Uradni list
Evropske unije

SL
Serija L

2025/1946

30.9.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/1946

z dne 29. septembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede kvalificiranih storitev hrambe kvalificiranih elektronskih podpisov in kvalificiranih elektronskih žigov

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 34(2) in člena 40 Uredbe,

ob upoštevanju naslednjega:

(1) Kvalificirane storitve hrambe kvalificiranih elektronskih podpisov in kvalificiranih elektronskih žigov zagotavljajo dolgoročno celovitost, avtentičnost, dokazilo o obstoju in dostopnost dokazil o hrambi navedenih elektronskih podpisov in elektronskih žigov. To omogoča dokazovanje njihove pravne veljavnosti v daljšem časovnem obdobju in zagotavlja, da jih je mogoče potrditi ne glede na prihodnje tehnološke spremembe. Te storitve se zagotavljajo neodvisno ali kot del druge kvalificirane storitve zaupanja, kot so kvalificirane storitve elektronskega arhiviranja.

(2) Domneva o skladnosti iz člena 34(1a) in člena 40 Uredbe (EU) št. 910/2014 bi se morala uporabljati le, kadar kvalificirane storitve hrambe za kvalificirane elektronske podpise in kvalificirane elektronske žige izpolnjujejo standarde 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 kvalificirane storitve zaupanja ter zmožnost preverjanja kvalificiranega statusa in tehnične veljavnosti podpisov in žigov skozi čas.

(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.

([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).

(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.

(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

Referenčni standardi in specifikacije iz člena 34(2) in člena 40 Uredbe (EU) št. 910/2014 so določeni v Prilogi 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

([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).

([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

Seznam referenčnih standardov in specifikacij iz člena 2

Standarda ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511“) in ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4“) se uporabljata z naslednjimi prilagoditvami:

1. Za ETSI TS 119 511

(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 TS 119 612 (V2.3.1) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zanesljivi seznami“.

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

— [6] Izvedbena uredba Komisije (EU) 2024/482 ([1]) 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.

— [7] Izvedbena uredba Komisije (EU) 2024/3144 ([2]) o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.

— [8] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Podpisna politika – 4. del: Pravila o uporabi podpisov (politika potrjevanja) evropskih kvalificiranih elektronskih podpisov/žigov z uporabo zanesljivih seznamov“.

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

(2) 3.1 Pogoji

— varna kriptografska naprava: naprava, ki hrani uporabnikov zasebni ključ, varuje ta ključ pred ogrožanjem in v imenu uporabnika izvaja funkcije podpisovanja ali dešifriranja.

(3) 6.4 Profili za hranjenje

— OVR-6.4-08A [WTS][WOS] Pričakovana hramba dokazov je skladna z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA 3 neveljavna.

(4) 6.5 Politika dokazov o hranjenju

— OVR-6.5-04A Uporabljeni kriptografski algoritmi so skladni z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA 1 neveljavna.

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

(5) 7.2 Človeški viri

— OVR-7.2-02 Osebje PSP v zaupanja vrednih vlogah in, kadar je to ustrezno, podizvajalci v zaupanja vrednih vlogah so sposobni izpolnjevati „strokovno znanje, izkušnje in kvalifikacije“, pridobljene s formalnim usposabljanjem in poverilnicami ali dejanske izkušnje ali kombinacijo obojega.

— OVR-7.2-03 Skladnost z OVR-7.2-02 vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

(6) 7.5 Kriptografski nadzor

— OVR-7.5-05 [POGOJNO] Ko PSP podpiše dokaz o hrambi (ali del njega), se zasebni ključ za podpisovanje PSP hrani in uporablja v varni kriptografski napravi, ki je zaupanja vreden sistem, certificiran v skladu s:

(a) 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:2022, 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

(b) EUCC [6][7] in po EAL 4 ali višje; ali

(c) do 31. decembra 2030, FIPS PUB 140-3 [5] 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 [6][7], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— OVR-7.5-06 [POGOJNO] neveljavno.

— OVR-7.5-07 [POGOJNO] Ko PSP podpiše dokaz o hrambi (ali del njega), se vse varnostne kopije zasebnih ključev za podpisovanje PSP zaščitijo, da se zagotovita njihova celovitost in zaupnost z varno kriptografsko napravo, preden se shranijo zunaj te naprave.

— OVR-7.5-08 Zasebni ključ za podpisovanje PSP se sme izvoziti in uvoziti v drugo varno kriptografsko napravo samo, če sta ta izvoz in uvoz izvedena varno in v skladu s certificiranjem teh naprav.

(7) 7.8 Varnost omrežja

— OVR-7.8-03 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtletje.

— OVR-7.8-04 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.

— OVR-7.8-05 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje PSP.

(8) 7.14 Kriptografski nadzor

— OVR-7.14-03A Ocena kriptografskih algoritmov v OVR-7.14.01 in OVR-7.14.02 je v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA[8].

— OPOMBA neveljavna.

(9) 7.12 Prenehanje in načrti za prenehanje TSP

— OVR-7.12-01A Načrt za prenehanje TSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.2].

(10) 7.17 Dobavna veriga

— OVR-7.17-01 Uporabljajo se naslednje zahteve, določene v določbi 7.14 ETSI EN 319 401 [1]:

(11) Priloga A (normativna): Kvalificirana storitev hrambe QES, kot je opredeljena v členu 34 Uredbe (EU) št. 910/2014

— OVR-A-02 [PDS][PDS+PGD]

(a) storitev hrambe hrani vse informacije, potrebne za preverjanje kvalificiranega statusa elektronskega podpisa ali žiga, ki ne bi bile javno dostopne do konca obdobja hrambe;

(b) storitev hrambe zagotovi, da so shranjene informacije kadar koli v obdobju hrambe take, da kadar so zagotovljene kot vhodne informacije za postopek iz določbe 4.4 ETSI TS 119 172-4 [9], rezultat tega postopka jasno določa, ali je bil digitalni podpis ali žig v času hrambe tehnično primeren za uporabo kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga EU ali ne.

— OVR-A-03 [PDS][PDS+PGD] Časovni žigi, ki se uporabljajo v dokazih o hrambi, so kvalificirani časovni žigi v skladu z Uredbo (EU) št. 910/2014 [i.2].

2. Za ETSI TS 119 172-4

(1) 2.1 Normativne reference:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Postopki za oblikovanje in validacijo digitalnih podpisov (AdES) – 1. del: Oblikovanje in validacija“.

— Vse reference na „ETSI TS 119 102-1 [1]“ se razumejo kot reference na „ETSI EN 319 102-1 [1]“.

— [2] ETSI TS 119 612 (V2.3.1) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zanesljivi seznami“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zahteve politike in varnosti za zahtevke za ustvarjanje in potrjevanje podpisa.“

(2) 4.2 Omejitve in postopki potrjevanja, zahteva REQ-4.2-03, oddelek „X.509 omejitve potrjevanja“, točka (c):

— (i) Če je potrdilo končnega subjekta sidro zaupanja, se RevocationCheckingConstraints ne uporablja.

— (ii) Če potrdilo končnega subjekta ni sidro zaupanja, se RevocationCheckingConstraints nastavijo na „eitherCheck“, kot je opredeljeno v ETSI TS 119 172-1 [3], določba A.4.2.1, preglednica A.2, vrstice (m)2.1.

— (iii) Če je potrdilo končnega subjekta sidro zaupanja, se RevocationFreshnessConstraints, opredeljene v ETSI TS 119 172-1 [3], določba A.4.2.1, preglednica A.2, vrstice (m)2.2, ne uporabljajo.

— (iv) Če potrdilo končnega subjekta ni sidro zaupanja, se za potrdilo o podpisu uporabijo RevocationFreshnessConstraints, opredeljene v ETSI TS 119 172-1 [3], določba A.4.2.1, preglednica A.2, vrstice (m)2.2, z največjo vrednostjo 0 za podpis potrdila, kar zagotavlja, da se informacije o preklicu sprejmejo samo, če so bile izdane po najustreznejšem času za podpis. Vrednost za RevocationFreshnessConstraints se ne določi za potrdila, razen za potrdilo za podpis, vključno s potrdili, ki podpirajo časovne žige.

(3) 4.3 Zahteve glede potrjevanja podpisa in prakse preverjanja pravil o uporabi

— REQ-4.3-02 Zahtevki za potrjevanje podpisa morajo biti skladni z ETSI TS 119 101 [13].

(4) 4.4 Postopek preverjanja tehnične uporabnosti (pravil)

— REQ-4.4.2-03 Če katero koli preverjanje, določeno v REQ-4.4.2-01, ni uspešno, potem:

— se postopek ustavi;

— je podpis tehnično določen kot nedoločen, tj. ne kot kvalificirani elektronski podpis EU ali kvalificirani elektronski žig EU;

— se zgornji rezultat in rezultati vseh vmesnih postopkov upoštevajo v poročilu o preverjanju pravil o uporabi podpisa.