Uradni list
Evropske unije

SL
Serija L

2025/1942

30.9.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/1942

z dne 29. septembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede kvalificiranih storitev potrjevanja kvalificiranih elektronskih podpisov in kvalificiranih storitev potrjevanja 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 33(2) in člena 40 Uredbe,

ob upoštevanju naslednjega:

(1) Kvalificirane storitve potrjevanja kvalificiranih elektronskih podpisov in kvalificiranih elektronskih žigov zagotavljajo celovitost, avtentičnost in pravilnost postopka in rezultatov potrjevanja veljavnosti kvalificiranih elektronskih podpisov oziroma kvalificiranih elektronskih žigov. Te kvalificirane storitve zaupanja imajo ključno vlogo v digitalnem poslovnem okolju, saj spodbujajo prehod s tradicionalnih papirnih postopkov na enakovredne elektronske postopke.

(2) Domneva o skladnosti iz člena 33(2) in člena 40 Uredbe (EU) št. 910/2014 bi se morala uporabljati le, kadar so kvalificirane storitve potrjevanja kvalificiranih elektronskih podpisov oziroma kvalificiranih elektronskih žigov skladne s tehničnimi 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 ter zmožnost preverjanja kvalificiranega statusa in tehnične veljavnosti kvalificiranih elektronskih podpisov oziroma kvalificiranih elektronskih žigov.

(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 33(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 za kvalificirane storitve potrjevanja veljavnosti kvalificiranih elektronskih podpisov in za kvalificirane storitve potrjevanja veljavnosti kvalificiranih elektronskih žigov

Standarda ETSI TS 119 441 V1.2.1 (2023-10) („ETSI TS 119 441“) ([1]) in ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4“) ([2]) se uporabljata z naslednjimi prilagoditvami:

1. Za ETSI TS 119 441:

(1) 2.1 Normativne reference

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

— [3] 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“.

— [4] ISO/IEC 15408-1:2022 – Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Merila za vrednotenje varnosti IT.

— [5] neveljavno.

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

— [7] Izvedbena uredba Komisije (EU) 2024/482 ([3]) 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.

— [8] 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“.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Postopki za oblikovanje in validacijo digitalnih podpisov (AdES) – 2. del: Poročilo o potrjevanju podpisa“.

— [10] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ([4]).

— [11] Izvedbena uredba Komisije (EU) 2024/3144 ([5]) o spremembi Izvedbene uredbe (EU) 2024/4822 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.

— [12] ETSI EN 319 411-1 „Elektronski podpisi in infrastrukture zaupanja (ESI) – Zahteve politike in varnosti za ponudnike storitev zaupanja, ki izdajajo potrdila – 1. del: Splošne zahteve“

([1]) ETSI TS 119 441 – Elektronski podpisi in infrastrukture zaupanja (ESI) – Zahteve politike za ponudnike storitev zaupanja, ki zagotavljajo storitve potrjevanja veljavnosti podpisa, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – 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, V1.1.1 (2021-05).
([3]) UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) UL L 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 2.2 Informativne reference

— [i.11] neveljavno.

(3) 3.3 Kratice

— EUCC evropska certifikacijska shema za kibernetsko varnost, ki temelji na skupnih merilih

(4) 4.3.3 Postopek

— OPOMBA 10: Za navodila glej ETSI EN 319 102-1 [3], za dodatna navodila za primer kvalificiranega podpisa ali žiga EU pa ETSI TS 119 172-4 [8].

(5) 6.1 Izjava o praksi storitve potrjevanja podpisa

— OVR-6.1-02 Izjava o praksi SVS mora biti strukturirana v skladu s Prilogo A.

— OVR-6.1-03 Izjava o praksi SVS mora navajati ali se sklicevati na podprte politike SVS (npr. prek OID) in jih na kratko opisati.

(6) 6.3 Informacijska varnostna politika

— OVR-6.3-02 V varnostni politiki so evidentirani nadzor varnosti in varstva zasebnosti, ki se izvajajo za varstvo osebnih podatkov.

(7) 7.2 Človeški viri

— OVR-7.2-02 Osebje SVSP 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-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.

(8) 7.5 Kriptografski nadzor

— OVR-7.5-02 [POGOJNO] Ko so poročila o potrjevanju podpisana, zaupanja vreden CA v skladu s politiko potrdil NCP+, kot je določena v ETSI EN 319 411-1 [12], izda potrdilo o javnem podpisu SVSP, ki ustreza zasebnemu ključu za podpis SVSP. Izdati bi se moral v skladu z ustrezno politiko potrdil, določeno v ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [POGOJNO] Ko se podpišejo poročila o potrjevanju, se zasebni ključ za podpisovanje SVSP 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 [4] 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 [7][11] in po EAL 4 ali višje; ali

(c) do 31. decembra 2030, FIPS PUB 140-3 [6] 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 [7][11], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— OVR-7.5-04 neveljavno.

— OVR-7.5-06 Zasebni ključ za podpisovanje SVSP 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.

(9) 7.7 Operativna varnost

— OVR-7.7-02 Za zagotovitev, da sistemi, na katerih je bila aplikacija pripravljena, uporabljajo ustrezne varnostne ukrepe in se prilagajajo posebnim okoljem aplikacije, SVA uporablja okolje aplikacije, ki je vzdrževano z najnovejšimi varnostnimi popravki.

— OVR-7.7-03 Za SVA se uporabljajo naslednje zahteve, določene v določbi 5.2 ETSI TS 119 101 [1]: GSM 1.3.

(10) 7.8 Varnost omrežja

— OVR-7.8-02 Če je dovoljen oddaljeni dostop do sistemov, ki shranjujejo ali obdelujejo zaupne podatke, mora biti uradna politika sprejeta in opisana kot del elementov, ki se zahtevajo na podlagi OVR-6.3-02.

— OVR-7.8-04 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtletje.

— OVR-7.8-05 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.

— OVR-7.8-06 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje SVSP.

(11) 7.12 Prenehanje zagotavljanja in načrti za prenehanje zagotavljanja storitev potrjevanja podpisa

— OVR-7.12-02 Načrt za prenehanje TSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.1].

(12) 7.14 Dobavna veriga

— OVR-7.14-01 Uporabljajo se naslednje zahteve, določene v določbi 7.14 ETSI EN 319 401 [2]:

(13) 8.1 Postopek potrjevanja podpisa

— VPR-8.1-07 Zahtevek za potrjevanje (SVA) mora izpolnjevati zahteve iz določbe 7.4 SIA 1 do SIA 4 v ETSI TS 119 101 [1].

— VPR-8.1-11 [POGOJNO] Kadar je namen SVS potrjevanje kvalificiranih elektronskih podpisov oziroma kvalificiranih elektronskih žigov v skladu s členom 32(1) (oziroma členom 40) Uredbe (EU) št. 910/2014 [i.1], postopek potrjevanja upošteva zahteve ETSI TS 119 172-4 [8].

(14) 8.2 Protokol za potrjevanje podpisa

— SVP-8.2-03 Odgovor na potrditev podpisa mora vsebovati OID politike SVS.

(15) 8.4 Poročilo o potrjevanju podpisa

— SVR-8.4-02 Poročilo o potrjevanju mora biti v skladu z ETSI TS 119 102-2 [9].

— SVR-8.4-07 [POGOJNO] Če SVS politike potrjevanja podpisa ne obdela v celoti, se v poročilu poleg poročanja o potrjenih omejitvah poroča tudi o omejitvah, ki so bile prezrte ali razveljavljene.

— SVR-8.4-15 V poročilu o potrditvi mora biti jasno naveden izvor vsakega dokaza o obstoju (na podlagi podpisa, od odjemalca, s strežnika).

— SVR-8.4-16 Poročilo o potrditvi mora biti opremljeno s podpisom poročila o potrditvi, ki je digitalni podpis SVSP.

— SVR-8.4-17 [POGOJNO] Ob podpisu poročil o potrditvi morata biti oblika in cilj podpisa v skladu z ETSI TS 119 102-2 [9].

(16) 9 Okvir za opredelitev politik storitev potrjevanja, ki temelji na politiki storitev zaupanja, opredeljeni v tem dokumentu:

— OVR-9-05 [POGOJNO] Pri oblikovanju politike SVS na podlagi politike skrbniških storitev, opredeljene v tem dokumentu, se izvede ocena tveganja, da se ocenijo poslovne zahteve in določijo varnostne zahteve, ki jih je treba vključiti v politiko za navedeno skupnost in uporabnost.

— OVR-9-06 [POGOJNO] Pri oblikovanju politike SVS na podlagi politike skrbniških storitev, opredeljene v tem dokumentu, se politika odobri in spremeni v skladu z opredeljenim postopkom pregleda, vključno z odgovornostmi za vzdrževanje politike.

— OVR-9-07 [POGOJNO] Pri oblikovanju politike SVS na podlagi politike storitev zaupanja, opredeljene v tem dokumentu, mora obstajati opredeljen postopek pregleda, da se zagotovi, da je politika podprta z izjavami o praksah.

— OVR-9-08 [POGOJNO] Pri oblikovanju politike SVS na podlagi politike storitev zaupanja, opredeljene v tem dokumentu, mora TSP svoji skupnosti uporabnikov dati na voljo politike, ki jih podpira.

— OVR-9-09 [POGOJNO] Pri oblikovanju politike SVS na podlagi politike skrbniških storitev, opredeljene v tem dokumentu, morajo biti naročnikom na voljo revizije politik, ki jih podpira TSP.

(17) Priloga B (normativna) Kvalificirana storitev potrjevanja za QES, kot je opredeljena v členu 33 Uredbe (EU) št. 910/2014:

— VPR-B-02 [POGOJNO] Če je SVSP QSVSP, mora izvajanje potekati v skladu z ETSI TS 119 172-4 [8].

— OPOMBA 2 neveljavna.

— OVR-B-04 [POGOJNO] Če je SVSP QSVSP, se s testiranjem na podlagi OVR-B-03 preverijo različni pozitivni in negativni primeri uporabe.

— VPR-B-11 [POGOJNO] Če je SVSP QSVSP, nadzoruje izračun zgoščene vrednosti (bodisi izvede izračun na strežniški strani bodisi nadzoruje odjemalca, če je to dovoljeno na strani odjemalca).

— OPOMBA 5 neveljavna.

— OPOMBA 6 neveljavna.

— VPR-B-15 [POGOJNO] Če je SVSP QSVSP, je za izpolnitev zahtev VPR-B-13 do VPR-B-14 poročilo o potrditvi skladno z ETSI TS 119 102-2 [9].

— VPR-B-16 [POGOJNO] Če je SVSP QSVSP, mora biti izvajanje v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [10] za uporabo ustreznih kriptografskih tehnik pri zagotavljanju kvalificiranih storitev potrjevanja kvalificiranih elektronskih podpisov oziroma kvalificiranih elektronskih žigov.

(18) Priloga C (informativno) Primerjava zahtev z Uredbo (EU) št. 910/2014, oddelek „Potrjevanje veljavnosti v skladu s členom 32(1)“, drugi odstavek:

— Za zagotovitev preverjanja vseh pogojev, ki jih zahtevata člena 32(1) in 40 Uredbe (EU) št. 910/2014 [i.1, je potreben pravilen algoritem za potrjevanje. Zagotavlja enak deterministični rezultat za podpis ali žig, predložen v potrditev. V ta namen je ključnega pomena politika potrjevanja podpisa. ETSI TS 119 172-4 [8], ki temelji na algoritmu za potrjevanje iz ETSI EN 319 102-1 [3], je bil izdan s tega vidika.

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 (2024-11) „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 24 ur. Vrednost za RevocationFreshnessConstraints se ne določi za potrdila, razen za potrdilo za podpis, vključno s potrdili, ki podpirajo časovne žige.

(3) 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:

(a) se postopek ustavi;

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

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