–V2–2020, by se uvedený přehled měl použít na procesy, které byly zahájeny před 1. říjnem 2026. V případě certifikačních procesů používajících profil ochrany *Java Card System – Open Configuration* (systém Java Card – otevřená konfigurace) (v3.1), BSI-CC-PP-0099-V2–2020, by se uvedený přehled měl vztahovat pouze na procesy zahájené před datem vstupu tohoto nařízení v platnost, neboť nová verze profilu ochrany *Java Card System – Open Configuration* je již k dispozici.

(9) Změna v přehledech aktuálních certifikačních postupů během certifikačního procesu by mohla narušit hodnocení produktu a zpozdit vydání certifikátu. Proto je pro nové nebo aktualizované přehledy aktuálních certifikačních postupů nutné stanovit vhodná přechodná pravidla, která prodejcům, zařízením ITSEF, certifikačním orgánům a dalším zúčastněným stranám umožní provést nezbytné úpravy. Použitelné aktualizované a nové přehledy aktuálních certifikačních postupů by se měly týkat žádostí o certifikaci, včetně žádostí o přehodnocení, přičemž by mělo být možné, aby probíhající certifikační procesy nadále používaly dřívější verze přehledů aktuálních certifikačních postupů.

(10) V přílohách II a III prováděcího nařízení (EU) 2024/482 jsou uvedeny profily ochrany certifikované na úrovni AVA_VAN 4 nebo 5 a doporučené profily ochrany. Vzhledem k aktualizaci profilů ochrany je několik odkazů neúplných nebo zastaralých. Tyto odkazy by měly být doplněny a aktualizovány, a kromě toho by měly být doplněny nové odkazy, aby se zajistilo komplexnější pokrytí bezpečných integrovaných obvodů, čipových karet a souvisejících zařízení a důvěryhodných počítačových systémů.

(11) Je nezbytné změnit článek 19 prováděcího nařízení (EU) 2024/482 s cílem vyjasnit, že příloha IV s nezbytnými změnami se použije na přezkum certifikátů EUCC pro profily ochrany.

(12) Vzhledem k tomu, že bezpečnostní cíl je klíčovým prvkem pro pochopení rozsahu certifikačního procesu, je rovněž nezbytné, aby agentura ENISA na svých internetových stránkách zveřejnila bezpečnostní cíl odpovídající každému certifikátu EUCC.

(13) Certifikační subjekty by dále měly agentuře ENISA poskytnout anglickou verzi bezpečnostního cíle a zprávy o certifikaci, aby agentura mohla tyto informace zpřístupnit v angličtině na příslušných internetových stránkách podle čl. 42 odst. 2 prováděcího nařízení (EU) 2024/482. Z tohoto důvodu by měli žadatelé o certifikaci poskytnout certifikačním orgánům na jejich žádost anglickou verzi bezpečnostního cíle.

(14) Není nutné, aby v jedinečné identifikaci certifikátu byl uveden odkaz na název certifikačního subjektu, neboť k jednoznačné identifikaci certifikačního subjektu postačuje jeho identifikační číslo. Nemusí se uvádět ani měsíc vydání, protože počítání certifikátů se provádí na roční bázi. Tento požadavek by proto měl být pro účely zjednodušení zrušen. Jelikož rok vydání certifikátu odpovídá vydání prvního certifikátu, mělo by být totéž datum uvedeno v jedinečné identifikaci na certifikátech vydaných po přezkumu, čímž se zajistí sledovatelnost.

(15) Prováděcí nařízení (EU) 2024/482 by proto mělo být odpovídajícím způsobem změněno.

(16) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 66 nařízení (EU) 2019/881,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Prováděcí nařízení (EU) 2024/482 se mění takto:

1) v článku 2 se doplňují body 16, 17 a 18, které znějí:

„16) „produktovou řadou“ se rozumí soubor produktů IKT žadatele, jež jsou vystavěny na stejném funkčním základě za účelem řešení stejných bezpečnostních potřeb, přičemž návrh, hardware, firmware nebo software se mohou u jednotlivých produktů IKT lišit;

17) „drobnou změnou“ se rozumí jakákoli změna certifikovaného cíle hodnocení nebo jeho prostředí, která nemá nepříznivý dopad na záruku vyjádřenou certifikátem EUCC;

18) „velkou změnou“ se rozumí jakákoli změna certifikovaného cíle hodnocení nebo jeho prostředí, která může mít nepříznivý dopad na záruku vyjádřenou certifikátem EUCC.“;

2) v článku 5 se doplňuje nový odstavec 3, který zní:

„3. Certifikační subjekt může povolit certifikaci produktové řady.“;

3) v čl. 9 odst. 2 se písmeno a) nahrazuje tímto:

„a) poskytnout certifikačnímu subjektu a zařízení ITSEF všechny nezbytné úplné a správné informace a na požádání poskytnout další potřebné informace, včetně anglické verze bezpečnostního cíle;“

4) v čl. 11 odst. 3 se písmeno b) nahrazuje tímto:

„b) jedinečnou identifikaci certifikátu, která se skládá z:

1) názvu systému;

2) identifikačního čísla certifikačního subjektu, který certifikát vydal, přiděleného v souladu s článkem 3 prováděcího nařízení (EU) 2024/3143;

3) roku vydání původního certifikátu;

4) identifikačního čísla přiděleného certifikačním subjektem, který certifikát vydal.“;

5) v článku 19 se odstavec 1 nahrazuje tímto:

„1. Na žádost držitele certifikátu nebo z jiných oprávněných důvodů může certifikační subjekt rozhodnout o přezkumu certifikátu EUCC pro profil ochrany. Přezkum se provádí v souladu s přílohou IV. Rozsah přezkumu určí certifikační subjekt. Je-li to pro přezkum nezbytné, certifikační subjekt požádá zařízení ITSEF o provedení přehodnocení certifikovaného profilu ochrany.“;

6) článek 42 se mění takto:

a) v odstavci 1 se doplňuje nové písmeno i), které zní:

„i) bezpečnostní cíl odpovídající každému certifikátu EUCC.“;

b) odstavec 2 se nahrazuje tímto:

„2 Informace uvedené v odstavci 1 jsou k dispozici alespoň v angličtině. Za tímto účelem poskytnou certifikační subjekty agentuře ENISA původní jazykové verze zpráv o certifikaci a bezpečnostních cílů a kromě toho bez zbytečného odkladu poskytnou rovněž anglickou verzi těchto dokumentů.“;

7) v článku 48 se odstavec 4 nahrazuje tímto:

„4. Není-li v příloze I nebo II stanoveno jinak, použijí se přehledy aktuálních certifikačních postupů na certifikační procesy včetně přehodnocení zahájené počínaje dnem použitelnosti pozměňujícího aktu, kterým byly začleněny do přílohy I nebo II.“;

8) příloha I se nahrazuje zněním uvedeným v příloze I tohoto nařízení;

9) příloha II se nahrazuje zněním uvedeným v příloze II tohoto nařízení;

10) příloha III se nahrazuje zněním uvedeným v příloze III tohoto nařízení;

11) příloha IV se mění v souladu s přílohou IV tohoto nařízení;

12) příloha V se mění v souladu s přílohou V tohoto nařízení;

13) příloha IX se nahrazuje zněním uvedeným v příloze VI tohoto nařízení.

Článek 2

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 8. prosince 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

„PŘÍLOHA I

Přehledy aktuálních certifikačních postupů pro technické oblasti a další přehledy aktuálních certifikačních postupů

1. Přehledy aktuálních certifikačních postupů pro technické oblasti na úrovni AVA_VAN 4 nebo 5:
   a) následující dokumenty týkající se harmonizovaného hodnocení technické oblasti „čipové karty a podobná zařízení“:
      1) *Minimum ITSEF requirements for security evaluations of smart cards and similar devices* (Minimální požadavky na bezpečnostní hodnocení čipových karet a podobných zařízení vůči zařízením ITSEF), verze 1.1;
      2) *Minimum Site Security Requirements* (Minimální bezpečnostní požadavky na lokalitu), verze 2;
      3) *Reusing evaluation results of site audits* (STAR) (Opětovné použití výsledků hodnocení z auditů na místě (STAR)), verze 1;
      4) *Application of Common Criteria to integrated circuits* (Použití společných kritérií na integrované obvody), verze 2;
      5) *Security Architecture requirements (ADV_ARC) for smart cards and similar devices* (Požadavky na bezpečnostní architekturu (ADV_ARC) pro čipové karty a podobná zařízení), verze 1.1;
      6) *Certification of 'open' smart card products* (Certifikace produktů „otevřených“ čipových karet), verze 1.1;
      7) *Composite product evaluation for smart cards and similar devices for CC3.1* (Hodnocení složených produktů pro čipové karty a podobná zařízení pro CC3.1), verze 2;
      8) *Composite product evaluation and certification for CC:2022* (Hodnocení a certifikace složených produktů pro CC:2022), verze 1;
      9) *Application of Attack Potential to Smartcards and Similar Devices* (Uplatnění potenciálu útoku na čipové karty a podobná zařízení), verze 2;
      10) *Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices* (Bezpečnostní hodnocení a certifikace prostředků pro vytváření kvalifikovaných elektronických podpisů/pečetí), verze 1;
      11) *ADV_SPM.1 interpretation for CC:2022 transition* (Výklad ADV_SPM.1 pro přechod na CC:2022), verze 1.1, k použití pro certifikační procesy používající tyto profily ochrany:
         a) profily ochrany *Security IC Platform PP with Augmentation Packages* (profil ochrany pro bezpečnostní platformu IC s rozšiřujícími balíky) (v1.0), BSI-CC-PP-0084–2014, nebo *Java Card System – Closed Configuration* (systém Java Card – uzavřená konfigurace) (v3.1), BSI-CC-PP-0101-V2–2020, u procesů zahájených před 1. říjnem 2026;
         b) profil ochrany *Java Card System – Open Configuration* (systém Java Card – otevřená konfigurace) (v3.1), BSI-CC-PP-0099-V2–2020, u procesů zahájených před 29. prosincem 2025;
   b) následující dokumenty týkající se harmonizovaného hodnocení technické oblasti „hardwarová zařízení s bezpečnostními schránkami“:
      1) *Minimum ITSEF requirements for security evaluations of hardware devices with security boxes* (Minimální požadavky na bezpečnostní hodnocení hardwarových zařízení s bezpečnostními schránkami vůči zařízením ITSEF), verze 1.1;
      2) *Minimum Site Security Requirements* (Minimální bezpečnostní požadavky na lokalitu), verze 2;
      3) *Reusing evaluation results of site audits* (STAR) (Opětovné použití výsledků hodnocení z auditů na místě (STAR)), verze 1;
      4) *Application of Attack Potential to hardware devices with security boxes* (Uplatnění potenciálu útoku na hardwarová zařízení s bezpečnostními schránkami), verze 2;
      5) *Hardware assessment in EN 419221-5 (HSM PP)* (Hodnocení hardwaru v normě EN 419221-5 (HSM PP)), verze 1;
      6) *JIL Tachograph MS PP Clarification* (Objasnění JIL pro profil ochrany pro tachografy – snímače pohybu (MS PP)), verze 1.
2. Přehledy aktuálních certifikačních postupů týkající se harmonizované akreditace subjektů posuzování shody:
   a) *Accreditation of ITSEFs for the EUCC* (Akreditace zařízení ITSEF pro systém EUCC), verze 1.1 pro akreditace vydané před 8. červencem 2025;
   b) *Accreditation of ITSEFs for the EUCC* (Akreditace zařízení ITSEF pro systém EUCC), verze 1.6c pro akreditace, které jsou nově vydané nebo přezkoumané po 8. červenci 2025;
   c) *Accreditation of CBs for the EUCC* (Akreditace certifikačních subjektů pro systém EUCC), verze 1.6b.“

PŘÍLOHA II

„PŘÍLOHA II

Profily ochrany certifikované na úrovni AVA_VAN 4 nebo 5

1. Pro prostředky pro vytváření kvalifikovaných podpisů a pečetí na dálku:

   a) *EN 419241-2:2019 – Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing* (EN 419241-2:2019 – Důvěryhodné systémy podporující podpisový server – Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis) (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) *EN 419221-5:2018 – Protection profiles for Trust Service Provider Cryptographic modules – Part 5: Cryptographic Module for Trust Services* (EN 419221-5:2018 – Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby) (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Profily ochrany, které byly přijaty jako přehledy aktuálních certifikačních postupů:

   [PRÁZDNÉ].“

PŘÍLOHA III

„PŘÍLOHA III

Doporučené profily ochrany

Profily ochrany používané při certifikaci produktů IKT, včetně produktů v technických oblastech:

1. čipové karty a podobná zařízení
   a) cestovní pas:
      1) *PP Machine Readable Travel Document with „ICAO Application" Basic Access Control* (profil ochrany pro strojově čitelný cestovní doklad se základní kontrolou přístupu „aplikace ICAO") (v1.10), BSI-CC-PP-0055-2009;
      2) *PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP)* (profil ochrany pro strojově čitelný cestovní doklad s použitím standardního kontrolního postupu 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 pro strojově čitelný cestovní doklad s rozšířenou kontrolou přístupu „aplikace ICAO" s PACE) (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   b) prostředky pro vytváření bezpečného podpisu:
      1) *EN 419211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation* (EN 419211-2:2013 – Profily ochrany pro prostředky pro vytváření bezpečného podpisu – část 2: Zařízení na generování klíče) (v1.03), BSI-CC-PP-0059–2009-MA-02;
      2) *EN 419211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import* (EN 419211-3:2013 – Profily ochrany pro prostředky pro vytváření bezpečného podpisu – část 3: Zařízení pro importování klíče) (v1.0.2), BSI-CC-PP-0075–2012-MA-01;
      3) *EN 419211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application* (EN 419211-4:2013 – Profily ochrany pro prostředky pro vytváření bezpečného podpisu – část 4: Rozšíření pro zařízení na generování klíče a spolehlivá komunikace s aplikací generování certifikátu) (v1.0.1), BSI-CC-PP-0071–2012-MA-01;
      4) *EN 419211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application* (EN 419211-5:2013 – Profily ochrany pro prostředky pro vytváření bezpečného podpisu – část 5: Rozšíření pro zařízení na generování klíče a spolehlivá komunikace s aplikací vytvářející podpis) (v1.0.1), BSI-CC-PP-0072–2012-MA-01;
      5) *EN 419211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application* (EN 419211-6:2014 – Profily ochrany pro prostředky pro vytváření bezpečného podpisu – část 6: Rozšíření pro zařízení pro importování klíče a spolehlivá komunikace s aplikací vytvářející podpis) (v1.0.4), BSI-CC-PP-0076–2013-MA-01;
   c) tachograf: *Digital Tachograph – Tachograph Card (TC PP)* (digitální tachograf – karta tachografu (TC PP)) (v1.0), BSI-CC-PP-0091–2017;
   d) bezpečnostní platforma IC, Java Card a eUICC:
      1) *Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations* (profil ochrany pro univerzální SIM Java Card, konfigurace základní a SCWS) (v2.0.2), ANSSI-CC-PP-2010/04 (základní), ANSSI-CC-PP-2010/05 (základní a SCWS);
      2) *Security IC Platform PP with Augmentation Packages* (profil ochrany pro bezpečnostní platformu IC s rozšiřujícími balíky) (v1.0), BSI-CC-PP-0084–2014;
      3) *Embedded UICC (eUICC) for Machine-to-Machine Devices* (vestavěné UICC (eUICC) pro zařízení pro komunikaci strojů) (v1.1), BSI-CC-PP-0089-2015;
      4) *Cryptographic Service Provider – CSP* (poskytovatel kryptografických služeb – CSP) (v0.9.8), BSI-CC-PP-0104–2019;
      5) *Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)* (poskytovatel kryptografických služeb – služba časového razítka a audit (PPC-CSP-TS-Au)) verze 0.9.5, BSI-CC-PP-0107–2019;
      6) *Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl)* (poskytovatel kryptografických služeb – služba časového razítka, audit a klastrování (PPC-CSP-TS-Au-Cl)) verze 0.9.4, BSI-CC-PP-0108–2019;
      7) *Java Card System – Closed Configuration* (systém Java Card – uzavřená konfigurace) (v3.1), BSI-CC-PP-0101-V2-2020;
      8) *Secure Element Protection Profile – GPC_SPE_174* (profil ochrany pro bezpečné prvky – GPC_SPE_174) (v1.0), CCN-CC-PP-5–2021;
      9) *Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile* (profil ochrany pro zabezpečené dílčí systémy v systémech na čipu (3S in SoC)) (v1.8), BSI-CC-PP-0117-V2–2023;
      10) *Java Card System – Open Configuration* (systém Java Card – otevřená konfigurace) (v3.2), BSI-CC-PP-0099-V3-2024;
      11) *Embedded UICC for Consumer Devices Protection Profile* (profil ochrany pro vestavěné UICC pro spotřebitelská zařízení) (v2.1), BSI-CC-PP-0100-V2–2025;
   e) modul důvěryhodné platformy: *Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0* (profil ochrany pro rodinu specifikací modulů důvěryhodné platformy 2.0 specifických pro klientskou platformu PC; úroveň 0); revize 1.59 (v1.3), ANSSI-CC-PP-2021/02;

2. hardwarová zařízení s bezpečnostními schránkami

   a) body (platební) interakce a platební terminály (POI):

      1) bod interakce „POI-CHIP-ONLY“ (v4.0), ANSSI-CC-PP-2015/01;

      2) bod interakce „POI-CHIP-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/02;

      3) bod interakce „POI-COMPREHENSIVE“ (v4.0), ANSSI-CC-PP-2015/03;

      4) bod interakce „POI-COMPREHENSIVE and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/04;

      5) bod interakce „POI-PED-ONLY“ (v4.0), ANSSI-CC-PP-2015/05;

      6) bod interakce „POI-PED-ONLY and Open Protocol Package“ (v4.0), ANSSI-CC-PP-2015/06;

   b) hardwarový bezpečnostní modul:

      1) *Cryptographic Module for CSP Signing Operations with Backup* (kryptografický modul pro podpisové operace CSP se zálohováním) – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;

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

      3) *Cryptographic Module for CSP Signing Operations without Backup* (kryptografický modul pro podpisové operace CSP bez zálohování) – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

   c) tachograf:

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

      2) *Digital Tachograph – Vehicle Unit (VU PP)* (digitální tachograf – celek ve vozidle (VU PP)) (v1.15), BSI-CC-PP-0094-V2–2021;

      3) *Digital Tachograph – External GNSS Facility (EGF PP)* (digitální tachograf – vnější zařízení GNSS (EGF PP)) (v1.10), BSI-CC-PP-0092-V2–2021.

3. jiné: *Trusted Execution Environment Protection Profile* (profil ochrany pro důvěryhodné spouštěcí prostředí) – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.“

PŘÍLOHA IV

Příloha IV prováděcího nařízení (EU) 2024/482 se mění takto:

1. v bodě IV.2 se podbod 4 nahrazuje tímto:

„4. Certifikační subjekt přezkoumá aktualizovanou hodnotící technickou zprávu a vypracuje zprávu o přehodnocení. Status původního certifikátu se poté změní v souladu s článkem 13 nebo článkem 19. Pokud je proces přehodnocení úspěšný, použije se čl. 13 odst. 2 písm. a) nebo c) v případě certifikace produktu a čl. 19 odst. 2 písm. a) nebo c) v případě certifikace profilu ochrany. Pokud je proces přehodnocení neúspěšný, použije se čl. 13 odst. 2 písm. b) nebo d) v případě certifikace produktu a čl. 19 odst. 2 písm. b) nebo d) v případě certifikace profilu ochrany.“;

2. bod IV.3 se mění takto:

a) název bodu IV.3 se nahrazuje tímto:

„IV.3 **Změny certifikovaného produktu IKT – zachování a přehodnocení“;**

b) podbody 4 a 5 se nahrazují tímto:

„4. Po přezkoumání certifikační subjekt určí rozsah změny jako drobný nebo velký podle jejího dopadu na záruku vyjádřenou certifikátem EUCC.

5. Pokud certifikační subjekt potvrdí, že změny jsou drobné, nevydává se v souladu s čl. 13 odst. 2 písm. a) nebo čl. 19 odst. 2 písm. a) pro pozměněný produkt IKT nový certifikát a k původní zprávě o certifikaci se vypracuje zpráva o zachování.“;

c) vkládá se nový bod 5a, který zní:

„5a. V případě jakýchkoli změn opatření pro zajištění záruky ve vývojovém prostředí, včetně doplnění požadavků na záruku z rodiny CC ALC_FLR (odstranění nedostatků), může certifikační orgán požádat zařízení ITSEF o provedení dílčího hodnocení dotčených opatření pro zajištění záruky. Zařízení ITSEF vydá technickou zprávu o částečném hodnocení, na jejímž základě certifikační subjekt potvrdí, že změny jsou buď drobné, nebo velké. Pokud certifikační subjekt potvrdí, že změny jsou drobné, použije se příloha IV.3 podbod 5. Pokud certifikační subjekt potvrdí, že změny jsou velké, použije se příloha IV.3 podbod 7.“

PŘÍLOHA V

V příloze V prováděcího nařízení (EU) 2024/482 se bod V.1 nahrazuje tímto:

„V.1 **Zpráva o certifikaci**

1. Na základě hodnotících technických zpráv poskytnutých zařízením ITSEF vypracuje certifikační subjekt zprávu o certifikaci, kterou zveřejní spolu s příslušným certifikátem EUCC a bezpečnostním cílem.

2. Zpráva o certifikaci je zdrojem podrobných a praktických informací o produktu IKT a o bezpečném nasazení produktu IKT. Musí proto obsahovat všechny veřejně dostupné informace, které lze sdílet a které jsou důležité pro uživatele a zúčastněné strany. Veřejně dostupné informace, které lze sdílet, mohou být ve zprávě o certifikaci uvedeny odkazem.

3. Zpráva obsahuje přinejmenším tyto informace:
   a) shrnutí;
   b) identifikace produktu IKT;
   c) kontaktní údaje související s hodnocením produktu IKT;
   d) bezpečnostní politiky;
   e) předpoklady a objasnění oblasti působnosti;
   f) informace o architektuře;
   g) případné doplňující informace o kybernetické bezpečnosti;
   h) shrnutí hodnocení produktu IKT a hodnocená konfigurace;
   i) výsledky hodnocení a informace o certifikátu;
   j) případné připomínky a doporučení;
   k) případné přílohy;
   l) odkaz na bezpečnostní cíl produktu IKT předloženého k certifikaci;
   m) označení nebo štítek přiřazené systému, jsou-li k dispozici;
   n) případně glosář;
   o) bibliografie.

4. Shrnutí uvedené v podbodě 3 písm. a) je stručným shrnutím celé zprávy o certifikaci. Poskytuje jasný a stručný přehled výsledků hodnocení a obsahuje následující informace:
   a) název hodnoceného produktu IKT;
   b) název zařízení ITSEF, které hodnocení provedlo;
   c) datum ukončení hodnocení;
   d) datum vydání certifikátu;
   e) v příslušných případech datum vydání původního certifikátu;
   f) doba platnosti;
   g) jedinečná identifikace certifikátu, jak je popsána v článku 11;
   h) stručný popis výsledků zprávy o certifikaci, včetně těchto informací:
      i) verze a případně vydání společných kritérií, která se na hodnocení vztahují;
      ii) balíček záruk podle společných kritérií nebo seznam složek bezpečnostní záruky, úroveň AVA_VAN použitá při hodnocení a odpovídající úroveň záruky podle článku 52 nařízení (EU) 2019/881, na kterou certifikát EUCC odkazuje;
      iii) v příslušných případech profil (profily) ochrany, s nímž (s nimiž) je produkt IKT podle prohlášení v souladu;
      iv) odkaz na bezpečnostní politiku hodnoceného produktu IKT;
      v) v příslušných případech prohlášení o vyloučení odpovědnosti.

5. Identifikace uvedená v podbodu 3 písm. b) spočívá v jasné identifikaci hodnoceného produktu IKT, včetně těchto informací:

   a) jedinečná identifikace hodnoceného produktu IKT;

   b) výčet součástí produktu IKT, které jsou předmětem hodnocení, s číslem verze každé součásti;

   c) odkaz na dodatečné požadavky na provozní prostředí certifikovaného produktu IKT.

6. Kontaktní údaje uvedené v podbodu 3 písm. c) obsahují alespoň tyto informace:

   a) jméno vývojáře;

   b) jméno a kontaktní údaje držitele certifikátu EUCC;

   c) název certifikačního subjektu, který certifikát vydal;

   d) odpovědný vnitrostátní orgán certifikace kybernetické bezpečnosti;

   e) název zařízení ITSEF, které hodnocení provedlo, a v příslušných případech seznam subdodavatelů.

7. Bezpečnostní politika uvedená v podbodu 3 písm. d) obsahuje popis bezpečnostní politiky produktu IKT jako souboru bezpečnostních služeb a politiky nebo pravidla, která hodnocený produkt IKT prosazuje nebo dodržuje. Obsahuje také tyto informace:

   a) popis postupů držitele certifikátu pro řízení zranitelností a jejich zveřejňování, který obsahuje pouze informace, jež mohou být zveřejněny;

   b) strategie kontinuity záruky držitele certifikátu, případně včetně popisu procesů řízení životního cyklu nebo produkčních procesů držitele certifikátu v souladu s oddílem IV.1 přílohy IV;

   c) v příslušných případech existence postupu správy oprav a výsledek jeho posouzení v souladu s oddílem IV.4 přílohy IV.

8. Předpoklady a objasnění oblasti působnosti uvedené v podbodu 3 písm. e) obsahují informace o okolnostech a cílech souvisejících se zamýšleným použitím produktu podle čl. 7 odst. 1 písm. c) a zahrnují tyto informace:

   a) předpoklady o použití a nasazení produktu IKT v podobě minimálních požadavků, jako je správná instalace a konfigurace a splnění požadavků na hardware;

   b) předpoklady o prostředí pro vyhovující provoz produktu IKT;

   c) popis hrozeb pro produkt IKT, které nejsou řešeny hodnocenými bezpečnostními funkcemi produktu, podle zamýšleného použití, je-li to považováno za relevantní pro potenciálního uživatele produktu IKT.

   Informace uvedené v prvním pododstavci musí být co nejjasnější a nejsrozumitelnější, aby potenciálním uživatelům certifikovaného produktu IKT umožnily přijímat informovaná rozhodnutí o rizicích spojených s jeho používáním.

9. Informace o architektuře uvedené v podbodu 3 písm. f) zahrnují obecný popis produktu IKT a jeho hlavních součástí na základě výstupů definovaných ve společných kritériích pro rodinu záruk Vývoj – design cíle hodnocení (ADV_TDS).

10. Doplňující informace o kybernetické bezpečnosti uvedené v podbodu 3 písm. g) obsahují odkaz na internetové stránky držitele certifikátu EUCC podle článku 55 nařízení (EU) 2019/881.

11. Hodnocení a konfigurace produktu IKT uvedené v podbodu 3 písm. h) popisuje testovací činnosti vývojáře i hodnotitele, nastiňuje přístup k testování, jeho konfiguraci a hloubku. Obsahuje alespoň tyto informace:

    a) identifikace použitých složek záruky z norem uvedených v článku 3;

    b) verze přehledů aktuálních certifikačních postupů a další kritéria hodnocení bezpečnosti použitá při hodnocení;

    c) nastavení a konfigurace cíle hodnocení použité pro testování a analýzu zranitelností;

    d) jakýkoli použitý profil ochrany, včetně následujících informací: název, verze, datum a certifikát profilu ochrany.

12. Výsledky hodnocení a informace týkající se certifikátu uvedené v podbodu 3 písm. i) zahrnují informace o dosažené úrovni záruky podle článku 4 tohoto nařízení a článku 52 nařízení (EU) 2019/881.

13. Připomínky a doporučení uvedené v podbodu 3 písm. j) se používají ke sdělení dodatečných informací o výsledcích hodnocení. Mohou se týkat nedostatků produktu IKT, které byly zjištěny během hodnocení, nebo zmiňovat prvky, které jsou obzvláště užitečné.

14. Přílohy uvedené v podbodu 3 písm. k) se používají k shrnutí jakýchkoli dalších informací, které mohou být pro čtenáře zprávy užitečné, ale logicky nespadají do předepsaných oddílů zprávy, a to i v případech úplného popisu bezpečnostní politiky.

15. Bezpečnostní cíl uvedený v podbodu 3 písm. l) odkazuje na hodnocený bezpečnostní cíl. Hodnocený bezpečnostní cíl se poskytne společně se zprávou o certifikaci pro účely zveřejnění na internetových stránkách podle čl. 50 odst. 1 nařízení (EU) 2019/881. Pokud je před zveřejněním nutná sanitizace hodnoceného bezpečnostního cíle, provede se v souladu s bodem V.2 přílohy V tohoto nařízení.

16. Označení nebo štítky spojené se systémem EUCC uvedené v podbodu 3 písm. m) se vloží do zprávy o certifikaci v souladu s pravidly a postupy stanovenými v článku 11.

17. Glosář uvedený v podbodu 3 písm. n) se používá ke zvýšení srozumitelnosti zprávy, neboť poskytuje definice zkratek nebo termínů, jejichž význam nemusí být zjevný.

18. Bibliografie uvedená v podbodu 3 písm. o) obsahuje odkazy na všechny dokumenty použité při sestavování zprávy o certifikaci. Jedná se alespoň o tyto dokumenty:

    a) kritéria hodnocení bezpečnosti, přehledy aktuálních certifikačních postupů a další použité relevantní specifikace;

    b) hodnotící technická zpráva;

    c) v příslušných případech hodnotící technická zpráva pro hodnocení složených produktů;

    d) technická referenční dokumentace;

    e) bezpečnostní pokyny vývojáře;

    f) seznam konfigurací vývojáře.

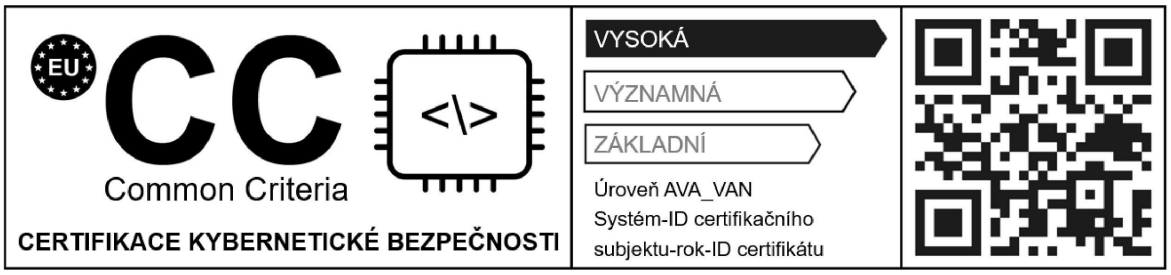
    Aby byla zaručena reprodukovatelnost hodnocení, musí být veškerá dokumentace, na kterou se odkazuje, jednoznačně identifikována správným datem vydání a správným číslem verze.“

PŘÍLOHA VI

„PŘÍLOHA IX

Označení a štítek

1. Podoba označení a štítku:



2. Pokud jsou označení a štítek zmenšeny nebo zvětšeny, musí být dodrženy proporce zobrazené v bodě 1.

3. Pokud jsou označení a štítek fyzicky přítomny, musí být vysoké nejméně 5 mm.“