Uradni list
Evropske unije

SL
Serija L

2025/2462

9.12.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/2462

z dne 8. decembra 2025

o spremembi Izvedbene uredbe (EU) 2024/482 glede opredelitev pojmov, certificiranja serij proizvodov IKT, neprekinjene zanesljivosti in najsodobnejših dokumentov

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (Agencija ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) ([1]) in zlasti člena 49(7) Uredbe,

ob upoštevanju naslednjega:

(1) Izvedbena uredba Komisije (EU) 2024/482 ([2]) določa vloge, pravila in obveznosti ter strukturo evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (v nadaljnjem besedilu: EUCC) v skladu z evropskim certifikacijskim okvirom za kibernetsko varnost iz Uredbe (EU) 2019/881.

(2) Skupna metodologija ocenjevanja, ki spremlja skupna merila, mednarodni standard za ocenjevanje informacijske varnosti, omogoča ocenjevanje varnosti proizvodov IKT za namene certificiranja. V tem okviru se lahko nekateri proizvodi IKT, imenovani tudi serija proizvodov, oblikujejo na enaki funkcionalni osnovi, da bi nudili podobne varnostne funkcionalnosti na različnih platformah ali napravah. Vendar se lahko zasnova, strojna oprema, strojna programska oprema ali programska oprema posameznih proizvodov IKT razlikujejo. Certifikacijski organ mora za vsak primer posebej odločiti, ali se serija proizvodov lahko certificira. Pogoje za certificiranje serij proizvodov bi lahko dodatno ponazorile podporne smernice o EUCC.

(3) Za ohranitev zanesljivosti certificiranih proizvodov je bistveno opredeliti, kaj predstavlja večjo in kaj manjšo spremembo cilja ocenjevanja ali njegovega okolja, vključno z operativnim ali razvojnim okoljem. Zato je treba navedene pojme opredeliti ob upoštevanju obstoječih in splošno uporabljanih tehničnih specifikacij skupine visokih uradnikov za varnost informacijskih sistemov in udeležencev dogovorov o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT.

(4) Za manjše spremembe je pogosto značilen omejen učinek na izjavo o zanesljivosti proizvoda, ki jo zagotavlja izdani certifikat EUCC. Zato bi bilo treba manjše spremembe upravljati v okviru postopkov vzdrževanja in zanje ni potrebno ponovno ocenjevanje varnostnih funkcionalnosti proizvoda. Primeri manjših sprememb, ki bi jih bilo treba obravnavati z vzdrževanjem, med drugim vključujejo redakcijske spremembe, spremembe cilja ocenjevalnega okolja, ki ne spreminjajo certificiranega cilja ocenjevanja, in spremembe certificiranega cilja ocenjevanja, ki ne vplivajo na dokaze o zanesljivosti. Tudi spremembe razvojnega okolja se lahko štejejo za manjše, če nimajo nadaljnjega učinka na obstoječe ukrepe glede zanesljivosti. Vendar lahko v nekaterih primerih zahtevajo delno ocenjevanje ustreznih ukrepov.

([1]) UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
([2]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Večja sprememba je vsaka sprememba certificiranega cilja ocenjevanja ali njegovega okolja, ki bi lahko negativno vplivala na zanesljivost, izraženo v certifikatu EUCC, in bi zato moralo biti potrebno ponovno ocenjevanje. Primeri večjih sprememb med drugim vključujejo spremembe sklopa zahtevanih zahtev glede zanesljivosti, razen zahtev glede zanesljivosti iz družine CC ALC_FLR (odprava napak); spremembe kontrol zaupnosti ali celovitosti razvojnega okolja, kadar bi take spremembe lahko vplivale na varen razvoj ali proizvodnjo cilja ocenjevanja, ali spremembe cilja ocenjevanja za odpravo šibke točke, ki jo je mogoče izkoristiti. Poleg tega se lahko kot večja sprememba opredeli tudi nabor manjših sprememb, ki skupaj pomembno vplivajo na varnost. Pomembno je tudi priznati, da lahko odprava programske napake sicer vpliva le na določen vidik cilja ocenjevanja, vendar lahko zaradi nepredvidljivosti in morebitnega vpliva na zanesljivost postane velika sprememba, če ogroža zagotavljanje varnosti, ki jo zagotavlja certificiranje.

(6) Spremembe okolja groženj nespremenjenega certificiranega proizvoda IKT bi lahko zahtevale ponovno oceno. Jasno bi bilo treba določiti možne rezultate takega postopka ponovne ocene, zlasti njegov vpliv na certifikat EUCC. Če je ponovna ocena uspešno zaključena, mora certifikacijski organ potrditi certifikat ali izdati nov certifikat s podaljšanim datumom poteka veljavnosti. Če postopek ponovne ocene ni uspešen, bi moral certifikacijski organ preklicati certifikat in po možnosti izdati nov certifikat z drugačnim področjem uporabe. Take določbe bi se morale smiselno uporabljati za ponovno oceno profilov zaščite.

(7) V Prilogi I k Izvedbeni uredbi (EU) 2024/482 so navedeni veljavni najsodobnejši dokumenti za ocenjevanje proizvodov IKT in profilov zaščite. Te najsodobnejše dokumente bi bilo treba posodobiti, da bi odražali najnovejši razvoj, kot je tisti, povezan s tehnološkim razvojem, okoljem kibernetskih groženj, industrijskimi praksami ali mednarodnimi standardi. Taka posodobitev je primerna za najsodobnejše dokumente v zvezi z minimalnimi varnostnimi zahtevami za lokacijo, uporabo potenciala napada na pametne kartice, uporabo potenciala napada na naprave strojne opreme z varnostnimi napravami, uporabo skupnih meril za integrirana vezja in ocenjevanje sestavljenih proizvodov za pametne kartice in podobne naprave. Poleg tega niso vključeni najsodobnejši dokumenti v zvezi z vrednotenjem in certificiranjem sestavljenih proizvodov z uporabo najnovejše različice standardov skupnih meril, ponovna uporaba rezultatov revizij na kraju samem in pojasnila o razlagi profilov zaščite v zvezi z napravami za ustvarjanje kvalificiranega elektronskega podpisa, tahografi in varnostnimi moduli strojne opreme. Za zagotovitev enotnega ocenjevanja proizvodov IKT v okviru EUCC bi bilo treba spremeniti Prilogo I, da se vključijo ti posodobljeni in novi najsodobnejši dokumenti po njihovi potrditvi s strani evropske certifikacijske skupine za kibernetsko varnost.

(8) Poleg tega bi bilo treba shemi dodati najsodobnejši dokument „Razlaga ADV_SPM.1 za prehod na CC:2022“, da se zagotovi, da se lahko postopki certificiranja, ki temeljijo na posebnih profilih zaščite, še naprej uporabljajo z uradnim modeliranjem (ADV_SPM.1), dokler se ne posodobijo ustrezni profili zaščite, na primer z dodatkom konfiguracije profila več ravni zanesljivosti v skladu s CC:2022, ki podpira ADV_SPM.1. Da bi trgu zagotovili dovolj časa za prehod na posodobljene standarde skupnih meril, je treba predvideti posebna pravila o prehodu za profile zaščite za platformo z varnostnim integriranim vezjem z dopolnilnimi paketi (v1.0), BSI-CC-PP-0084-2014, sistem Java kartice – zaprta konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020, ali sistem Java kartice – odprta konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020. Da bi se izognili motnjam na trgu, je primerno določiti, da se najsodobnejši dokument o razlagi ADV_SPM.1 za prehod na CC:2022 uporablja za postopke certificiranja, ki so se začeli pred sprejetjem te uredbe. Vendar bi morala biti uporaba tega dokumenta strogo omejena na to, kar je potrebno, ob upoštevanju časa, ki je potreben za dokončanje posodobitve ustreznih profilov zaščite. Natančneje, za postopke certificiranja, pri katerih se uporabljajo profili zaščite za platformo z varnostnim integriranim vezjem z dopolnilnimi paketi (v1.0), BSI-CC-PP-0084-2014, ali sistem Java kartice – zaprta konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020, bi se moral najsodobnejši dokument uporabljati za tiste postopke, ki so se začeli pred 1. oktobrom 2026. Za postopke certificiranja, pri katerih se uporablja profil zaščite za sistem Java kartice – odprta konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020, bi se moral najsodobnejši dokument uporabljati le za postopke, ki so se začeli pred datumom začetka veljavnosti te uredbe, saj je nova različica profila zaščite sistem Java kartice – odprta konfiguracija že na voljo.

(9) Sprememba najsodobnejših dokumentov med postopkom certificiranja bi lahko ovirala ocenjevanje proizvoda in odložila izdajo certifikata. Zato so potrebna ustrezna prehodna pravila za nove ali posodobljene najsodobnejše dokumente, da bi lahko prodajalci, centri za ocenjevanje varnosti informacijske tehnologije, certifikacijski organi in drugi deležniki izvedli potrebne prilagoditve. Veljavni posodobljeni in novi najsodobnejši dokumenti bi se morali nanašati na vloge za certificiranje, vključno z vlogami za ponovno oceno in ponovno vrednotenje, medtem ko bi moralo biti omogočeno, da se za tekoče postopke certificiranja uporabljajo prejšnje različice najsodobnejših dokumentov.

(10) V Prilogi II in Prilogi III k Izvedbeni uredbi (EU) 2024/482 so navedeni profili zaščite, certificirani na ravneh 4 ali 5 AVA_VAN, in priporočeni profili zaščite. Več sklicev je zaradi posodobitve profilov zaščite nepopolnih ali zastarelih. Navedena sklicevanja bi bilo treba dopolniti, poleg tega pa vključiti nova, da se zagotovi celovitejša pokritost varnih integriranih vezij, pametnih kartic in sorodnih naprav ter zaupanja vrednega računalništva.

(11) Treba je spremeniti člen 19 Izvedbene uredbe (EU) 2024/482, da se pojasni, da se Priloga IV s potrebnimi spremembami uporablja za pregled certifikatov EUCC za profile zaščite.

(12) Ker je varnostni cilj ključni element za razumevanje obsega postopka certificiranja, mora Agencija ENISA na svojem spletišču objaviti tudi varnostni cilj, ki ustreza vsakemu certifikatu EUCC.

(13) Poleg tega bi morali certifikacijski organi Agenciji ENISA zagotoviti angleško različico varnostnega cilja in poročilo o certificiranju, da bi lahko te informacije v skladu s členom 42(2) Izvedbene uredbe (EU) 2024/482 dala na voljo v angleščini na ustreznem spletišču. Zato bi morali vložniki vloge za certificiranje certifikacijskim organom, kadar koli se to zahteva, zagotoviti angleško različico varnostnega cilja.

(14) Ni nujno, da se sklic na ime certifikacijskega organa pojavi v edinstvenem identifikatorju certifikata, saj identifikacijska številka certifikacijskega organa zadostuje za edinstveno identifikacijo tega organa. Prav tako ni treba navesti meseca izdaje, saj se certifikati štejejo vsako leto posebej. Zato bi bilo treba to zahtevo zaradi poenostavitve črtati. Ker leto izdaje certifikata ustreza izdaji prvega certifikata, bi moral biti isti datum naveden v edinstveni identifikaciji na certifikatih, izdanih po pregledu, da se zagotovi sledljivost.

(15) Izvedbeno uredbo (EU) 2024/482 bi bilo zato treba ustrezno spremeniti.

(16) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega s členom 66 Uredbe (EU) 2019/881 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Izvedbena uredba (EU) 2024/482 se spremeni:

(1) v členu 2 se dodajo naslednje točke (16), (17) in (18):

„(16) ‚serija proizvodov‘ pomeni sklop proizvodov IKT, ki ga pripravi vložnik in ima isto funkcionalno podlago, da bi zadostil istim varnostnim potrebam, z zasnovo, strojno opremo, strojno programsko opremo ali programsko opremo, ki se lahko med posameznimi proizvodi IKT razlikuje;

(17) ‚manjša sprememba‘ pomeni vsako spremembo certificiranega cilja ocenjevanja ali njegovega okolja, ki ne vpliva negativno na zanesljivost, izraženo v certifikatu EUCC;

(18) ‚večja sprememba‘ pomeni vsako spremembo certificiranega cilja ocenjevanja ali njegovega okolja, ki bi lahko negativno vplivala na zanesljivost, izraženo v certifikatu EUCC.“;

(2) v členu 5 se doda naslednji odstavek 3:

„3. Certifikacijski organ lahko dovoli certificiranje serije proizvodov.“;

(3) v členu 9, odstavek (2), se točka (a) nadomesti z naslednjim:

„(a) certifikacijskemu organu in centru za ocenjevanje varnosti informacijske tehnologije zagotoviti vse potrebne popolne in točne informacije, na zahtevo pa tudi dodatne potrebne informacije, vključno z angleško različico varnostnega cilja;“;

(4) v členu 11, odstavek 3, se točka (b) nadomesti z naslednjim:

„(b) enotno identifikacijo certifikata, ki vsebuje:

(1) ime sheme;

(2) identifikacijsko številko certifikacijskega organa, ki je izdal certifikat, v skladu s členom 3 Izvedbene uredbe (EU) 2024/3143;

(3) leto izdaje prvotnega certifikata;

(4) identifikacijsko številko, ki jo dodeli certifikacijski organ, ki je izdal certifikat.“;

(5) v členu 19 se odstavek 1 nadomesti z naslednjim:

„1. Certifikacijski organ se lahko na zahtevo imetnika certifikata ali iz drugih utemeljenih razlogov odloči pregledati certifikat EUCC za profil zaščite. Pregled se opravi v skladu s Prilogo IV. Certifikacijski organ določi obseg pregleda. Kadar je to potrebno za pregled, od centra za ocenjevanje varnosti informacijske tehnologije zahteva, da ponovno oceni certificirani profil zaščite.“;

(6) člen 42 se spremeni:

(a) v odstavku 1 se doda naslednja točka (i):

„(i) varnostni cilj, ki ustreza vsakemu certifikatu EUCC.“;

(b) odstavek 2 se nadomesti z naslednjim:

„2. Informacije iz odstavka 1 se dajo na voljo vsaj v angleščini. V ta namen certifikacijski organi Agenciji ENISA predložijo izvirne jezikovne različice poročil o certificiranju in varnostnih ciljev, poleg tega pa brez nepotrebnega odlašanja zagotovijo tudi angleško različico takih dokumentov.“;

(7) v členu 48 se odstavek 4 nadomesti z naslednjim:

„4. Če v Prilogi I ali II ni določeno drugače, se najsodobnejši dokumenti uporabljajo za postopke certificiranja, vključno s ponovnim ocenjevanjem in ponovnim vrednotenjem, od datuma začetka uporabe akta o spremembi, s katerim so bili najsodobnejši dokumenti vključeni v Prilogo I ali II.“;

(8) Priloga I se nadomesti z besedilom iz Priloge I k tej uredbi;

(9) Priloga II se nadomesti z besedilom iz Priloge II k tej uredbi;

(10) Priloga III se nadomesti z besedilom iz Priloge III k tej uredbi;

(11) Priloga IV se spremeni v skladu s Prilogo IV k tej uredbi;

(12) Priloga V se spremeni v skladu s Prilogo V k tej uredbi;

(13) Priloga IX se nadomesti z besedilom iz Priloge VI k tej uredbi.

Člen 2

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. decembra 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

„PRILOGA I

Najsodobnejši dokumenti za tehnična področja in drugi najsodobnejši dokumenti

1. Najsodobnejši dokumenti za tehnična področja na ravni 4 ali 5 AVA_VAN:

   (a) naslednji dokumenti, povezani s harmoniziranim ocenjevanjem tehnične domene ‚Pametne kartice in podobne naprave‘:

      (1) ‚Minimalne zahteve centra za ocenjevanje varnosti informacijske tehnologije za ocenjevanje varnosti pametnih kartic in podobnih naprav‘, različica 1.1;

      (2) ‚Minimalne varnostne zahteve za lokacijo‘, različica 2;

      (3) ‚Ponovna uporaba rezultatov revizij na kraju samem (STAR)‘, različica 1;

      (4) ‚Uporaba skupnih meril za integrirana vezja‘, različica 2;

      (5) ‚Zahteve za varnostno arhitekturo (ADV_ARC) pametnih kartic in podobnih naprav‘, različica 1.1;

      (6) ‚Certificiranje ‚odprtih‘ proizvodov za pametne kartice‘, različica 1.1;

      (7) ‚Ocenjevanje sestavljenih proizvodov za pametne kartice in podobne naprave za CC3.1‘, različica 2;

      (8) ‚Vrednotenje in certificiranje sestavljenega proizvoda za CC:2022‘, različica 1;

      (9) ‚Uporaba potenciala napada na pametne kartice in podobne naprave‘, različica 2;

      (10) ‚Varnostno vrednotenje in certificiranje naprav za ustvarjanje kvalificiranega elektronskega podpisa/žiga‘, različica 1;

      (11) ‚Razlaga ADV_SPM.1 za prehod na CC:2022‘, različica 1.1, ki se uporablja za postopke certificiranja z uporabo naslednjih profilov zaščite:

         (a) profila zaščite za platformo z varnostnim integriranim vezjem z dopolnilnimi paketi (v1.0), BSI-CC-PP-0084-2014 ali sistem Java kartice – zaprta konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020, ki sta se začela izvajati pred 1. oktobrom 2026;

         (b) profila zaščite za sistem Java kartice – odprta konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020, ki se je začel izvajati pred 29. decembrom 2025;

   (b) naslednji dokumenti, povezani s harmoniziranim ocenjevanjem tehnične domene ‚Naprave strojne opreme z varnostnimi napravami‘:

      (1) ‚Minimalne zahteve centra za ocenjevanje varnosti informacijske tehnologije za ocenjevanje varnosti naprav strojne opreme z varnostnimi napravami‘, različica 1.1;

      (2) ‚Minimalne varnostne zahteve za lokacijo‘, različica 2;

      (3) ‚Ponovna uporaba rezultatov revizij na kraju samem (STAR)‘, različica 1;

      (4) ‚Uporaba potenciala napada na naprave strojne opreme z varnostnimi napravami‘, različica 2;

      (5) ‚Ocena strojne opreme v EN 419221-5 (HSM PP)‘, različica 1;

      (6) ‚Pojasnitev profila zaščite za tipalo gibanja za tahograf Jil‘, različica 1.

2. Najsodobnejši dokumenti, povezani s harmonizirano akreditacijo organov za ugotavljanje skladnosti:

   (a) ‚Akreditacija centrov za ocenjevanje varnosti informacijske tehnologije za EUCC‘, različica 1.1, za akreditacije, izdane pred 8. julijem 2025;

   (b) ‚Akreditacija centrov za ocenjevanje varnosti informacijske tehnologije za EUCC‘, različica 1.6c, za akreditacije, izdane prvič ali pregledane po 8. juliju 2025;

   (c) ‚Akreditacija certifikacijskih organov za EUCC‘, različica 1.6b.“.

PRILOGA II

„PRILOGA II

Profili zaščite, certificirani na ravni AVA_VAN 4 ali 5

1. Za naprave za ustvarjanje kvalificiranega podpisa in žiga na daljavo:

   (a) EN 419241-2:2019 – Zaupanja vredni sistemi, ki podpirajo strežniško podpisovanje – 2. del: Profil zaščite za QSCD za strežniško podpisovanje (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 – Profili zaščite za ponudnike storitev zaupanja za kriptografske module – 5. del: Kriptografski modul za storitve zaupanja (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Profili zaščite, ki so bili sprejeti kot najsodobnejši dokumenti:

   [PRAZNO].“.

PRILOGA III

„PRILOGA III

Priporočeni profili zaščite

Profili zaščite, ki se uporabljajo pri certificiranju proizvodov IKT, vključno s proizvodi na tehničnih področjih:

1. pametne kartice in podobne naprave:
   (a) potni list:
      (1) profil zaščite za strojno berljivo potno listino z „aplikacijo ICAO“ za osnovni nadzor dostopa (v1.10), BSI-CC-PP-0055-2009;
      (2) profil zaščite za strojno berljivo potno listino z uporabo standardnega postopka pregleda z vzpostavitvijo z geslom zaščitene povezave (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;
      (3) profil zaščite za strojno berljivo potno listino z „aplikacijo ICAO“ za razširjen nadzor dostopa z vzpostavitvijo z geslom zaščitene povezave (PACE) (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   (b) naprave za varno tvorjenje podpisa (SSCD):
      (1) EN 419211-2:2013 – Profil zaščite sredstva za varno elektronsko podpisovanje – 2. del: Naprava z ustvarjanjem ključa (v1.03), BSI-CC-PP-0059-2009-MA-02;
      (2) EN 419211-3:2013 – Profil zaščite sredstva za varno elektronsko podpisovanje – 3. del: Naprava z uvozom ključa (v1.0.2), BSI-CC-PP-0075-2012-MA-01;
      (3) EN 419211-4:2013 – Profil zaščite sredstva za varno elektronsko podpisovanje – 4. del: Podaljšek za sredstvo, ki ustv ariin zaupno komunicira prek aplikacije z ustvarjanjem (v1.0.1), BSI-CC-PP-0071-2012-MA-01;
      (4) EN 419211-5:2013 – Profil zaščite sredstva za varno elektronsko podpisovanje – 5. del: Podaljšek za sredstvo, ki ustvari ključ in zaupno komunicira prek aplikacije s podpisovanjem (v1.0.1), BSI-CC-PP-0072-2012-MA-01;
      (5) EN 419211-6:2014 – Profil zaščite sredstva za varno elektronsko podpisovanje – 6. del: Podaljšek za sredstvo, ki uvozi ključ in zaupno komunicira prek aplikacije s podpisovanjem (v1.0.4), BSI-CC-PP-0076-2013-MA-01;
   (c) tahograf: profil zaščite za digitalni tahograf – tahografska kartica (v1.0), BSI-CC-PP-0091-2017;
   (d) varno integrirano vezje, platforma Java kartice in eUICC:
      (1) univerzalni profil zaščite za platformo SIM Java kartice – osnovna konfiguracija in konfiguracija SCWS (v2.0.2), ANSSI-CC-PP-2010/04 (osnovna), ANSSI-CC-PP-2010/05 (osnovna in SCWS);
      (2) profil zaščite za platformo z varnostnim integriranim vezjem z dopolnilnimi paketi (v1.0), BSI-CC-PP-0084-2014;
      (3) vgrajena univerzalna pametna kartica za naprave z vzajemno povezavo med napravami (v1.1), BSI-CC-PP-0089-2015;
      (4) ponudnik kriptografskih storitev – CSP (v0.9.8), BSI-CC-PP-0104-2019;
      (5) ponudnik kriptografskih storitev – storitev časovnega žiga in revizija (PPC-CSP-TS-Au), različica 0.9.5, BSI-CC-PP-0107-2019;
      (6) ponudnik konfiguracije kriptografskih storitev – storitev časovnega žiga, revizija in združevanje (PPC-CSP-TS-Au), različica 0.9.4, BSI-CC-PP-0108-2019;
      (7) sistem Java kartice – zaprta konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020;
      (8) profil zaščite varnih elementov – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;
      (9) varen podsistem v profilu zaščite sistema na čipu (3S v SoC) (v1.8), BSI-CC-PP-0117-V2-2023;
      (10) sistem Java kartice – odprta konfiguracija (v3.2), BSI-CC-PP-0099-V3-2024;
      (11) vgrajena univerzalna pametna kartica za profil zaščite za potrošniške naprave (v2.1), BSI-CC-PP-0100-V2-2025;
   (e) modul zaupanja vredne platforme: profil zaščite za na potrebe stranke osredotočen modul zaupanja vredne platforme za osebne računalnike 2.0; raven 0; revizija 1.59 (v1.3), ANSSI-CC-PP-2021/02;

2. naprave strojne opreme z varnostnimi napravami:
   (a) točke (plačilne) interakcije in plačilni terminali (POI):
      (1) točka interakcije „POI-CHIP-ONLY“ (v4.0), ANSSI-CC-PP-2015/01;
      (2) točka interakcije „POI-CHIP-ONLY in paket odprtega protokola“ (v4.0), ANSSI-CC-PP-2015/02;
      (3) točka interakcije „POI-COMPREHENSIVE“ (v4.0), ANSSI-CC-PP-2015/03;
      (4) točka interakcije „POI-COMPREHENSIVE in paket odprtega protokola“ (v4.0), ANSSI-CC-PP-2015/04;
      (5) točka interakcije „POI-PED-ONLY“ (v4.0), ANSSI-CC-PP-2015/05;
      (6) točka interakcije „POI-PED-ONLY in paket odprtega protokola“ (v4.0), ANSSI-CC-PP-2015/06;
   (b) varnostni modul strojne opreme:
      (1) kriptografski modul za postopke podpisovanja ponudnika kriptografskih storitev z varnostnim kopiranjem – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;
      (2) kriptografski modul za storitve ustvarjanja ključa ponudnika kriptografskih storitev – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;
      (3) kriptografski modul za postopke podpisovanja ponudnika kriptografskih storitev brez varnostnega kopiranja – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;
   (c) tahograf:
      (1) digitalni tahograf – tipalo gibanja (MS PP) (v1.0), BSI-CC-PP-0093-2017;
      (2) digitalni tahograf – enota v vozilu (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021;
      (3) digitalni tahograf – zunanja GNSS oprema (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021;
3. drugo: profil zaščite zaupanja vrednega okolja izvrševanja ukazov – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.“.

PRILOGA IV

Priloga IV k Izvedbeni uredbi (EU) 2024/482 se spremeni:

1. v točki IV.2 se točka 4 nadomesti z naslednjim:

„4. Certifikacijski organ navedeno poročilo pregleda in pripravi poročilo o ponovni oceni. Status prvotnega certifikata se nato spremeni v skladu s členom 13 ali členom 19. Če je postopek ponovne ocene uspešen, se v primeru certificiranja proizvoda uporablja člen 13(2), točka (a) ali (c), v primeru certificiranja profila zaščite pa člen 19(2), točka (a) ali (c). Če postopek ponovne ocene ni uspešen, se v primeru certificiranja proizvoda uporablja člen 13(2), točka (b) ali (d), v primeru certificiranja profila zaščite pa člen 19(2), točka (b) ali (d).“;

2. točka IV.3 se spremeni:

(a) naslov IV.3 se nadomesti z naslednjim:

„IV.3 **Spremembe certificiranega proizvoda IKT – vzdrževanje in ponovna ocena**“;

(b) točki 4 in 5 se nadomestita z naslednjim:

„4. Po preučitvi opredeli obseg spremembe kot manjšo ali večjo glede na njene posledice na zanesljivost, ki jo izraža certifikat EUCC.

5. Kadar certifikacijski organ potrdi, da so spremembe manjše, se za spremenjeni proizvod IKT ne izda nov certifikat v skladu s členom 13(2), točka (a), ali členom 19(2), točka (a), in se pripravi poročilo o vzdrževanju, priloženo prvotnemu poročilu o certificiranju.“;

(c) vstavi se naslednja točka 5a:

„5.a V primeru kakršnih koli sprememb ukrepov glede zanesljivosti v razvojnem okolju, vključno z dodatnimi zahtevami glede zanesljivosti iz družine CC ALC_FLR (odprava napak), lahko certifikacijski organ od centra za ocenjevanje varnosti informacijske tehnologije zahteva, da izvede podsklop ocenjevanja zadevnih ukrepov glede zanesljivosti. Center za ocenjevanje varnosti informacijske tehnologije izda delno tehnično poročilo o ocenjevanju, na podlagi katerega certifikacijski organ potrdi, da so spremembe manjše ali večje. Kadar certifikacijski organ potrdi, da so spremembe manjše, se uporablja točka 5 Priloge IV.3. Kadar certifikacijski organ potrdi, da so spremembe večje, se uporablja točka 7 Priloge IV.3.“.

PRILOGA V

Točka V.1 Priloge V k Izvedbeni uredbi (EU) 2024/482 se nadomesti z naslednjim:

„V.1 **Poročilo o certificiranju**

1. Certifikacijski organ na podlagi tehničnih poročil o ocenjevanju, ki jih je predložil center za ocenjevanje varnosti informacijske tehnologije, pripravi poročilo o certificiranju za objavo skupaj z ustreznim certifikatom EUCC in varnostnim ciljem.

2. Poročilo o certificiranju je vir podrobnih in praktičnih informacij o proizvodu IKT in varni uvedbi proizvoda IKT. Zato vključuje vse javno dostopne in skupne informacije, ki so pomembne za uporabnike in zainteresirane strani. Na take informacije lahko napotuje poročilo o certificiranju.

3. Navedeno poročilo vsebuje vsaj naslednje informacije:
   (a) povzetek;
   (b) identifikacijo proizvoda IKT;
   (c) kontaktne podatke, povezane z ocenjevanjem proizvoda IKT;
   (d) varnostne politike;
   (e) predpostavke in pojasnitev obsega;
   (f) informacije o arhitekturi;
   (g) kadar je ustrezno, dodatne informacije o kibernetski varnosti;
   (h) povzetek ocene in ocenjeno konfiguracijo proizvoda IKT;
   (i) rezultate ocenjevanja in informacije o certifikatu;
   (j) pripombe in priporočila, če je ustrezno;
   (k) priloge, če je ustrezno;
   (l) sklicevanje na varnostni cilj proizvoda IKT, predloženega v certificiranje;
   (m) kadar sta na voljo, znak ali oznako, povezana s shemo;
   (n) glosar, če je ustrezno;
   (o) seznam literature.

4. V povzetku iz odstavka 3, točka (a), je na kratko povzeto celotno poročilo o certificiranju. V njem je jasen in jedrnat pregled rezultatov ocenjevanja ter so zajete naslednje informacije:
   (a) ime ocenjenega proizvoda IKT;
   (b) ime centra za ocenjevanje varnosti informacijske tehnologije, ki je opravil oceno;
   (c) datum dokončanja ocenjevanja;
   (d) datum izdaje certifikata;
   (e) kadar je ustrezno, datum izdaje prvotnega certifikata;
   (f) obdobje veljavnosti;
   (g) enotno identifikacijo certifikata, kot je opisano v členu 11;
   (h) kratek opis rezultatov poročila o certificiranju, ki zajema:
      (i) različico in, kadar je ustrezno, izdajo skupnih meril, uporabljenih pri ocenjevanju;
      (ii) paket zanesljivosti skupnih meril ali seznam komponent z ravnjo varnosti, ravnjo AVA_VAN, ki je uporabljena pri ocenjevanju in ustreza ravni zanesljivosti, kakor je določena v členu 52 Uredbe (EU) 2019/881, na katerega se sklicuje certifikat EUCC;
      (iii) kadar je ustrezno, profile zaščite, za katere se za proizvod IKT trdi, da je skladen;
      (iv) sklic na varnostno politiko ocenjenega proizvoda IKT;
      (v) izjave o omejitvi odgovornosti, če je ustrezno.

5. Opredelitev iz odstavka 3, točka (b), jasno opredeljuje ocenjeni proizvod IKT, vključno z naslednjimi informacijami:

   (a) enotno identifikacijo ocenjenega proizvoda IKT;

   (b) navedbo komponent proizvoda IKT, vključenih v ocenjevanje s številko različice vsake komponente;

   (c) sklic na dodatne zahteve za operacijsko okolje certificiranega proizvoda IKT.

6. Kontaktni podatki iz odstavka 3, točka (c), vključujejo vsaj naslednje informacije:

   (a) ime razvijalca;

   (b) ime in kontaktne podatke imetnika certifikata EUCC;

   (c) ime certifikacijskega organa, ki je izdal certifikat;

   (d) pristojni nacionalni certifikacijski organ za kibernetsko varnost;

   (e) ime centra za ocenjevanje varnosti informacijske tehnologije in, kadar je ustrezno, seznam podizvajalcev.

7. Oddelek o varnostni politiki iz odstavka 3, točka (d), vsebuje opis varnostne politike proizvoda IKT kot zbirke varnostnih politik in politik ali pravil, ki jih bo izvajal ali izpolnjeval ocenjeni proizvod IKT. Vsebovati mora tudi naslednje podatke:

   (a) opis postopkov za obvladovanje šibkih točk in postopkov za razkrivanje šibkih točk imetnika certifikata, ki se dopolnijo izključno z informacijami, ki se lahko javno objavijo;

   (b) politiko neprekinjene zanesljivosti imetnika certifikata, kadar je ustrezno vključno z opisom postopkov upravljanja življenjskega cikla ali proizvodnih postopkov imetnika certifikata v skladu z oddelkom IV.1 Priloge IV;

   (c) kadar je ustrezno, postopek upravljanja popravkov in rezultat njegove ocene v skladu z oddelkom IV.4 Priloge IV.

8. Predpostavke in pojasnitev obsega iz odstavka 3, točka (e), vsebujejo informacije o okoliščinah in ciljih v zvezi s predvideno uporabo proizvoda, kakor je navedeno v členu 7(1), točka (c), ter vključujejo naslednje:

   (a) predpostavke o uporabi in uvajanju proizvoda IKT v obliki minimalnih zahtev, kot je izpolnjevanje zahtev v zvezi z ustrezno namestitvijo in konfiguracijo ter zahtev glede strojne opreme;

   (b) predpostavke o okolju za skladno delovanje proizvoda IKT;

   (c) opis kakršnih koli groženj za proizvod IKT, proti katerim se ne borijo ocenjene varnostne funkcije proizvoda glede na predvideno uporabo, če se šteje, da so pomembne za potencialnega uporabnika proizvoda IKT.

   Informacije iz prvega pododstavka so čim bolj jasne in razumljive, da bi lahko potencialni uporabniki certificiranega proizvoda IKT sprejemali informirane odločitve o tveganjih, povezanih z njegovo uporabo.

9. Informacije o arhitekturi iz odstavka 3, točka (f), vključujejo opis proizvoda IKT in njegovih glavnih komponent na visoki ravni na podlagi rezultatov, opredeljenih v skupnih merilih za družino zanesljivosti: razvoj – zasnova cilja ocenjevanja (ADV_TDS).

10. Dodatne informacije o kibernetski varnosti iz odstavka 3, točka (g), vključujejo povezavo do spletišča imetnika certifikata EUCC iz člena 55 Uredbe (EU) 2019/881.

11. Pri ocenjevanju in konfiguraciji proizvoda IKT iz odstavka 3, točka (h), se opišejo prizadevanja razvijalca in ocenjevalca glede testiranja ter opišejo pristop k testiranju, konfiguracija in temeljitost. Vsebuje vsaj naslednje podatke:

    (a) opredelitev uporabljenih komponent zanesljivosti iz standardov iz člena 3;

    (b) različico najsodobnejših dokumentov in dodatna merila za ocenjevanje varnosti, uporabljena pri ocenjevanju;

    (c) nastavitve in konfiguracije cilja ocenjevanja, ki se uporabljajo za preizkušanje in analizo šibkih točk;

    (d) vsak uporabljeni profil zaščite, vključno z naslednjimi informacijami: ime profila zaščite, različico, datum in certifikat.

12. Rezultati ocenjevanja in informacije v zvezi s certifikatom iz odstavka 3, točka (i), vključujejo informacije o doseženi ravni zanesljivosti iz člena 4 te uredbe in člena 52 Uredbe (EU) 2019/881.

13. Pripombe in priporočila iz odstavka 3, točka (j), se uporabljajo za posredovanje dodatnih informacij o rezultatih ocenjevanja. Te pripombe in priporočila so lahko v obliki pomanjkljivosti proizvoda IKT, odkritih med ocenjevanjem, ali navedbe značilnosti, ki so še posebej koristne.

14. Priloge iz odstavka 3, točka (k), se uporabljajo za opis kakršnih koli dodatnih informacij, ki bi lahko bile koristne za naslovnike poročila, vendar se logično ne ujemajo s predpisanimi oddelki poročila, tudi v primerih popolnega opisa varnostne politike.

15. Varnostni cilj iz odstavka 3, točka (l), se sklicuje na ocenjeni varnostni cilj. Ocenjenemu varnostnemu cilju se predloži poročilo o certificiranju za namene objave na spletišču iz člena 50(1) Uredbe (EU) 2019/881. Če je pred objavo potrebno prečiščevanje ocenjenega varnostnega cilja, se izvede v skladu s točko V.2 Priloge V k tej uredbi.

16. V poročilo o certificiranju se lahko vključijo znaki ali oznake, povezani s shemo EUCC iz odstavka 3, točka (m), v skladu s pravili in postopki iz člena 11.

17. Glosar iz odstavka 3, točka (n), se uporablja za večjo berljivost poročila z opredelitvijo kratic ali izrazov, katerih pomenov morda ni mogoče zlahka razbrati.

18. V oddelku o seznamu literature iz odstavka 3, točka (o), so zajeti sklici na vse dokumente, uporabljene pri pripravi poročila o certificiranju. Te informacije vključujejo najmanj naslednje:

    (a) merila za ocenjevanje varnosti, najsodobnejše dokumente ter dodatne uporabljene ustrezne specifikacije;

    (b) tehnično poročilo o ocenjevanju;

    (c) tehnično poročilo o ocenjevanju za ocenjevanje sestavljenih proizvodov, kadar je ustrezno;

    (d) tehnične referenčne dokumente;

    (e) varnostne smernice razvijalca;

    (f) seznam konfiguracij razvijalca.

    Da bi se ocenjevanje lahko ponovilo, morajo biti vsi dokumenti edinstveno označeni z ustreznim datumom izdaje in ustrezno številko različice.“.

PRILOGA VI

„PRILOGA IX

Znak in oznaka

1. Oblika znaka in oznake:



2. Če sta znak in oznaka pomanjšana ali povečana, se upošteva razmerje iz točke 1.

3. Če sta znak in oznaka fizično prisotna, sta visoka najmanj 5 mm.“.