2025/2462

9.12.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/2462

od 8. prosinca 2025.

o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu definicija, certifikacije serije IKT proizvoda, kontinuiteta jamstva i specifikacija najsuvremenijih tehnika

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) ([1]), a posebno njezin članak 49. stavak 7.,

budući da:

(1) Provedbenom uredbom Komisije (EU) 2024/482 ([2]) utvrđuju se uloge, pravila i obveze te struktura Europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) u skladu s europskim okvirom za kibernetičkosigurnosnu certifikaciju utvrđenim u Uredbi (EU) 2019/881.

(2) Zajednička evaluacijska metodologija koja dolazi uz zajedničke kriterije, međunarodnu normu za evaluaciju informacijske sigurnosti, omogućuje evaluaciju sigurnosti IKT proizvoda za potrebe certifikacije. U tom kontekstu neki IKT proizvodi mogu imati istu funkcionalnu osnovu kako bi se na različitim platformama ili uređajima ponudile slične sigurnosne funkcije, a nazivaju se i serija proizvoda. Međutim, ti proizvodi mogu imati različit dizajn, hardver, ugrađeni program ili softver. Certifikacijsko tijelo na pojedinačnoj osnovi odlučuje može li se provesti certifikacija serije proizvoda. Uvjeti za certifikaciju serije proizvoda mogli bi se detaljnije pojasniti u popratnim smjernicama za EUCC.

(3) Kako bi certificirani proizvodi ostali pouzdani, ključno je definirati što čini veću i manju promjenu predmeta evaluacije ili njegova okruženja, uključujući njegovo radno ili razvojno okruženje. Stoga te pojmove treba utvrditi uzimajući u obzir postojeće i često korištene tehničke specifikacije Skupine viših dužnosnika za sigurnost informacijskih sustava (SOG-IS) i sudionika Sporazumâ o priznavanju certifikata zajedničkih kriterija u području informatičke sigurnosti (CCRA).

(4) Manje promjene često imaju ograničen utjecaj na izjavu o jamstvu za proizvod sadržanu u izdanom EUCC certifikatu. Stoga bi manjim promjenama trebalo upravljati u okviru postupaka održavanja te u pogledu njih nije potrebna ponovna evaluacija sigurnosnih funkcija proizvoda. Primjeri manjih promjena koje bi trebalo razmotriti u okviru održavanja uključuju, među ostalim, uredničke izmjene, promjene okruženja predmeta evaluacije kojima se ne mijenja certificirani predmet evaluacije i promjene certificiranog predmeta evaluacije koje ne utječu na dokaze na kojima se temelji jamstvo. Promjene u razvojnom okruženju također se mogu smatrati manjim promjenama, pod uvjetom da nemaju naknadnih učinaka na postojeće mjere jamstva. Međutim, u pogledu njih u nekim slučajevima može biti potrebno provesti djelomičnu evaluaciju relevantnih mjera.

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

([2]) Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) (SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Veća promjena svaka je promjena certificiranog predmeta evaluacije ili njegova okruženja koja bi mogla negativno utjecati na jamstvo navedeno u EUCC certifikatu, zbog koje bi stoga trebalo provesti ponovnu evaluaciju. Veće su promjene, na primjer, promjene skupa zahtjeva za navedeno jamstvo, osim zahtjeva za jamstvo za porodicu CC ALC_FLR (otklanjanje nedostatka), promjene kontrola povjerljivosti ili cjelovitosti razvojnog okruženja ako bi takve promjene mogle utjecati na sigurnost razvoja ili proizvodnje predmeta evaluacije, ili promjene predmeta evaluacije kako bi se uklonila ranjivost koja se može iskoristiti. Osim toga, skup manjih promjena koje zajedno znatno utječu na sigurnost također se može smatrati većom promjenom. Važno je prepoznati da ispravljanje pogreške, premda možda utječe samo na određeni aspekt predmeta evaluacije, može zbog nepredvidljivosti i mogućeg utjecaja na jamstvo dovesti do veće promjene ako narušava sigurnosna jamstva iz certifikata.

(6) Ako dođe do promjene u pogledu prijetnji za nepromijenjeni certificirani IKT proizvod, možda bi ga trebalo ponovno ocijeniti. Trebalo bi jasno utvrditi moguće ishode takvog postupka ponovnog ocjenjivanja, posebno njegov utjecaj na EUCC certifikat. Ako je ponovno ocjenjivanje bilo pozitivno, certifikacijsko tijelo trebalo bi potvrditi certifikat ili izdati novi s produljenim datumom isteka. Ako postupak ponovnog ocjenjivanja nije bio pozitivan, certifikacijsko tijelo trebalo bi povući certifikat i eventualno izdati novi s drukčijim opsegom. Takve bi se odredbe trebale primjenjivati *mutatis mutandis* na ponovno ocjenjivanje profilâ zaštite.

(7) U Prilogu I. Provedbenoj uredbi (EU) 2024/482 navedene su specifikacije najsuvremenijih tehnika koje se primjenjuju za evaluaciju IKT proizvoda i profila zaštite. Te bi specifikacije najsuvremenijih tehnika trebalo ažurirati u skladu s najnovijim kretanjima, na primjer u području tehnološkog razvoja, kibernetičkih prijetnji, sektorskih praksi ili međunarodnih normi. Takvo ažuriranje prikladno je za specifikacije najsuvremenijih tehnika koje se odnose na minimalne sigurnosne zahtjeve za lokaciju, primjenu potencijala za napad na pametne kartice, primjenu potencijala za napad na hardverske uređaje sa sigurnosnim kutijama, primjenu zajedničkih kriterija na integrirane krugove i evaluaciju složenih proizvoda za pametne kartice i slične uređaje. Nisu obuhvaćene specifikacije najsuvremenijih tehnika povezane s evaluacijom i certifikacijom složenih proizvoda upotrebom najnovije verzije normi na temelju zajedničkih kriterija, ponovnom upotrebom rezultata evaluacije revizija na lokaciji i pojašnjenjima koja se odnose na tumačenje profila zaštite za sredstva za izradu kvalificiranog elektroničkog potpisa, tahografe i hardverske sigurnosne module. Kako bi se osigurala ujednačena evaluacija IKT proizvoda u okviru EUCC-a, Prilog I. trebalo bi izmijeniti kako bi se uključile ažurirane i nove specifikacije najsuvremenijih tehnika nakon što ih odobri Europska skupina za kibernetičkosigurnosnu certifikaciju (ECCG).

(8) Osim toga, u program bi trebalo dodati specifikaciju najsuvremenijih tehnika „Tumačenje sigurnosnog zahtjeva ADV_SPM.1 za prelazak na verziju CC:2022” kako bi se u postupcima certifikacije koji se temelje na posebnim profilima zaštite moglo i dalje koristiti formalno modeliranje (ADV_SPM.1) dok se ne ažuriraju odgovarajući profili zaštite, primjerice dodavanjem konfiguracije profila zaštite s višestrukim jamstvom usklađene s verzijom CC:2022 koja podržava ADV_SPM.1. Kako bi se osiguralo dovoljno vremena da tržište prijeđe na ažurirane norme na temelju zajedničkih kriterija, treba predvidjeti posebna prijelazna pravila za profile zaštite Profil zaštite za platformu sigurnosnog integriranog kruga s paketima proširenja (v1.0), BSI-CC-PP-0084-2014, Sustav Java Card – zatvorena konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020 ili Sustav Java Card – otvorena konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020. Kako bi se izbjegli poremećaji na tržištu, primjereno je utvrditi da se specifikacija najsuvremenijih tehnika o tumačenju sigurnosnog zahtjeva ADV_SPM.1 za prelazak na verziju CC:2022 primjenjuje na postupke certifikacije koji su pokrenuti prije donošenja ove Uredbe. Međutim, primjena te specifikacije trebala bi biti strogo ograničena na ono što je potrebno s obzirom na vrijeme potrebno za dovršetak ažuriranja odgovarajućih profila zaštite. Točnije, specifikacija najsuvremenijih tehnika za postupke certifikacije u kojima se koriste profili zaštite Profil zaštite za platformu sigurnosnog integriranog kruga s paketima za proširenje (v1.0), BSI-CC-PP-0084-2014 ili Sustav Java Card – zatvorena konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020, trebala bi se primjenjivati na postupke koji su pokrenuti prije 1. listopada 2026. Kad je riječ o postupcima certifikacije u kojima se koristi profil zaštite Sustav Java Card – otvorena konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020, specifikacija najsuvremenijih tehnika trebala bi se primjenjivati samo na postupke pokrenute prije datuma stupanja na snagu ove Uredbe jer je nova verzija profila zaštite Sustav Java Card – otvorena konfiguracija već dostupna.

(9) Promjena u specifikacijama najsuvremenijih tehnika u postupku certifikacije mogla bi poremetiti evaluaciju proizvoda i odgoditi izdavanje certifikata. Stoga su potrebna odgovarajuća prijelazna pravila za nove ili ažurirane specifikacije najsuvremenijih tehnika kako bi se dobavljačima, ITSEF-ovima, certifikacijskim tijelima i drugim dionicima omogućilo da provedu potrebne prilagodbe. Primjenjive ažurirane i nove specifikacije najsuvremenijih tehnika trebale bi se odnositi na zahtjeve za certifikaciju, uključujući zahtjeve za ponovno ocjenjivanje i ponovnu evaluaciju, a u postupcima certifikacije koji su u tijeku trebalo bi biti moguće nastaviti koristiti ranije verzije tih specifikacija.

(10) U Prilogu II. i Prilogu III. Provedbenoj uredbi (EU) 2024/482 navode se profili zaštite certificirani na razini AVA_VAN 4 ili 5 i preporučeni profili zaštite. Nekoliko upućivanja nepotpuno je ili zastarjelo jer su profili zaštite ažurirani. Ta bi upućivanja trebalo dopuniti i navesti nova kako bi se bolje obuhvatili sigurni integrirani krugovi, pametne kartice i povezani uređaji te tehnologija pouzdanog računalstva (engl. „trusted computing").

(11) Potrebno je izmijeniti članak 19. Provedbene uredbe (EU) 2024/482 kako bi se pojasnilo da se Prilog IV. uz potrebne izmjene primjenjuje na reviziju EUCC certifikata za profile zaštite.

(12) S obzirom na to da je potrebna sigurnost ključan element za razumijevanje opsega postupka certifikacije, potrebno je i da ENISA na svojim internetskim stranicama objavi potrebnu sigurnost koja odgovara svakom EUCC certifikatu.

(13) Nadalje, certifikacijska tijela trebala bi ENISA-i dostaviti verziju potrebne sigurnosti i izvješća o certifikaciji na engleskom jeziku kako bi ona mogla te informacije objaviti na engleskom jeziku na odgovarajućim internetskim stranicama, u skladu s člankom 42. stavkom 2. Provedbene uredbe (EU) 2024/482. Zbog toga bi podnositelji zahtjeva za certifikaciju trebali certifikacijskim tijelima na zahtjev dostaviti verziju potrebne sigurnosti na engleskom jeziku.

(14) Ime certifikacijskog tijela ne mora biti navedeno na jedinstvenoj identifikacijskoj oznaci certifikata jer je njegov identifikacijski broj dovoljan da ga se identificira na jedinstven način. Ne treba navesti ni mjesec izdavanja jer se certifikati evidentiraju na godišnjoj osnovi. Stoga bi radi pojednostavnjenja taj zahtjev trebalo izbrisati. Budući da godina izdavanja certifikata odgovara izdavanju prvog certifikata, taj bi datum trebao biti naveden u jedinstvenoj identifikacijskoj oznaci na certifikatima izdanima nakon revizije kako bi bili sljedivi.

(15) Provedbenu uredbu (EU) 2024/482 trebalo bi stoga na odgovarajući način izmijeniti.

(16) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 66. Uredbe (EU) 2019/881,

DONIJELA JE OVU UREDBU:

Članak 1.

Provedbena uredba (EU) 2024/482 mijenja se kako slijedi:

1. u članku 2. dodaju se sljedeće točke 16., 17. i 18.:

„16. ‚serija proizvoda' znači skup IKT proizvoda podnositelja zahtjeva koji imaju istu funkcionalnu osnovu kako bi se odgovorilo na iste sigurnosne potrebe, a čiji se dizajn, hardver, ugrađeni program ili softver mogu razlikovati;

17. ‚manja promjena' znači svaka promjena certificiranog predmeta evaluacije ili njegova okruženja koja ne utječe negativno na jamstvo navedeno u EUCC certifikatu;

18. ‚veća promjena' znači svaka promjena certificiranog predmeta evaluacije ili njegova okruženja koja bi mogla negativno utjecati na jamstvo navedeno u EUCC certifikatu.";

2. u članku 5. dodaje se sljedeći stavak 3.:

„3. Certifikacijsko tijelo može dopustiti certifikaciju serije proizvoda.";

3. u članku 9. stavku 2. točka (a) zamjenjuje se sljedećim:

„(a) certifikacijskom tijelu i ITSEF-u dostaviti sve potrebne potpune i točne informacije te, na zahtjev, dostaviti dodatne potrebne informacije, uključujući verziju potrebne sigurnosti na engleskom jeziku;";

4. u članku 11. stavku 3. točka (b) zamjenjuje se sljedećim:

„(b) jedinstvenu identifikacijsku oznaku certifikata koja se sastoji od:

1. imena programa;

2. identifikacijskog broja certifikacijskog tijela koje je izdalo certifikat, u skladu s člankom 3. Provedbene uredbe (EU) 2024/3143;

3. godine izdavanja početnog certifikata;

4. identifikacijskog broja koji dodjeljuje certifikacijsko tijelo koje je izdalo certifikat.”;

5. u članku 19. stavak 1. zamjenjuje se sljedećim:

„1. Na zahtjev nositelja certifikata ili iz drugih opravdanih razloga certifikacijsko tijelo može odlučiti revidirati EUCC certifikat za određeni profil zaštite. Revizija se provodi u skladu s Prilogom IV. Opseg revizije određuje certifikacijsko tijelo. Ako je to potrebno radi revizije, certifikacijsko tijelo zahtijeva od ITSEF-a da provede ponovnu evaluaciju certificiranog profila zaštite.”;

6. članak 42. mijenja se kako slijedi:

(a) u stavku 1. dodaje se sljedeća točka (i):

„(i) potrebnu sigurnost za svaki EUCC certifikat;”;

(b) stavak 2. zamjenjuje se sljedećim:

„2. Informacije iz stavka 1. moraju biti barem na engleskom jeziku. U tu svrhu certifikacijska tijela ENISA-i dostavljaju izvorne jezične verzije izvješća o certifikaciji i potrebnih sigurnosti te bez nepotrebne odgode dostavljaju i verziju takvih dokumenata na engleskom jeziku.”;

7. u članku 48. stavak 4. zamjenjuje se sljedećim:

„4. Ako u Prilogu I. ili II. nije navedeno drukčije, specifikacije najsuvremenijih tehnika primjenjuju se na postupke certifikacije, uključujući ponovno ocjenjivanje i ponovnu evaluaciju, koji su pokrenuti od datuma početka primjene akta o izmjeni kojim su specifikacije najsuvremenijih tehnika uvrštene u Prilog I. ili II.”;

8. Prilog I. zamjenjuje se tekstom iz Priloga I. ovoj Uredbi;

9. Prilog II. zamjenjuje se tekstom iz Priloga II. ovoj Uredbi;

10. Prilog III. zamjenjuje se tekstom iz Priloga III. ovoj Uredbi;

11. Prilog IV. mijenja se u skladu s Prilogom IV. ovoj Uredbi;

12. Prilog V. mijenja se u skladu s Prilogom V. ovoj Uredbi;

13. Prilog IX. zamjenjuje se tekstom iz Priloga VI. ovoj Uredbi.

Članak 2.

Ova Uredba stupa na snagu dvadesetog dana od dana objave *u Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 8. prosinca 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

„PRILOG I.

Specifikacije najsuvremenijih tehnika za tehničke domene i druge specifikacije najsuvremenijih tehnika

1. Specifikacije najsuvremenijih tehnika za tehničke domene na razini AVA_VAN 4 ili 5:
   (a) sljedeće specifikacije koje se odnose na usklađenu evaluaciju tehničke domene „pametne kartice i slični uređaji”:
      1. „Minimalni zahtjevi ITSEF-a za sigurnosne evaluacije pametnih kartica i sličnih uređaja”, verzija 1.1;
      2. „Minimalni sigurnosni zahtjevi za lokaciju”, verzija 2;
      3. „Ponovna upotreba rezultata evaluacije revizija na lokaciji (STAR)”, verzija 1;
      4. „Primjena zajedničkih kriterija na integrirane krugove”, verzija 2;
      5. „Zahtjevi za sigurnosnu arhitekturu (ADV_ARC) za pametne kartice i slične uređaje”, verzija 1.1;
      6. „Certifikacija proizvoda s „otvorenom” tehnologijom pametnih kartica”, verzija 1.1;
      7. „Evaluacija složenih proizvoda za pametne kartice i slične uređaje za CC3.1”, verzija 2;
      8. „Evaluacija i certifikacija složenih proizvoda za CC:2022”, verzija 1;
      9. „Primjena potencijala za napad na pametne kartice i slične uređaje”, verzija 2;
      10. „Sigurnosna evaluacija i certifikacija kvalificiranih sredstava za izradu elektroničkih potpisa/pečata”, verzija 1;
      11. „Tumačenje sigurnosnog zahtjeva ADV_SPM.1 za prelazak na CC:2022”, verzija 1.1., primjenjivo za postupke certifikacije u kojima se koriste sljedeći profili zaštite:
         (a) profili zaštite Profil zaštite za platformu sigurnosnog integriranog kruga s paketima za proširenje (v1.0), BSI-CC-PP-0084-2014 ili Sustav Java Card – zatvorena konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020, pokrenuti prije 1. listopada 2026.;
         (b) profil zaštite Sustav Java Card – otvorena konfiguracija (v3.1), BSI-CC-PP-0099-V2-2020., pokrenut prije 29. prosinca 2025.;
   (b) sljedeće specifikacije koje se odnose na usklađenu evaluaciju tehničke domene „hardverski uređaji sa sigurnosnim kutijama”:
      1. „Minimalni zahtjevi za ITSEF za sigurnosne evaluacije hardverskih uređaja sa sigurnosnim kutijama”, verzija 1.1.;
      2. „Minimalni sigurnosni zahtjevi za lokaciju”, verzija 2;
      3. „Ponovna upotreba rezultata evaluacije revizija na lokaciji (STAR)”, verzija 1;
      4. „Primjena potencijala za napad na hardverske uređaje sa sigurnosnim kutijama”, verzija 2;
      5. „Ocjenjivanje hardvera prema normi EN 419221-5 (HSM PP)”, verzija 1;
      6. „JIL-ovo pojašnjenje profila zaštite za senzor kretanja tahografa”, verzija 1;

2. specifikacije najsuvremenijih tehnika koje se odnose na usklađenu akreditaciju tijela za ocjenjivanje sukladnosti:
   (a) „Akreditacija ITSEF-a za EUCC”, verzija 1.1. za akreditacije izdane prije 8. srpnja 2025.;
   (b) „Akreditacija ITSEF-a za EUCC”, verzija 1.6c, za akreditacije koje su novoizdane ili revidirane nakon 8. srpnja 2025.;
   (c) „Akreditacija certifikacijskih tijela za EUCC”, verzija 1.6b.”.

PRILOG II.

„PRILOG II.

Profili zaštite certificirani na razini AVA_VAN 4 ili 5

1. Za kvalificirana sredstava za udaljenu izradu elektroničkih potpisa i pečata:

   (a) EN 419241-2:2019 – Vjerodostojni sustavi za potporu potpisivanja na poslužitelju – 2. dio: Profil zaštite za kvalificirano sredstvo za izradu elektroničkog potpisa za potpisivanje na poslužitelju (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 – Profili zaštite kriptografskih modula pružatelja usluga povjerenja (TSP-a) – 5. dio: Kriptografski modul za usluge povjerenja (v0.15), ANSSI-CC-PP-2016/05-M01

2. Profili zaštite koji su doneseni kao specifikacije najsuvremenijih tehnika:

   [PRAZNO].”

PRILOG III.

„PRILOG III.

Preporučeni profili zaštite

Profili zaštite koji se koriste u certifikaciji IKT proizvoda, uključujući proizvode u tehničkim domenama:

1. pametne kartice i slični uređaji

   (a) putovnica:

      1. Profil zaštite za strojno čitljivu putnu ispravu s osnovnom kontrolom pristupa za ICAO (v1.10), BSI-CC-PP-0055-2009;

      2. Profil zaštite za strojno čitljivu putnu ispravu za koju se koristi standardni postupak pregleda s PACE-om (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01;

      3. Profil zaštite za strojno čitljivu putnu ispravu s proširenom kontrolom pristupa za ICAO s PACE-om (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;

   (b) sigurna sredstva za izradu potpisa (SSCD):

      1. EN 419211-2:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 2. dio: Sredstvo za generiranje ključa (v1.03), BSI-CC-PP-0059-2009-MA-02;

      2. EN 419211-3:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 3. dio: Sredstvo za uvođenje ključa (v1.0.2), BSI-CC-PP-0075-2012-MA-01;

      3. EN 419211-4:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 4. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za generiranje certifikata (v1.0.1), BSI-CC-PP-0071-2012-MA-01;

      4. EN 419211-5:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 5. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za izradu elektroničkog potpisa (v1.0.1), BSI-CC-PP-0072-2012-MA-01;

      5. EN 419211-6:2014 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 6. dio: Dodatna zaštita sredstava za uvođenje ključa i povjerljivi kanal do aplikacije za izradu elektroničkog potpisa (v1.0.4), BSI-CC-PP-0076-2013-MA-01;

   (c) tahograf: Digitalni tahograf – tahografska kartica (TC PP) (v1.0), BSI-CC-PP-0091-2017;

   (d) sigurnosni integrirani krug, platforma Java Card i eUICC:

      1. Osnovni profil zaštite za platformu Java Card za univerzalnu SIM karticu i SCWS konfiguracije (v2.0.2), ANSSI-CC-PP-2010/04 (osnovni), ANSSI-CC-PP-2010/05 (osnovni i SCWS);

      2. Profil zaštite za platformu sigurnosnog integriranog kruga s paketima za proširenje (v1.0), BSI-CC-PP-0084-2014;

      3. Ugrađeni UICC (eUICC) za uređaje koji izravno komuniciraju s drugim strojevima (v1.1), BSI-CC-PP-0089-2015;

      4. Pružatelj kriptografskih usluga – CSP (v0.9.8), BSI-CC-PP-0104-2019;

      5. Pružatelj kriptografskih usluga – usluga vremenskog žiga i revizija (PPC-CSP-TS-Au) verzija 0,9.5, BSI-CC-PP-0107-2019;

      6. Pružatelj konfiguriranja kriptografskih usluga – usluga vremenskog žiga, revizija i klasteriranje (PPC-CSP-TS-Au-Cl) verzija 0,9.4, BSI-CC-PP-0108-2019;

      7. Sustav Java Card – zatvorena konfiguracija (v3.1), BSI-CC-PP-0101-V2-2020;

      8. Profil zaštite sigurnih elemenata – GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021;

      9. Profil zaštite za sigurnosni podsustav u sustavu na čipu (3S u SoC) (v1.8), BSI-CC-PP-0117-V2-2023;

      10. Sustav Java Card – otvorena konfiguracija (v3.2), BSI-CC-PP-0099-V3-2024;

      11. Profil zaštite za ugrađeni UICC za potrošačke uređaje (v2.1), BSI-CC-PP-0100-V2-2025;

   (e) Trusted Platform Module: Profil zaštite za porodicu modula u skladu sa standardom Trusted Platform Module za klijentsko osobno računalo 2.0, razina 0, revizija 1.59 (v1.3), ANSSI-CC-PP-2021/02;

2. hardverski uređaji sa sigurnosnim kutijama:
   (a) za kategoriju točaka interakcije (za plaćanja) i terminala za plaćanje (POI):
      1. Točka interakcije „POI-CHIP-ONLY” (v4.0), ANSSI-CC-PP-2015/01;
      2. Točka interakcije „POI-CHIP-ONLY i paket otvorenog 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 i paket otvorenog 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 i paket otvorenog protokola” (v4.0), ANSSI-CC-PP-2015/06;
   (b) sigurnosni modul za hardver:
      1. Kriptografski modul za operacije potpisivanja pružatelja kriptografskih usluga sa sigurnosnom kopijom – PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08;
      2. Kriptografski modul za usluge generiranja ključeva pružatelja kriptografskih usluga – PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09;
      3. Kriptografski modul za operacije potpisivanja pružatelja kriptografskih usluga bez sigurnosne kopije – PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;
   (c) tahograf:
      1. Digitalni tahograf – senzor kretanja (PZ za MS) (v1.0), BSI-CC-PP-0093-2017;
      2. Digitalni tahograf – jedinica u vozilu (PZ za VU) (v1.15.), BSI-CC-PP-0094-V2-2021
      3. Digitalni tahograf – vanjski uređaj GNSS-a (PZ za EGP) (v1.10), BSI-CC-PP-0092-V2-2021;
3. ostalo: Pouzdani profil zaštite okruženja izvršenja – GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02.”.

PRILOG IV.

Prilog IV. Provedbenoj uredbi (EU) 2024/482 mijenja se kako slijedi:

1. u točki IV.2. podtočka 4. zamjenjuje se sljedećim:

„4. Certifikacijsko tijelo pregledava ažurirano tehničko izvješće o evaluaciji i sastavlja izvješće o ponovnom ocjenjivanju. Zatim se status početnog certifikata mijenja u skladu s člankom 13. ili člankom 19. Ako je postupak ponovnog ocjenjivanja bio pozitivan, za certifikaciju proizvoda primjenjuje se članak 13. stavak 2. točka (a) ili (c), a za certifikaciju profila zaštite primjenjuje se članak 19. stavak 2. točka (a) ili (c). Ako postupak ponovnog ocjenjivanja nije bio pozitivan, za certifikaciju proizvoda primjenjuje se članak 13. stavak 2. točka (b) ili (d), a za certifikaciju profila zaštite primjenjuje se članak 19. stavak 2. točka (b) ili (d).”;

2. točka IV.3. mijenja se kako slijedi:

(a) naslov točke IV.3. zamjenjuje se sljedećim:

„IV.3. **Promjene certificiranog IKT proizvoda – održavanje i ponovna evaluacija**”;

(b) podtočke 4. i 5. zamjenjuju se sljedećim:

„4. Nakon ispitivanja certifikacijsko tijelo kvalificira razmjere promjene kao manje ili veće s obzirom na njezin utjecaj na jamstvo navedeno u EUCC certifikatu.

5. Ako certifikacijsko tijelo potvrdi da je riječ o manjim promjenama, ne izdaje se novi certifikat za izmijenjeni IKT proizvod u skladu s člankom 13. stavkom 2. točkom (a) ili člankom 19. stavkom 2. točkom (a) te se sastavlja izvješće o održavanju uz izvješće o početnoj certifikaciji.”;

(c) umeće se sljedeća točka 5.a:

„5.a U slučaju bilo kakvih promjena mjera jamstva u razvojnom okruženju, uključujući dodavanje zahtjeva za jamstvo iz porodice CC ALC_FLR (otklanjanje nedostataka), certifikacijsko tijelo može zatražiti od ITSEF-a da provede djelomičnu evaluaciju promijenjenih mjera jamstva. ITSEF izdaje tehničko izvješće o djelomičnoj evaluaciji na temelju kojeg certifikacijsko tijelo potvrđuje da su promjene manje ili veće. Ako certifikacijsko tijelo potvrdi da je riječ o manjim promjenama, primjenjuje se točka 5. Priloga IV.3. Ako certifikacijsko tijelo potvrdi da je riječ o većim promjenama, primjenjuje se točka 7. Priloga IV.3.”.

PRILOG V.

Točka V.1. Priloga V. Provedbenoj uredbi (EU) 2024/482 zamjenjuje se sljedećim:

„V.1. **Izvješće o certifikaciji**

1. Certifikacijsko tijelo na temelju tehničkih izvješća o evaluaciji koje dostavlja ITSEF sastavlja izvješće o certifikaciji koje se objavljuje zajedno s odgovarajućim EUCC certifikatom i potrebnom sigurnošću.

2. Izvješće o certifikaciji je referencija s detaljnim i praktičnim informacijama o IKT proizvodu i o sigurnom stavljanju IKT proizvoda u upotrebu. Stoga mora sadržavati sve javno dostupne i objavljive informacije koje su relevantne korisnicima i zainteresiranim stranama. Izvješće o certifikaciji može sadržavati upućivanja na javno dostupne i objavljive informacije.

3. Izvješće o certifikaciji sadržava barem sljedeće informacije:
   (a) sažetak;
   (b) informacije o kojem je IKT proizvodu riječ;
   (c) podatke za kontakt povezane s evaluacijom IKT proizvoda;
   (d) sigurnosne politike;
   (e) pretpostavke i objašnjenje opsega;
   (f) informacije o arhitekturi;
   (g) prema potrebi, dodatne informacije o kibernetičkoj sigurnosti;
   (h) sažetak evaluacije IKT proizvoda i evaluiranu konfiguraciju;
   (i) rezultate evaluacije i informacije o certifikatu;
   (j) primjedbe i preporuke (ako postoje);
   (k) priloge (ako postoje);
   (l) upućivanje na potrebnu sigurnost IKT proizvoda podnesenog na certifikaciju;
   (m) ako su dostupni, oznaku ili etiketu povezane s programom;
   (n) pojmovnik, prema potrebi;
   (o) bibliografiju.

4. Sažetak iz stavka 3. točke (a) kratak je sažetak cjelokupnog izvješća o certifikaciji. U njemu se daje jasan i jezgrovit pregled rezultata evaluacije i mora sadržavati sljedeće informacije:
   (a) ime evaluiranog IKT proizvoda;
   (b) ime ITSEF-a koji je proveo evaluaciju;
   (c) datum završetka evaluacije;
   (d) datum izdavanja certifikata;
   (e) prema potrebi, datum izdavanja početnog certifikata;
   (f) razdoblje valjanosti;
   (g) jedinstvenu identifikacijsku oznaku certifikata kako je opisano u članku 11.;
   (h) kratak opis rezultata izvješća o certifikaciji, uključujući:
      i. verziju i, prema potrebi, izdanje zajedničkih kriterija primijenjenih u evaluaciji;
      ii. sigurnosni jamstveni paket i komponente sigurnosnog jamstva zajedničkih kriterija, uključujući razinu AVA_VAN, primijenjene u evaluaciji i odgovarajuću jamstvenu razinu iz članka 52. Uredbe (EU) 2019/881 na koju se odnosi EUCC certifikat;
      iii. ako je primjenjivo, profil ili profile zaštite s kojima je IKT proizvod deklarirano sukladan;
      iv. upućivanje na sigurnosnu politiku evaluiranog IKT proizvoda;
      v. izjave o ograničenju odgovornosti, prema potrebi.

5. U identifikaciji iz stavka 3. točke (b) jasno se utvrđuje evaluirani IKT proizvod, uključujući sljedeće informacije:

(a) jedinstvenu identifikacijsku oznaku evaluiranog IKT proizvoda;

(b) popis komponenti IKT proizvoda koji su dio evaluacije s brojem verzije svake komponente;

(c) upućivanje na dodatne zahtjeve za radno okruženje certificiranog IKT proizvoda.

6. Podaci za kontakt iz stavka 3. točke (c) uključuju barem sljedeće informacije:

(a) ime proizvođača;

(b) ime i podatke za kontakt nositelja EUCC certifikata;

(c) ime certifikacijskog tijela koje je izdalo certifikat;

(d) odgovorno nacionalno tijelo za kibernetičkosigurnosnu certifikaciju;

(e) ime ITSEF-a koji je proveo evaluaciju i, ako je primjenjivo, popis podugovaratelja.

7. Sigurnosna politika iz stavka 3. točke (d) sadržava opis sigurnosne politike IKT proizvoda kao skupa sigurnosnih usluga te politike ili pravila koje evaluirani IKT proizvod mora primjenjivati ili s kojima mora biti sukladan. U njoj se navode i sljedeće informacije:

(a) opis postupaka za upravljanje ranjivostima i obavješćivanje o ranjivostima nositelja certifikata, koji sadržava isključivo informacije koje se mogu javno objaviti;

(b) politika kontinuiteta jamstva nositelja certifikata, uključujući, ako je primjenjivo, opis procesa upravljanja životnim ciklusom odnosno proizvodnje koje provodi nositelj certifikata u skladu s odjeljkom IV.1. Priloga IV.;

(c) ako je primjenjivo, postoji li postupak upravljanja zakrpama i ishod ocjene tog postupka u skladu s odjeljkom IV.4. Priloga IV.

8. Pretpostavke i pojašnjenje opsega iz stavka 3. točke (e) sadržavaju informacije o okolnostima i ciljevima povezanima s namjenom proizvoda iz članka 7. stavka 1. točke (c) i uključuju sljedeće:

(a) pretpostavke za korištenje i uvođenje IKT proizvoda u obliku minimalnih zahtjeva, npr. da su ispunjeni zahtjevi koji se odnose na pravilnu instalaciju i konfiguraciju te hardver;

(b) pretpostavke za okruženje za rad IKT proizvoda u skladu sa zahtjevima;

(c) opis svih prijetnji IKT proizvodu za koje ne postoje evaluirane sigurnosne funkcije proizvoda koje bi ih neutralizirale u skladu s namjenom, ako se to smatra relevantnim za potencijalne korisnike IKT proizvoda.

Informacije iz prvog podstavka moraju biti što jasnije i razumljivije kako bi potencijalni korisnici certificiranog IKT proizvoda mogli donijeti utemeljene odluke o rizicima povezanima s njegovom upotrebom.

9. Informacije o arhitekturi iz stavka 3. točke (f) moraju sadržavati opis IKT proizvoda i njegovih glavnih komponenti više razine na temelju rezultata definiranih u porodici jamstava iz zajedničkih kriterija: Razvoj – dizajn predmeta evaluacije (ADV_TDS).

10. Dodatne informacije o kibernetičkoj sigurnosti iz stavka 3. točke (g) uključuju poveznicu na internetske stranice nositelja EUCC certifikata iz članka 55. Uredbe (EU) 2019/881.

11. U evaluaciji i konfiguraciji IKT proizvoda iz stavka 3. točke (h) opisuju se aktivnosti ispitivanja i proizvođača i evaluatora te se navode pristup, konfiguracija i detaljnost ispitivanja. Uključuju barem sljedeće informacije:

    (a) identifikacijske podatke o primijenjenim jamstvenim komponentama iz normi iz članka 3.;

    (b) verziju specifikacije najsuvremenijih tehnika i dodatne kriterije za evaluaciju sigurnosti korištene u evaluaciji;

    (c) postavke i konfiguraciju predmeta evaluacije korištene za ispitivanje i analizu ranjivosti;

    (d) korištene profile zaštite, uključujući sljedeće informacije: ime, verziju, datum i certifikat profila zaštite.

12. Rezultati evaluacije i informacije o certifikatu iz stavka 3. točke (i) uključuju informacije o postignutoj razini jamstva iz članka 4. ove Uredbe i članka 52. Uredbe (EU) 2019/881.

13. Primjedbe i preporuke iz stavka 3. točke (j) koriste se za davanje dodatnih informacija o rezultatima evaluacije. U tim primjedbama i preporukama mogu se navesti nedostaci IKT proizvoda utvrđeni tijekom evaluacije ili posebno korisne značajke.

14. Prilozi iz stavka 3. točke (k) koriste se za navođenje svih dodatnih informacija koje bi mogle biti korisne osobama kojima je namijenjeno izvješće, ali se logično ne uklapaju u propisane odjeljke izvješća, među ostalim ako se navodi potpuni opis sigurnosne politike.

15. Potrebna sigurnost iz stavka 3. točke (l) odnosi se na evaluiranu potrebnu sigurnost. Evaluirana potrebna sigurnost navodi se u izvješću o certifikaciji za potrebe objave na internetskim stranicama iz članka 50. stavka 1. Uredbe (EU) 2019/881. Ako je evaluiranu potrebnu sigurnost potrebno pročistiti prije objave, to se provodi u skladu s točkom V.2. Priloga V. ovoj Uredbi.

16. Znakovi ili oznake povezani s EUCC-om iz stavka 3. točke (m) umeću se u izvješće o certifikaciji u skladu s pravilima i postupcima utvrđenima u članku 11.

17. Pojmovnik iz stavka 3. točke (n) koristi se radi boljeg razumijevanja izvješća tako što se u njemu navode definicije pokrata ili pojmova čije značenje možda nije odmah očigledno.

18. Bibliografija iz stavka 3. točke (o) sadržava upućivanja na sve dokumente korištene pri sastavljanju izvješća o certifikaciji. Te informacije uključuju barem sljedeće:

    (a) kriterije za evaluaciju sigurnosti, specifikacije najsuvremenijih tehnika i druge relevantne korištene specifikacije;

    (b) tehničko izvješće o evaluaciji;

    (c) prema potrebi, tehničko izvješće o evaluaciji za složenu evaluaciju;

    (d) tehničku referentnu dokumentaciju;

    (e) sigurnosne smjernice proizvođača;

    (f) popis konfiguracija proizvođača.

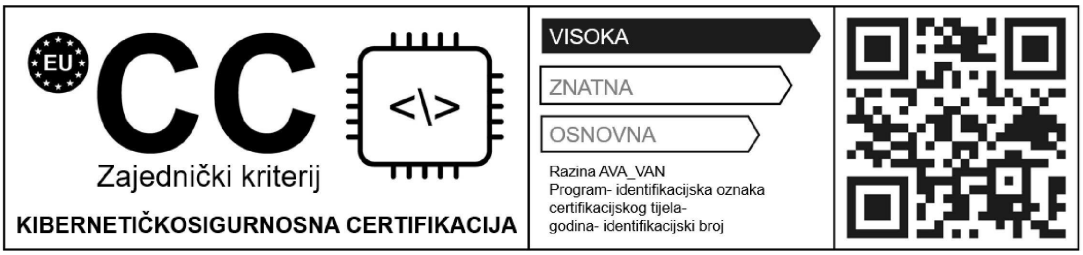
    Kako bi se zajamčila obnovljivost evaluacije, sva navedena dokumentacija mora biti jedinstveno označena ispravnim datumom izdanja i ispravnim brojem verzije.”.

PRILOG VI.

„PRILOG IX.

Oznaka i etiketa

1. Oblik oznake i etikete:



2. Ako se oznaka i etiketa smanje ili povećaju, moraju se zadržati proporcije iz točke 1.

3. Visina fizičke oznake i etikete mora biti najmanje 5 mm.”.