2025/1943

30.9.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1943

od 29. rujna 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu referentnih normi za kvalificirane certifikate za elektroničke potpise i kvalificirane certifikate za elektroničke pečate

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ ([1]), a posebno njezin članak 28. stavak 6. i članak 38. stavak 6.,

budući da:

(1) Kvalificirani certifikati za elektroničke potpise i kvalificirani certifikati za elektroničke pečate imaju bitnu ulogu u digitalnom poslovnom okruženju jer pospješuju prelazak s tradicionalnih postupaka koji koriste papir na elektroničke ekvivalente. Kvalificirani certifikati povećavaju sigurnost u identitet potpisnika i autora pečata time što povezuju podatke za validaciju elektroničkog potpisa ili elektroničkog pečata s fizičkom ili pravnom osobom i potvrđuju ime te osobe.

(2) Pretpostavka sukladnosti utvrđena u članku 28. stavku 6. i članku 38. stavku 6. Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge povjerenja za izdavanje kvalificiranih certifikata za elektroničke potpise i kvalificirane usluge povjerenja za izdavanje kvalificiranih certifikata za elektroničke pečate pridržavaju normi utvrđenih u ovoj Uredbi. Te bi norme trebale odražavati ustaljenu praksu i biti općepriznate u relevantnim sektorima. Trebalo bi ih prilagoditi tako da uključuju dodatne kontrole kojima se jamče sigurnost i vjerodostojnost kvalificiranih usluga povjerenja i sadržaja kvalificiranih certifikata.

(3) Ako pružatelj usluga povjerenja ispunjava zahtjeve utvrđene u Prilogu ovoj Uredbi, nadzorna tijela trebala bi pretpostaviti sukladnost s relevantnim zahtjevima Uredbe (EU) br. 910/2014 i tu pretpostavku primjereno uzeti u obzir kod dodjele ili potvrđivanja kvalificiranog statusa usluge povjerenja. Međutim, kvalificirani pružatelj usluga povjerenja i dalje može na druge načine dokazati sukladnost sa zahtjevima Uredbe (EU) br. 910/2014.

(4) Komisija redovito ocjenjuje nove tehnologije, prakse, norme ili tehničke specifikacije. U skladu s uvodnom izjavom 75. Uredbe (EU) 2024/1183 Europskog parlamenta i Vijeća ([2]) Komisija bi ovu uredbu trebala preispitivati i prema potrebi ažurirati kako bi bila u skladu s globalnim kretanjima, novim tehnologijama, normama ili tehničkim specifikacijama te provjerenim praksama na unutarnjem tržištu.

(5) Na aktivnosti obrade osobnih podataka na temelju ove Uredbe primjenjuju se Uredba (EU) 2016/679 Europskog parlamenta i Vijeća ([3]) i, prema potrebi, Direktiva 2002/58/EZ Europskog parlamenta i Vijeća ([4]).

([1]) SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Uredba (EU) 2024/1183 Europskog parlamenta i Vijeća od 11. travnja 2024. o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostave europskog okvira za digitalni identitet (SL L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([3]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([4]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([5]) te je on dao mišljenje 6. lipnja 2025.

(7) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 48. Uredbe (EU) br. 910/2014,

DONIJELA JE OVU UREDBU:

Članak 1.

Referentne norme i specifikacije za kvalificirane certifikate za elektroničke potpise i elektroničke pečate

1. Referentne norme i specifikacije iz članka 28. stavka 6. Uredbe (EU) br. 910/2014 utvrđene su u Prilogu I. ovoj Uredbi.

2. Referentne norme i specifikacije iz članka 38. stavka 6. Uredbe (EU) br. 910/2014 utvrđene su u Prilogu II. ovoj Uredbi.

Članak 2.

Stupanje na snagu

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 29. rujna 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

([5]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRILOG I.

Popis referentnih normi i specifikacija za kvalificirane certifikate za elektroničke potpise

Primjenjuju se norme ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2”), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1”), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2”) i ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5”) uz sljedeće prilagodbe:

1. Za ETSI EN 319 411-2

(1) 2.1. Normativna upućivanja

— [1] ETSI EN 319 401 V3.1.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Zahtjevi općih pravila za pružatelje usluga povjerenja”.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Zahtjevi za opća pravila i za sigurnost za vjerodostojne davatelje usluga certificiranja – 1. dio: Opći zahtjevi”, uz sljedeće prilagodbe:

točka 2.1. Normativna upućivanja norme ETSI EN 319 411-1 V1.5.1 mijenjaju se kako slijedi:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Zahtjevi općih pravila za pružatelje usluga povjerenja”.

— [10] ETSI EN 319 412-2 V2.4.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 2. dio: Profil certifikata za certifikate koji se izdaju fizičkim osobama”.

— [14] ETSI EN 319 412-1 V1.6.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 1. dio: Pregled i struktura zajedničkih podataka”.

— [3] ETSI EN 319 412-5 V2.5.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 5. dio: QC izjave”.

— [5] ETSI EN 319 412-1 V1.6.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 1. dio: Pregled i struktura zajedničkih podataka”.

— [6] CEN/TS 419261:2015 „Sigurnosni zahtjevi za pouzdane sustave upravljanja certifikatima i vremenskim žigovima”.

— [7] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, publikacija Agencije Europske unije za kibersigurnost („ENISA”) ([1]).

— [8] Provedbena uredba Komisije (EU) 2024/482 ([2]) 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).

— [9] Provedbena uredba Komisije (EU) 2024/3144 ([3]) o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe.

— [10] ISO/IEC 15408:2022 (od 1. do 5. dijela): „Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Kriteriji za vrednovanje sigurnosti IT-a”.

— [11] FIPS PUB 140 – 3 (2019.), Sigurnosni zahtjevi za kriptografske module.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) SL L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 5.2. Zahtjevi za izjavu o certifikacijskoj praksi

— OVR-5.2-02 Zahtjevi za profile certifikata koji će se primjenjivati navode se u CP-ovima utvrđenima u dokumentaciji TSP-a.

(3) 5.3. Ime i identifikacijski podaci certifikatske politike

— OVR-5.3-01 Ako se u CP kako je opisan u točki 4.2.2. unesu bilo kakve izmjene koje utječu na primjenjivost, mora se promijeniti identifikator politike.

(4) 6.1. Dužnosti povezane s objavljivanjem i repozitorijima

— OVR-6.1-02 Informacije utvrđene u DIS-6.1-04 norme ETSI EN 319 411-1 [2] moraju biti javno i međunarodno dostupne.

(5) 6.2.2. Prva validacija identiteta

— REG-6.2.2-01A Prikupljanje atributa i dokaza o identitetu subjekta te njihova validacija moraju biti kako je specificirano u skladu s provedbenim aktima donesenima na temelju članka 24. stavka 1.c Uredbe (EU) br. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] i [QCP-n-qscd] Identitet fizičke osobe i, ako je primjenjivo, svi specifični atributi osobe provjeravaju se u skladu s provedbenim aktima donesenima na temelju članka 24. stavka 1.c Uredbe (EU) br. 910/2014 [i.1].

— Napomena 1. nevažeća.

(6) 6.3.3. Izdavanje certifikata

— GEN-6.3.3-01 Primjenjuju se zahtjevi od GEN-6.3.3-01 do GEN-6.3.3-10 utvrđeni u točki 6.3.3. norme ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 [UVJETNO] Ako se certifikat izdaje fizičkoj osobi identificiranoj u vezi s pravnom osobom, atributi subjekta kojima se identificira organizacija u certifikatu moraju predstavljati pravnu osobu ili podsubjekt te pravne osobe, a identifikator subjekta u certifikatu mora biti fizička osoba.

— GEN-6.3.3-03 Identifikator CP-a je [ODABIR]:

(a) [QCP-n]

— kako je navedeno u točki 5.3. podtočki (a), i/ili

— OID koji dodjeljuje TSP, drugi relevantni dionik ili daljnja standardizacija za certifikatsku politiku koja poboljšava odgovarajuće primjenjive zahtjeve politike utvrđene u ovom dokumentu.

(b) [QCP-n-qscd]

— kako je navedeno u točki 5.3. podtočki (c), i/ili

— OID koji dodjeljuje TSP, drugi relevantni dionik ili daljnja standardizacija za certifikatsku politiku koja poboljšava odgovarajuće primjenjive zahtjeve politike utvrđene u ovom dokumentu.

(7) 6.3.5. Upotreba parova ključeva i certifikata

— SDP-6.3.5-02A [UVJETNO] Ako TSP upravlja QSCD-om za subjekt, TSP mora biti kvalificirani pružatelj usluga povjerenja koji pruža kvalificiranu uslugu povjerenja za upravljanje kvalificiranim sredstvom za izradu elektroničkog potpisa na daljinu, u skladu s Uredbom (EU) br. 910/2014 [i.1].

— SDP-6.3.5-11A Ako ugovaratelj usluge ili subjekt generira ključeve subjekta, obveze ugovaratelja usluge (vidjeti točku 6.3.4.) uključuju:

(a) obvezu generiranja ključeva subjekta korištenjem algoritma sukladnog s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju [7] i objavila ENISA za upotrebu certificiranog ključa kako je utvrđeno u CP-u,

(b) obvezu korištenja duljine ključa i algoritma sukladno s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju [7] i objavila ENISA za upotrebu certificiranog ključa kako je utvrđeno u CP-u tijekom razdoblja valjanosti certifikata.

(8) 6.3.10. Usluge za status certifikata

— CSS-6.3.10-08 [UVJETNO] Ako su dostupni CRL-ovi, TSP čuva cjelovitost i raspoloživost zadnjeg CRL-a barem tijekom razdoblja određenog u CPS-u kako se zahtijeva u CSS-6.3.10-12.

(9) 6.4.4. Provjere osoblja

— OVR-6.4.4-02 Osoblje TSP-a na pouzdanim funkcijama i, ako je primjenjivo, njegovi podugovaratelji na pouzdanim funkcijama, moraju moći ispuniti zahtjev da posjeduju „stručno znanje, iskustvo i kvalifikacije” proizišlo iz formalnog osposobljavanja i relevantnih potvrda ili iz stvarnog iskustva ili iz kombinacije toga.

— OVR-6.4.4-03 Sukladnost s OVR-6.4.4-02 uključuje redovita (najmanje svakih 12 mjeseci) informiranja o novim prijetnjama i aktualnim sigurnosnim praksama.

— OVR-6.4.4-04 Uz pouzdane funkcije utvrđene u ETSI EN 319 401 [1] (točka 7.2.-15), podržane su pouzdane funkcije službenika za registraciju i opoziv s odgovornostima kako je definirano u TS 419261 [6]. U slučajevima kad QTSP-om izravno upravlja država članica ili tijelo javnog sektora ili se njime upravlja u njihovo ime, te dodatne pouzdane funkcije može obavljati jedan ili više službenih predstavnika umjesto i u ime službenika za registraciju i opoziv u lokalnim ili regionalnim upravama.

(10) 6.4.9. Prekid rada CA-a ili RA-a

— OVR-6.4.9-02 TSP-ov plan prekida mora ispunjavati zahtjeve utvrđene u provedbenim aktima donesenima na temelju članka 24. stavka 5. Uredbe (EU) br. 910/2014 [i.1].

(11) 6.5.1. Generiranje i instaliranje parova ključeva

— OVR-6.5.1-01A Generiranje parova ključeva CA-a radi se korištenjem algoritma sukladnog s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za CA-ove potrebe potpisivanja.

— OVR-6.5.1-01B Odabrana duljina ključa i algoritam za potpisni ključ CA-a moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za CA-ove potrebe potpisivanja.

— OVR-6.5.1-01C [UVJETNO] Ako CA generira ključeve subjekta, ključevi subjekta koje je generirao CA moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za potrebe navedene u CP-u tijekom razdoblja valjanosti certifikata.

(12) 6.5.2. Zaštita privatnih ključeva i tehničke kontrole kriptografskog modula

— GEN-6.5.2-01 Primjenjuju se svi zahtjevi utvrđeni u točki 6.5.2. norme ETSI EN 319 411-1 [2], osim zahtjeva OVR-6.5.2-01, OVR-6.5.2-03 i OVR-6.5.2-04.

— GEN-6.5.2-02 Generiranje parova ključeva TSP-a, uključujući ključeve koje koriste usluge opoziva i registracije, radi se unutar sigurnog kriptografskog uređaja koji je pouzdan sustav certificiran u skladu:

— sa zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normi ISO/IEC 15408 [10] ili u zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije, verzija CC:2002, od 1. do 5. dijela, publikacija sudionika Sporazuma o priznavanju certifikata na temelju zajedničkih kriterija u području IT sigurnosti, te certificiran na razini EAL 4 ili višoj, ili

— s europskim programom kibernetičkosigurnosne certifikacije temeljenim na zajedničkim kriterijima (EUCC) [8][9] i certificiran na razini EAL 4 ili višoj, ili

— do 31.12.2030. normom FIPS PUB 140-3 [11] na razini 3.

Ta se certifikacija radi s obzirom na potrebnu sigurnost ili profil zaštite ili na izvedbu modula i sigurnosnu dokumentaciju, koji ispunjavaju zahtjeve ovog dokumenta, na temelju analize rizika i uzimajući u obzir fizičke i druge netehničke sigurnosne mjere.

Ako se na sigurni kriptografski uređaj primjenjuje EUCC [8][9] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom,

— GEN-6.5.2-03 Privatni potpisni ključ CA-a čuva se i koristi unutar sigurnog kriptografskog uređaja koji ispunjava zahtjeve GEN-6.5.2-01 i GEN-6.5.2-02.

(13) 6.5.7. Mjere mrežne sigurnosti

— OVR-6.5.7-02 Potraga za ranjivim točkama koja je obvezna prema REQ-7.8-13 norme ETSI EN 319 401 [1] obavlja se najmanje svaka tri mjeseca.

— OVR-6.5.7-03 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319 401 [1] obavlja se najmanje jedanput u godini.

— OVR-6.5.7-04 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad TSP-a.

(14) 6.6.1. Profil certifikata

— GEN-6.6.1-05 Certifikat mora sadržavati jedan od identifikatora politike navedenih u GEN-6.3.3-03 [ODABIR]. Certifikat može sadržavati druge OID-ove koje je dodijelio TSP.

2. Za ETSI EN 319 412-2

(1) 2.1. Normativna upućivanja

— [2] ETSI EN 319 412-5 V2.5.1 – Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 5. dio: QC izjave".

— [9] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi", publikacija ENISA-e.

(2) 4.2.2. Potpis

— GEN-4.2.2-2 Potpisni algoritam odabire se u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [9].

— NAPOMENA nevažeća.

(3) 4.2.3.1. Izdavatelji koji su pravne osobe

— GEN-4.2.3.1-3 Ako je poznato da postoji odgovarajući registracijski broj, identitet izdavatelja mora sadržavati „organizationIdentifier” s tim registracijskim brojem kako je naveden u odgovarajućoj javnoj ispravi kojom je utvrđen.

(4) 4.2.5. Informacije o javnom ključu subjekta

— GEN-4.2.5-2 Javni ključ subjekta odabire se u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [9].

— NAPOMENA nevažeća.

(5) 4.2.6. Serijski broj

— GEN-4.2.6-01 Certifikatov „serialNumber” (kako je specificiran u točki 4.1.2.2. norme IETF RFC 5280 [1]) mora biti jedinstven za svaki certifikat koji je izdao TSP.

PRILOG II.

Popis referentnih normi i specifikacija za kvalificirane certifikate za elektroničke pečate

Primjenjuju se norme ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2”), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1”), ETSI EN 319 412-3 V1.3.1 („ETSI EN 319 412-3”), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2”) i ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5”) uz sljedeće prilagodbe:

1. Za ETSI EN 319 411-2

(1) 2.1. Normativna upućivanja

— [1] ETSI EN 319 401 V3.1.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Zahtjevi općih pravila za pružatelje usluga povjerenja”.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Zahtjevi za opća pravila i za sigurnost za vjerodostojne davatelje usluga certificiranja – 1. dio: Opći zahtjevi”, uz sljedeće prilagodbe:

točka 2.1. Normativna upućivanja norme ETSI EN 319 411-1 V1.5.1 mijenjaju se kako slijedi:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Zahtjevi općih pravila za pružatelje usluga povjerenja”.

— [10] ETSI EN 319 412-2 V2.4.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 2. dio: Profil certifikata za certifikate koji se izdaju fizičkim osobama”.

— [14] ETSI EN 319 412-1 V1.6.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 1. dio: Pregled i struktura zajedničkih podataka”.

— [3] ETSI EN 319 412-5 V2.5.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 5. dio: QC izjave”.

— [5] ETSI EN 319 412-1 V1.6.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 1. dio: Pregled i struktura zajedničkih podataka”.

— [6] CEN/TS 419261:2015 „Sigurnosni zahtjevi za pouzdane sustave upravljanja certifikatima i vremenskim žigovima”, (izradio CEN).

— [7] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, objavila ENISA.

— [8] Provedbena uredba (EU) 2024/482 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).

— [9] Provedbena uredba (EU) 2024/3144 o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe.

— [10] ISO/IEC 15408:2022 (dijelovi od 1. do 5.) „Sigurnost informacija, kibernetička sigurnost i zaštita privatnosti – Kriteriji za evaluaciju informatičke sigurnosti”.

— [11] FIPS PUB 140 – 3 (2019.), Sigurnosni zahtjevi za kriptografske module.

(2) 5.2. Zahtjevi za izjavu o certifikacijskoj praksi

— OVR-5.2-02 Zahtjevi za profile certifikata koji će se primjenjivati navode se u CP-ovima utvrđenima u dokumentaciji TSP-a.

(3) 5.3. Ime i identifikacijski podaci certifikatske politike

— OVR-5.3-01 Ako se u CP kako je opisan u točki 4.2.2. unesu bilo kakve izmjene koje utječu na primjenjivost, mora se promijeniti identifikator politike.

(4) 6.1. Dužnosti povezane s objavljivanjem i repozitorijima

— OVR-6.1-02 Informacije utvrđene u DIS-6.1-04 norme ETSI EN 319 411-1 [2] moraju biti javno i međunarodno dostupne.

(5) 6.2.2. Prva validacija identiteta

— REG-6.2.2-01A Prikupljanje atributa i dokaza o identitetu subjekta te njihova validacija moraju biti kako je specificirano u skladu s provedbenim aktima donesenima na temelju članka 24. stavka 1.c Uredbe (EU) br. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] i [QCP-l-qscd] Identitet pravne osobe i, ako je primjenjivo, svi specifični atributi osobe provjeravaju se u skladu s provedbenim aktima donesenima na temelju članka 24. stavka 1.c Uredbe (EU) br. 910/2014 [i.1].

— NAPOMENA 3. Vidjeti napomenu 2.

(6) 6.3.3. Izdavanje certifikata

— GEN-6.3.3-01 Primjenjuju se zahtjevi od GEN-6.3.3-01 do GEN-6.3.3-10 utvrđeni u točki 6.3.3. norme ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 Identifikator CP-a je [ODABIR]:

(a) [QCP-l]

— kako je navedeno u točki 5.3. podtočki (b), i/ili

— OID koji dodjeljuje TSP, drugi relevantni dionik ili daljnja standardizacija za certifikatsku politiku koja poboljšava odgovarajuće primjenjive zahtjeve politike utvrđene u ovom dokumentu.

(b) [QCP-n-qscd]

— kako je navedeno u točki 5.3. podtočki (d), i/ili

— OID koji dodjeljuje TSP, drugi relevantni dionik ili daljnja standardizacija za certifikatsku politiku koja poboljšava primjenjive zahtjeve politike utvrđene u ovom dokumentu.

(7) 6.3.5. Upotreba parova ključeva i certifikata

— SDP-6.3.5-02A [UVJETNO] Ako TSP upravlja QSCD-om za subjekt, TSP mora biti kvalificirani pružatelj usluga povjerenja koji pruža kvalificiranu uslugu povjerenja za upravljanje kvalificiranim sredstvom za izradu elektroničkog pečata na daljinu, u skladu s Uredbom (EU) br. 910/2014 [i.1].

— SDP-6.3.5-11A Ako ugovaratelj usluge ili subjekt generira ključeve subjekta, obveze ugovaratelja usluge (vidjeti točku 6.3.4.) uključuju:

(a) obvezu generiranja ključeva subjekta korištenjem algoritma sukladnog s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za upotrebu certificiranog ključa kako je utvrđeno u CP-u, i

(b) obvezu korištenja duljine ključa i algoritma sukladno s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za upotrebu certificiranog ključa kako je utvrđeno u CP-u tijekom razdoblja valjanosti certifikata.

(8) 6.3.10. Usluge za status certifikata

— CSS-6.3.10-08 [UVJETNO] Ako su dostupni CRL-ovi, TSP čuva cjelovitost i raspoloživost zadnjeg CRL-a barem tijekom razdoblja određenog u CPS-u kako se zahtijeva u CSS-6.3.10-12.

(9) 6.4.4. Provjere osoblja

— OVR-6.4.4-02 Osoblje TSP-a na pouzdanim funkcijama i, ako je primjenjivo, njegovi podugovaratelji na pouzdanim funkcijama, moraju moći ispuniti zahtjev da posjeduju „stručno znanje, iskustvo i kvalifikacije" proizišlo iz formalnog osposobljavanja i relevantnih potvrda ili iz stvarnog iskustva ili iz kombinacije toga.

— OVR-6.4.4-03 Sukladnost s OVR-6.4.4-02 uključuje redovita (najmanje svakih 12 mjeseci) informiranja o novim prijetnjama i aktualnim sigurnosnim praksama.

— OVR-6.4.4-04 Uz pouzdane funkcije utvrđene u ETSI EN 319 401 [1] (točka 7.2.-15), podržane su pouzdane funkcije službenika za registraciju i opoziv s odgovornostima kako je definirano u TS 419261 [6]. U slučajevima kad QTSP-om izravno upravlja država članica ili tijelo javnog sektora ili se njime upravlja u njihovo ime, te dodatne pouzdane funkcije može obavljati jedan ili više službenih predstavnika umjesto i u ime službenika za registraciju i opoziv u lokalnim ili regionalnim upravama.

(10) 6.4.9. Prekid rada CA-a ili RA-a

— OVR-6.4.9-02 TSP-ov plan prekida mora ispunjavati zahtjeve utvrđene u provedbenim aktima donesenima na temelju članka 24. stavka 5. Uredbe (EU) br. 910/2014 [i.1]].

(11) 6.5.1. Generiranje i instaliranje parova ključeva

— OVR-6.5.1-01A Generiranje parova ključeva CA-a radi se korištenjem algoritma sukladnog s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za CA-ove potrebe potpisivanja.

— OVR-6.5.1-01B Odabrana duljina ključa i algoritam za potpisni ključ CA-a moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za CA-ove potrebe potpisivanja.

— OVR-6.5.1-01C [UVJETNO] Ako CA generira ključeve subjekta, ključevi subjekta koje je generirao CA moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [7] za potrebe navedene u CP-u tijekom razdoblja valjanosti certifikata.

(12) 6.5.2. Zaštita privatnih ključeva i tehničke kontrole kriptografskog modula

— GEN-6.5.2-01 Primjenjuju se svi zahtjevi utvrđeni u točki 6.5.2. norme ETSI EN 319 411-1 [2], osim zahtjeva OVR-6.5.2-01, OVR-6.5.2-03 i OVR-6.5.2-04.

— GEN-6.5.2-02 Generiranje parova ključeva TSP-a, uključujući ključeve koje koriste usluge opoziva i registracije, radi se unutar sigurnog kriptografskog uređaja koji je pouzdan sustav certificiran u skladu:

  — sa zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normi ISO/IEC 15408 [10] ili u zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije, verzija CC:2002, od 1. do 5. dijela, publikacija sudionika Sporazuma o priznavanju certifikata na temelju zajedničkih kriterija u području IT sigurnosti, te certificiran na razini EAL 4 ili višoj, ili

  — s europskim programom kibernetičkosigurnosne certifikacije temeljenim na zajedničkim kriterijima (EUCC) [8][9] i certificiran na razini EAL 4 ili višoj, ili

  — do 31.12.2030. normom FIPS PUB 140-3 [11] na razini 3.

Ta se certifikacija radi s obzirom na potrebnu sigurnost ili profil zaštite ili na izvedbu modula i sigurnosnu dokumentaciju, koji ispunjavaju zahtjeve ovog dokumenta, na temelju analize rizika i uzimajući u obzir fizičke i druge netehničke sigurnosne mjere.

Ako se na sigurni kriptografski uređaj primjenjuje EUCC [8][9] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom,

— GEN-6.5.2-03 Privatni potpisni ključ CA-a čuva se i koristi unutar sigurnog kriptografskog uređaja koji ispunjava zahtjeve GEN-6.5.2-01 i GEN-6.5.2-02.

(13) 6.5.7. Mjere mrežne sigurnosti

— OVR-6.5.7-02 Potraga za ranjivim točkama koja je obvezna prema REQ-7.8-13 norme ETSI EN 319 401 [1] obavlja se najmanje svaka tri mjeseca.

— OVR-6.5.7-03 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319 401 [1] obavlja se najmanje jedanput u godini.

— OVR-6.5.7-04 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad TSP-a.

(14) 6.6.1. Profil certifikata

— GEN-6.6.1-05 Certifikat mora sadržavati jedan od identifikatora politike navedenih u GEN-6.3.3-02 [ODABIR].

2. Za ETSI EN 319 412-3

(1) 2.1. Normativna upućivanja

— [2] ETSI EN 319 412-2 V2.4.1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 2. dio: Profil certifikata za certifikate koji se izdaju fizičkim osobama”.

(2) 4.2.1. Subjekt

— LEG-4.2.1-6 Atribut „organizationIdentifier” mora sadržavati identifikacijsku oznaku organizacije subjekta koja se razlikuje od imena organizacije. Ako je poznato da postoji odgovarajući registracijski broj, atribut „organizationIdentifier” mora sadržavati taj registracijski broj kako je naveden u odgovarajućoj javnoj ispravi kojom je utvrđen.

3. Za ETSI EN 319 412-2:

(1) 2.1. Normativna upućivanja

— [2] ETSI EN 319 412-5 V2.5.1 – Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Profili certifikata – 5. dio: QC izjave”.

— [9] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, objavila ENISA.

(2) 2.2. Informativna upućivanja

— [i.7] nevažeće.

(3) 4.2.2. Potpis

— GEN-4.2.2-2 Potpisni algoritam odabire se u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [9].

— NAPOMENA nevažeća.

(4) 4.2.3.1. Izdavatelji koji su pravne osobe

— GEN-4.2.3.1-3 Ako je poznato da postoji odgovarajući registracijski broj, identitet izdavatelja mora sadržavati „organizationIdentifier” s tim registracijskim brojem kako je naveden u odgovarajućoj javnoj ispravi kojom je utvrđen.

(5) 4.2.5. Informacije o javnom ključu subjekta

— GEN-4.2.5-2 Javni ključ subjekta odabire se u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [9].

— NAPOMENA nevažeća.

(6) 4.2.6. Serijski broj

— GEN-4.2.6-01 Certifikatov „serialNumber” (kako je specificiran u točki 4.1.2.2. norme IETF RFC 5280 [1]) mora biti jedinstven za svaki certifikat koji je izdao TSP.