Uradni list
Evropske unije

SL
Serija L

2025/1943

30.9.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/1943

z dne 29. septembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede referenčnih standardov za kvalificirana potrdila za elektronske podpise in kvalificirana potrdila za elektronske žige

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) ter zlasti člena 28(6) in člena 38(6) Uredbe,

ob upoštevanju naslednjega:

(1) Kvalificirana potrdila za elektronske podpise in kvalificirana potrdila za elektronske žige imajo ključno vlogo v digitalnem poslovnem okolju, saj spodbujajo prehod s tradicionalnih papirnih postopkov na enakovredne elektronske postopke. Kvalificirana potrdila s povezovanjem podatkov za potrjevanje veljavnosti elektronskega podpisa ali podatkov za potrjevanje veljavnosti elektronskega žiga s fizično ali pravno osebo in s potrditvijo imena te osebe povečujejo gotovost glede identitete podpisnika in ustvarjalca žiga.

(2) Domneva o skladnosti iz člena 28(6) in člena 38(6) Uredbe (EU) št. 910/2014 bi se morala uporabljati le, kadar so kvalificirane storitve zaupanja za izdajo kvalificiranih potrdil za elektronske podpise in kvalificirane storitve zaupanja za izdajo kvalificiranih potrdil za elektronske žige skladne s standardi iz te uredbe. Ti standardi bi morali odražati uveljavljene prakse in biti splošno priznani v ustreznih sektorjih. Prilagoditi bi jih bilo treba tako, da bi vključevali dodaten nadzor, ki bi zagotavljal varnost in zanesljivost kvalificiranih storitev zaupanja in vsebine kvalificiranih potrdil.

(3) Če ponudnik storitev zaupanja izpolnjuje zahteve iz Priloge k tej uredbi, bi morali nadzorni organi domnevati skladnost z ustreznimi zahtevami iz Uredbe (EU) št. 910/2014 in ustrezno upoštevati tako domnevo za podelitev ali potrditev kvalificiranega statusa storitve zaupanja. Vendar se lahko ponudnik kvalificiranih storitev zaupanja pri dokazovanju skladnosti z zahtevami iz Uredbe (EU) št. 910/2014 še vedno zanaša na druge prakse.

(4) Komisija redno ocenjuje nove tehnologije, prakse, standarde ali tehnične specifikacije. V skladu z uvodno izjavo 75 Uredbe (EU) 2024/1183 Evropskega parlamenta in Sveta ([2]) bi morala Komisija pregledovati in po potrebi posodabljati to izvedbeno uredbo, da bi bila usklajena s svetovnim razvojem, novimi tehnologijami, standardi ali tehničnimi specifikacijami ter sledila najboljšim praksam na notranjem trgu.

(5) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ([3]) in, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([4]) se uporabljata za dejavnosti obdelave osebnih podatkov na podlagi te uredbe.

([1]) UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Uredba (EU) 2024/1183 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto (UL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([5]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 6. junija 2025.

(7) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Referenčni standardi in specifikacije za kvalificirana potrdila za elektronske podpise in elektronske žige

1. Referenčni standardi in specifikacije iz člena 28(6) Uredbe (EU) št. 910/2014 so določeni v Prilogi I k tej uredbi.

2. Referenčni standardi in specifikacije iz člena 38(6) Uredbe (EU) št. 910/2014 so določeni v Prilogi II k tej uredbi.

Člen 2

Začetek veljavnosti

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, 29. septembra 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

([5]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRILOGA I

Seznam referenčnih standardov in specifikacij za kvalificirana potrdila za elektronske podpise

Standardi 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“) in ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) se uporabljajo z naslednjimi prilagoditvami:

1. Za ETSI EN 319 411-2

(1) 2.1 Normativne reference

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Splošne zahteve politike za ponudnike storitev zaupanja“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo digitalna potrdila – 1. del: Splošne zahteve“ z naslednjimi prilagoditvami:

Določba 2.1 Normativne reference ETSI EN 319 411-1 V1.5.1 se spremenijo:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Splošne zahteve politike za ponudnike storitev zaupanja“.

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 2. del: Profil potrdila za potrdila, izdana fizičnim osebam“.

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 1. del: Pregled in skupne podatkovne strukture“.

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – Del 5: Izjave QC“.

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 1. del: Pregled in skupne podatkovne strukture“.

— [6] CEN/TS 419261:2015 „Varnostne zahteve za zaupanja vredne sisteme, ki upravljajo potrdila in časovne žige“.

— [7] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ([1]).

— [8] Izvedbena uredba Komisije (EU) 2024/482 o določitvi pravil za uporabo Uredbe (EU) 2019/881 ([2]) Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih.

— [9] Izvedbena uredba Komisije (EU) 2024/3144 ([3]) o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.

— [10] ISO/IEC 15408:2022 (1. do 5. del): „Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Merila za vrednotenje varnosti IT“.

— [11] FIPS PUB 140-3 (2019) „Varnostne zahteve za kriptografske module“.

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

(2) 5.2 Zahteve za izjave o praksi certificiranja

— OVR-5.2-02 CP, opredeljene v dokumentaciji TSP, določajo zahteve glede profilov potrdil, ki jih je treba uporabiti.

(3) 5.3 Ime in opredelitev politike potrdil

— OVR-5.3-01 Če se CP spremeni, kot je opisano v določbi 4.2.2, kar vpliva na veljavnost, se spremeni tudi identifikator politike.

(4) 6.1 Odgovornosti v zvezi z objavo in repozitorijem

— OVR-6.1-02 Informacije iz DIS-6.1-04 ETSI EN 319 411-1 [2] morajo biti javno in mednarodno dostopne.

(5) 6.2.2 Začetna potrditev istovetnosti

— REG-6.2.2-01A Zbiranje atributov in dokazov o identiteti subjekta ter njihovo potrjevanje se določita v skladu z izvedbenimi akti, sprejetimi na podlagi člena 24(1c) Uredbe (EU) št. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] in [QCP-n-qscd] Identiteta fizične osebe in po potrebi njeni posebni atributi se preverijo v skladu z izvedbenimi akti, sprejetimi na podlagi člena 24(1c) Uredbe (EU) št. 910/2014 [i.1].

— OPOMBA 1 neveljavna.

(6) 6.3.3 Izdaja potrdil

— GEN-6.3.3-01 Uporabljajo se zahteve GEN-6.3.3-01 do GEN-6.3.3-10, opredeljene v določbi 6.3.3 ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 [POGOJNO] Če se potrdilo izda fizični osebi, opredeljeni v povezavi s pravno osebo, potem atributi subjekta, ki opredeljujejo organizacijo v potrdilu, predstavljajo pravno osebo ali podsubjekt te pravne osebe, identifikator subjekta v potrdilu pa je fizična oseba.

— GEN-6.3.3-03 Identifikator CP je [IZBIRA]:

(a) [QCP-n]

— kot je določeno v določbi 5.3, točka (a), in/ali

— OID, ki ga dodeli TSP, drugi zadevni deležnik ali nadaljnja standardizacija za politiko potrdil, ki krepi ustrezne veljavne zahteve politike, opredeljene v tem dokumentu.

(b) [QCP-n-qscd]

— kot je določeno v določbi 5.3, točka (c), in/ali

— OID, ki ga dodeli TSP, drugi zadevni deležnik ali nadaljnja standardizacija za politiko potrdil, ki krepi ustrezne veljavne zahteve politike, opredeljene v tem dokumentu.

(7) 6.3.5 Uporaba para ključev in potrdil

— SDP-6.3.5-02A [POGOJNO] Če TSP upravlja QSCD za subjekt, je TSP ponudnik kvalificiranih storitev zaupanja, ki zagotavlja kvalificirano storitev zaupanja za upravljanje naprave za ustvarjanje kvalificiranega elektronskega podpisa na daljavo v skladu z Uredbo (EU) št. 910/2014 [i.1].

— SDP-6.3.5-11A Obveznosti naročnika (glej določbo 6.3.4), če naročnik ali subjekt ustvari ključe subjekta, vključujejo:

(a) obveznost ustvarjanja ključev z uporabo algoritma, skladnega z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost [7] in objavila ENISA, za uporabe certificiranega ključa, kot je opredeljen v CP;

(b) obveznost uporabe dolžine ključa in algoritma, skladnih z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost [7] in objavila ENISA, za uporabe certificiranega ključa, kot je opredeljen v CP med veljavnostjo potrdila.

(8) 6.3.10 Storitve za preverjanje statusa veljavnosti potrdila

— CSS-6.3.10-08 [POGOJNO] Če so zagotovljeni CRL, mora TSP ohraniti celovitost in razpoložljivost zadnjega CRL vsaj za obdobje, določeno v CPS, kot se zahteva v CSS-6.3.10-12.

(9) 6.4.4 Nadzor osebja

— OVR-6.4.4-02 Osebje TSP v zaupanja vrednih vlogah in, kadar je to ustrezno, podizvajalci v zaupanja vrednih vlogah so sposobni izpolnjevati zahtevo po „strokovnem znanju, izkušnjah in kvalifikacijah“, pridobljenih s formalnim usposabljanjem in poverilnicami, ali dejanskih izkušnjah ali kombinacijo obeh.

— OVR-6.4.4-03 Skladnost z OVR-6.4.4-02 vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

— OVR-6.4.4-04 Poleg zaupanja vrednih vlog, opredeljenih v ETSI EN 319 401 [1] (določba 7.2-15), se podprejo zaupanja vredne vloge uradnikov za registracijo in preklic z odgovornostmi, kot so opredeljene v TS 419261 [6]. Kadar QTSP neposredno upravlja ali deluje v imenu države članice ali organa javnega sektorja, lahko te dodatne zaupanja vredne vloge izpolnjuje eden ali več uradnih predstavnikov, ki nastopajo v vlogi in v imenu uradnikov za registracijo in preklic, ki delujejo v lokalnih ali regionalnih upravah.

(10) 6.4.9 Prenehanje CA ali RA

— OVR-6.4.9-02 Načrt za prenehanje TSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.1].

(11) 6.5.1 Ustvarjanje in namestitev parov ključev

— OVR-6.5.1-01A Ustvarjanje para ključev CA se izvede z algoritmom, skladnim z dogovorjenimi kriptografskimi mehanizmi, ki jih je za namene podpisa CA podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7].

— OVR-6.5.1-01B Izbrana dolžina ključa in algoritem za ključ CA za podpisovanje, skladnim z dogovorjenimi kriptografskimi mehanizmi, ki jih je za namene podpisa CA podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7].

— OVR-6.5.1-01C [POGOJNO] Če CA ustvari ključe subjekta, morajo biti ti ključi skladni z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7], za namene, navedene v CP, med veljavnostjo potrdila.

(12) 6.5.2 Zaščita zasebnih ključev in nadzor nad zasnovo kriptografskih modulov

— GEN-6.5.2-01 Uporabljajo se vse zahteve iz določbe 6.5.2 ETSI EN 319 411-1 [2], razen zahtev OVR-6.5.2-01, OVR-6.5.2-03 in OVR-6.5.2-04.

— GEN-6.5.2-02 Ustvarjanje para ključev TSP, vključno s ključi, ki jih uporabljajo storitve preklica in registracije, se izvede v okviru varne kriptografske naprave, ki je zaupanja vreden sistem, certificiran v skladu s:

— skupnimi merili za ocenjevanje varnosti informacijske tehnologije, kot so določena v ISO/IEC 15408 [10] ali v skupnih merilih za ocenjevanje varnosti informacijske tehnologije, različica CC:2002, deli 1 do 5, ki so jih objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih merilih na področju varnosti IT, in po EAL 4 ali višje; ali

— evropsko certifikacijsko shemo za kibernetsko varnost, ki temelji na skupnih merilih (EUCC) [8][9], in po EAL 4 ali višje; ali

— do 31. decembra 2030, FIPS PUB 140-3 [11] stopnja 3.

To certificiranje se izvede za varnostni cilj ali profil zaščite ali zasnovo modula in varnostno dokumentacijo, ki izpolnjuje zahteve tega dokumenta, na podlagi analize tveganja in ob upoštevanju fizičnih in drugih netehničnih varnostnih ukrepov.

Če je varna kriptografska naprava certificirana po EUCC [8][9], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— GEN-6.5.2-03 Zasebni ključ CA za podpisovanje se hrani in uporablja v varni kriptografski napravi, ki izpolnjuje zahteve iz GEN-6.5.2-01 in GEN-6.5.2-02.

(13) 6.5.7 Nadzor varnosti omrežja

— OVR-6.5.7-02 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtletje.

— OVR-6.5.7-03 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.

— OVR-6.5.7-04 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje TSP.

(14) 6.6.1 Profil potrdila

— GEN-6.6.1-05 Potrdilo vključuje enega od identifikatorjev politike, opredeljenih v GEN-6.3.3-03 [IZBIRA]. Potrdilo lahko vključuje druge OID, ki jih dodeli TSP.

2. Za ETSI EN 319 412-2

(1) 2.1 Normativne reference

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – Del 5: Izjave QC“.

— [9] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila ENISA.

(2) 4.2.2 Podpis

— GEN-4.2.2-2 Algoritem za podpis se izbere v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [9].

— OPOMBA neveljavna.

(3) 4.2.3.1 Izdajatelji pravnih oseb

— GEN-4.2.3.1-3 Če je znano, da obstaja ustrezna registracijska številka, identiteta izdajatelja vsebuje identifikator organizacije z vrednostjo te registracijske številke, kot je navedena v ustreznem uradnem zapisu, ki določa to registracijsko številko.

(4) 4.2.5 Informacije o javnem ključu subjekta

— GEN-4.2.5-2 Javni ključ subjekta se izbere v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [9].

— OPOMBA neveljavna.

(5) 4.2.6 Serijska številka

— GEN-4.2.6-01 Serijska številka potrdila (kot je določena v določbi 4.1.2.2 IETF RFC 5280 [1]) mora biti enotna za vsako potrdilo, ki ga izda TSP.

PRILOGA II

Seznam referenčnih standardov in specifikacij za kvalificirana potrdila za elektronske žige

Standardi 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“) in ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5“) se uporabljajo z naslednjimi prilagoditvami:

1. Za ETSI EN 319 411-2

(1) 2.1 Normativne reference

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Splošne zahteve politike za ponudnike storitev zaupanja“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo digitalna potrdila – 1. del: Splošne zahteve“ z naslednjimi prilagoditvami:

Določba 2.1 Normativne reference ETSI EN 319 411-1 V1.5.1 se spremenijo:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Splošne zahteve politike za ponudnike storitev zaupanja“.

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 2. del: Profil potrdila za potrdila, izdana fizičnim osebam“.

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 1. del: Pregled in skupne podatkovne strukture“.

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – Del 5: Izjave QC“.

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 1. del: Pregled in skupne podatkovne strukture“.

— [6] CEN/TS 419261:2015 „Varnostne zahteve za zaupanja vredne sisteme, ki upravljajo potrdila in časovne žige“, (ki jih je ustvaril Evropski odbor za standardizacijo (CEN).

— [7] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila ENISA.

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

— [9] Izvedbena uredba (EU) 2024/3144 o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.

— [10] ISO/IEC 15408:2022 (deli 1 do 5) „Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Merila za vrednotenje varnosti IT“.

— [11] FIPS PUB 140-3 (2019) „Varnostne zahteve za kriptografske module“.

(2) 5.2 Zahteve za izjave o praksi certificiranja

— OVR-5.2-02 CP, opredeljene v dokumentaciji TSP, določajo zahteve glede profilov potrdil, ki jih je treba uporabiti.

(3) 5.3 Ime in opredelitev politike potrdil

— OVR-5.3-01 Če se CP spremeni, kot je opisano v določbi 4.2.2, kar vpliva na veljavnost, se spremeni tudi identifikator politike.

(4) 6.1 Odgovornosti v zvezi z objavo in repozitorijem

— OVR-6.1-02 Informacije iz DIS-6.1-04 ETSI EN 319 411-1 [2] morajo biti javno in mednarodno dostopne.

(5) 6.2.2 Začetna potrditev istovetnosti

— REG-6.2.2-01A Zbiranje atributov in dokazov o identiteti subjekta ter njihovo potrjevanje se določita v skladu z izvedbenimi akti, sprejetimi na podlagi člena 24(1c) Uredbe (EU) št. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] in [QCP-l-qscd] Identiteta pravne osebe in po potrebi njeni posebni atributi se preverijo v skladu z izvedbenimi akti, sprejetimi na podlagi člena 24(1c) Uredbe (EU) št. 910/2014 [i.1].

— OPOMBA 3: Glej opombo 2.

(6) 6.3.3 Izdaja potrdil

— GEN-6.3.3-01 Uporabljajo se zahteve GEN-6.3.3-01 do GEN-6.3.3-10, opredeljene v določbi 6.3.3 ETSI EN 319 411-1 [2].

— GEN-6.3.3-02 Identifikator CP je [IZBIRA]:

(a) [QCP-l]

— kot je določeno v določbi 5.3, točka (b), in/ali

— OID, ki ga dodeli TSP, drugi zadevni deležnik ali nadaljnja standardizacija za politiko potrdil, ki krepi ustrezne veljavne zahteve politike, opredeljene v tem dokumentu.

(b) [QCP-l-qscd]

— kot je določeno v določbi 5.3, točka (d), in/ali

— OID, ki ga dodeli TSP, drugi zadevni deležnik ali pri nadaljnji standardizaciji za politiko potrdil, ki krepi veljavne zahteve politike, opredeljene v tem dokumentu.

(7) 6.3.5 Uporaba para ključev in potrdil

— SDP-6.3.5-02A [POGOJNO] Če TSP upravlja QSCD za subjekt, je TSP ponudnik kvalificiranih storitev zaupanja, ki zagotavlja kvalificirano storitev zaupanja za upravljanje naprave za ustvarjanje kvalificiranega elektronskega žiga na daljavo v skladu z Uredbo (EU) št. 910/2014 [i.1].

— SDP-6.3.5-11A Obveznosti naročnika (glej določbo 6.3.4), če naročnik ali subjekt ustvari ključe subjekta, vključujejo:

(a) obveznost ustvarjanja ključev z uporabo algoritma, skladnega z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7], za uporabe certificiranega ključa, kot je opredeljen v CP, ter

(b) obveznost uporabe dolžine ključa in algoritma, skladnih z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7], za uporabe certificiranega ključa, kot je opredeljen v CP med veljavnostjo potrdila.

(8) 6.3.10 Storitve za preverjanje statusa veljavnosti potrdila

— CSS-6.3.10-08 [POGOJNO] Če so zagotovljeni CRL, mora TSP ohraniti celovitost in razpoložljivost zadnjega CRL vsaj za obdobje, določeno v CPS, kot se zahteva v CSS-6.3.10-12.

(9) 6.4.4 Nadzor osebja

— OVR-6.4.4-02 Osebje TSP v zaupanja vrednih vlogah in, kadar je to ustrezno, podizvajalci v zaupanja vrednih vlogah so sposobni izpolnjevati zahtevo po „strokovnem znanju, izkušnjah in kvalifikacijah“, pridobljenih s formalnim usposabljanjem in poverilnicami, ali dejanskih izkušnjah ali kombinacijo obeh.

— OVR-6.4.4-03 Skladnost z OVR-6.4.4-02 vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

— OVR-6.4.4-04 Poleg zaupanja vrednih vlog, opredeljenih v ETSI EN 319 401 [1] (določba 7.2-15), se podprejo zaupanja vredne vloge uradnikov za registracijo in preklic z odgovornostmi, kot so opredeljene v TS 419261 [6]. Kadar QTSP neposredno upravlja ali deluje v imenu države članice ali organa javnega sektorja, lahko te dodatne zaupanja vredne vloge izpolnjuje eden ali več uradnih predstavnikov, ki nastopajo v vlogi in v imenu uradnikov za registracijo in preklic, ki delujejo v lokalnih ali regionalnih upravah.

(10) 6.4.9 Prenehanje CA ali RA

— OVR-6.4.9-02 Načrt za prenehanje TSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.1]].

(11) 6.5.1 Ustvarjanje in namestitev parov ključev

— OVR-6.5.1-01A Ustvarjanje para ključev CA se izvede z algoritmom, skladnim z dogovorjenimi kriptografskimi mehanizmi, ki jih je za namene podpisa CA podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7].

— OVR-6.5.1-01B Izbrana dolžina ključa in algoritem za ključ CA za podpisovanje, skladnim z dogovorjenimi kriptografskimi mehanizmi, ki jih je za namene podpisa CA podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7].

— OVR-6.5.1-01C [POGOJNO] Če CA ustvari ključe subjekta, morajo biti ti ključi skladni z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [7], za namene, navedene v CP, med veljavnostjo potrdila.

(12) 6.5.2 Zaščita zasebnih ključev in nadzor nad zasnovo kriptografskih modulov

— GEN-6.5.2-01 Uporabljajo se vse zahteve iz določbe 6.5.2 ETSI EN 319 411-1 [2], razen zahtev OVR-6.5.2-01, OVR-6.5.2-03 in OVR-6.5.2-04.

— GEN-6.5.2-02 Ustvarjanje para ključev TSP, vključno s ključi, ki jih uporabljajo storitve preklica in registracije, se izvede v okviru varne kriptografske naprave, ki je zaupanja vreden sistem, certificiran v skladu s:

  — skupnimi merili za ocenjevanje varnosti informacijske tehnologije, kot so določena v ISO/IEC 15408 [10] ali v skupnih merilih za ocenjevanje varnosti informacijske tehnologije, različica CC:2002, deli 1 do 5, ki so jih objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih merilih na področju varnosti IT, in po EAL 4 ali višje; ali

  — evropsko certifikacijsko shemo za kibernetsko varnost, ki temelji na skupnih merilih (EUCC) [8][9], in po EAL 4 ali višje; ali

  — do 31. decembra 2030, FIPS PUB 140-3 [11] stopnja 3.

To certificiranje se izvede za varnostni cilj ali profil zaščite ali zasnovo modula in varnostno dokumentacijo, ki izpolnjuje zahteve tega dokumenta, na podlagi analize tveganja in ob upoštevanju fizičnih in drugih netehničnih varnostnih ukrepov.

Če je varna kriptografska naprava certificirana po EUCC [8][9], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— GEN-6.5.2-03 Zasebni ključ CA za podpisovanje se hrani in uporablja v varni kriptografski napravi, ki izpolnjuje zahteve iz GEN-6.5.2-01 in GEN-6.5.2-02.

(13) 6.5.7 Nadzor varnosti omrežja

— OVR-6.5.7-02 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtletje.

— OVR-6.5.7-03 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.

— OVR-6.5.7-04 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje TSP.

(14) 6.6.1 Profil potrdila

— GEN-6.6.1-05 Potrdilo vključuje enega od identifikatorjev politike, opredeljenih v GEN-6.3.3-02 [IZBIRA].

2. Za ETSI EN 319 412-3

(1) 2.1 Normativne reference

— [2] ETSI EN 319 412-2 V2.4.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – 2. del: Profil potrdil za potrdila, izdana fizičnim osebam“.

(2) 4.2.1 Predmet

— LEG-4.2.1-6 Atribut organizationIdentifier mora vsebovati identifikacijo zadevne organizacije, ki se razlikuje od imena organizacije. Če je znano, da obstaja ustrezna registracijska številka, atribut organizationIdentifier vsebuje vrednost te registracijske številke, kot je navedena v ustreznem uradnem zapisu, ki določa to registracijsko številko.

3. Za ETSI EN 319 412-2:

(1) 2.1 Normativne reference

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Profili potrdil – Del 5: Izjave QC“.

— [9] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila ENISA.

(2) 2.2 Informativne reference

— [i.7] neveljavno.

(3) 4.2.2 Podpis

— GEN-4.2.2-2 Algoritem za podpis se izbere v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [9].

— OPOMBA neveljavna.

(4) 4.2.3.1 Izdajatelji pravnih oseb

— GEN-4.2.3.1-3 Če je znano, da obstaja ustrezna registracijska številka, identiteta izdajatelja vsebuje identifikator organizacije z vrednostjo te registracijske številke, kot je navedena v ustreznem uradnem zapisu, ki določa to registracijsko številko.

(5) 4.2.5 Informacije o javnem ključu subjekta

— GEN-4.2.5-2 Javni ključ subjekta se izbere v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [9].

— OPOMBA neveljavna.

(6) 4.2.6 Serijska številka

— GEN-4.2.6-01 Serijska številka potrdila (kot je določena v določbi 4.1.2.2 IETF RFC 5280 [1]) mora biti enotna za vsako potrdilo, ki ga izda TSP.