



2025/1944

30.9.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/1944

z dne 29. septembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede referenčnih standardov za postopke pošiljanja in prejemanja podatkov v okviru kvalificiranih storitev elektronske priporočene dostave ter glede interoperabilnosti teh storitev

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 44(2) in člena 44(2b) Uredbe,

ob upoštevanju naslednjega:

- (1) Kvalificirane storitve elektronske priporočene dostave zagotavljajo varen kanal za prenos dokumentov, vključno z dokazilom o oddaji in prejemu podatkov. Njihov namen je zagotoviti gotovost pri identifikaciji naslovnika in visoko raven zaupanja v identifikacijo pošiljatelja.
- (2) Domneva o skladnosti iz člena 44(1a) Uredbe (EU) št. 910/2014 bi se morala uporabljati samo, kadar so kvalificirane storitve zaupanja za zagotavljanje kvalificiranih storitev elektronske priporočene dostave 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 kvalificirane storitve zaupanja.
- (3) Če ponudnik storitev zaupanja izpolnjuje zahteve iz Priloge I 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) V skladu s členom 44(2a) Uredbe (EU) št. 910/2014 je pomembno, da ponudniki kvalificiranih storitev zaupanja, kadar se dogovorijo, da bodo njihove storitve interoperabilne, upoštevajo ustrezne standarde in specifikacije iz Priloge II k tej izvedbeni uredbi, da se omogoči enostaven prenos elektronsko registriranih podatkov med dvema ali več ponudniki kvalificiranih storitev zaupanja in spodbujajo poštene prakse na notranjem trgu.
- (5) 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 posodabljaliti 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>).

- (6) 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 vse dejavnosti obdelave osebnih podatkov na podlagi te uredbe.
- (7) 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.
- (8) 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 kvalificirane storitve elektronske priporočene dostave

Referenčni standardi in specifikacije iz člena 44(2) Uredbe (EU) št. 910/2014 so določeni v Prilogi I k tej uredbi.

Člen 2

Referenčni standardi in specifikacije za interoperabilnost med kvalificiranimi storitvami elektronske priporočene dostave

Referenčni standardi in specifikacije iz člena 44(2b) Uredbe (EU) št. 910/2014 so določeni v Prilogi II k tej uredbi.

Člen 3

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 I

Seznam referenčnih standardov in specifikacij iz člena 1

Standard ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521“) se uporablja z naslednjimi prilagoditvami:

1. Za ETSI EN 319 521

(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 potrdila – 1. del: Splošne zahteve“.
- [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Storitve elektronske priporočene dostave – 1. del: Ogrodje in arhitektura“.
- [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Storitve elektronske priporočene dostave – 2. del: Semantične vsebine“.
- [5] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ⁽¹⁾.
- [6] ISO/IEC 15408-1:2022 – Informacijska varnost, kibernetska varnost in varstvo zasebnosti – Merila za vrednotenje varnosti IT.
- [7] Izvedbena uredba Komisije (EU) 2024/482 ⁽²⁾ 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 ⁽³⁾.
- [8] Izvedbena uredba Komisije (EU) 2024/3144 o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.
- [9] FIPS PUB 140-3 (2019) „Varnostne zahteve za kriptografske module“.

(2) 3.1 Pogoji

- napredni elektronski žig: kot je opredeljeno v Uredbi (EU) št. 910/2014 [i.1].
- napredni elektronski podpis: kot je opredeljeno v Uredbi (EU) št. 910/2014 [i.1].
- kvalificirani elektronski žig: kot je opredeljeno v Uredbi (EU) št. 910/2014 [i.1].
- kvalificirani elektronski podpis: kot je opredeljeno v Uredbi (EU) št. 910/2014 [i.1].
- varna kriptografska naprava: naprava, ki hrani uporabnikov zasebni ključ, varuje ta ključ pred ogrožanjem in v imenu uporabnika izvaja funkcije podpisovanja ali dešifriranja.

⁽¹⁾ https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

⁽²⁾ UL L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

⁽³⁾ UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

(3) 5.1.1 Skupne določbe

- REQ-ERDS-5.1.1-01 Storitve elektronske priporočene dostave zagotovi, da so razpoložljivost, celovitost in zaupnost uporabniške vsebine ustrezno zagotovljene, medtem ko jo obravnava storitev elektronske priporočene dostave, pri čemer izbere ustrezne kriptografske tehnike za zagotavljanje celovitosti in zaupnosti v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [5].

(4) 5.2.1.1 Splošno

- REQ-QERDS-5.2.1.1-01 Ponudnik kvalificiranih storitev elektronske priporočene dostave z zelo visoko stopnjo zaupanja preveri identiteto prejemnika bodisi neposredno bodisi z zanašanjem na tretjo osebo in z uporabo enega od naslednjih sredstev ali njihove kombinacije, kot je potrebno:
 - (a) s fizično prisotnostjo fizične osebe ali pooblaščenega predstavnika pravne osebe z ustreznimi dokazi in postopki v skladu z nacionalnim pravom;
 - (b) na daljavo z uporabo sredstev elektronske identifikacije, ki izpolnjujejo zahteve iz člena 8 Uredbe (EU) št. 910/2014 [i.1] glede ravni zanesljivosti „visoka“, ali z evropsko denarnico za digitalno identiteto;
 - (c) s potrdilom kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga;
 - (d) z uporabo drugih načinov identifikacije, ki zagotavljajo identifikacijo fizične osebe ali pooblaščenega zastopnika pravne osebe z zelo visoko stopnjo zaupanja. Zagotovilo, da se ta identifikacija izvaja z zelo visoko stopnjo zaupanja, potrdi organ za ugotavljanje skladnosti.
- REQ-QERDS-5.2.1.1-01A Ponudnik kvalificiranih storitev elektronske priporočene dostave preveri identiteto pošiljatelja z ustreznimi sredstvi, bodisi neposredno ali prek tretje osebe, na podlagi enega od naslednjih načinov ali njihove kombinacije:
 - (a) s fizično prisotnostjo fizične osebe ali pooblaščenega predstavnika pravne osebe z ustreznimi dokazi in postopki v skladu z nacionalnim pravom;
 - (b) na daljavo z evropsko denarnico za digitalno identiteto ali priglašnim sredstvom elektronske identifikacije, ki izpolnjuje zahteve iz člena 8 Uredbe (EU) št. 910/2014 [i.1] v zvezi z „znatno“ ravno zanesljivosti, če je bila izdana na podlagi predhodne fizične navzočnosti fizične osebe ali pooblaščenega zastopnika pravne osebe;
 - (c) s potrdilom o naprednem elektronskem podpisu ali naprednem elektronskem žigu, če je bilo potrdilo izdano fizični osebi ali pooblaščenemu zastopniku pravne osebe v skladu z običajno politiko glede potrdil (*Normalised Certificate Policy – NCP*), kot je opredeljena v ETSI EN 319 411-1 [2]; ali
 - (d) z uporabo drugih načinov identifikacije, ki zagotavljajo identifikacijo fizične osebe ali pooblaščenega zastopnika pravne osebe z zelo visoko stopnjo zaupanja. Zagotovilo, da se ta identifikacija izvaja z visoko stopnjo zaupanja, potrdi organ za ugotavljanje skladnosti.
- OPOMBA Tretja oseba, ki preverja identiteto pošiljatelja in prejemnika, je lahko drug ponudnik kvalificiranih storitev elektronske priporočene dostave, če sta pošiljatelj in prejemnik naročena na različne ponudnike kvalificiranih storitev elektronske priporočene dostave.

(5) 5.2.1.2 Identifikacija prejemnika in predaja vsebin uporabnikov

- REQ-QERDS-5.2.1.2-03 Če identifikacija prejemnika temelji na notranjem postopku kvalificiranih storitev elektronske priporočene dostave, mora ponudnik kvalificiranih storitev elektronske priporočene dostave celoten postopek izvesti v zavarovanem in nadzorovanem okolju.

(6) 5.2.2 Določbe za avtentikacijo kvalificiranih storitev elektronske priporočene dostave EU

- REQ-QERDS-5.2.2-03 [CONDITIONAL] Kadar ponudnik kvalificiranih storitev elektronske priporočene dostave povezuje sredstva avtentikacije z identiteto pošiljatelja, preverjeno v skladu z določbo 5.2.1, mora uporabiti eno od naslednjega:

- (a) mehanizmi za dvofaktorsko avtentikacijo;
 - (b) evropska denarnica za digitalno identiteto ali priglašeno sredstvo elektronske identifikacije, ki izpolnjuje zahteve iz člena 8 Uredbe (EU) št. 910/2014 [i.1] glede „visoke“ ali „znatne“ ravni zanesljivosti;
 - (c) vzajemna avtentikacija varnosti transportne plasti (TLS), ki vključuje potrdilo, izdano pošiljatelju v skladu z NCP, kot je opredeljena v ETSI EN 319 411-1 [2];
 - (d) digitalni podpis, podprt s potrdilom, izdanim v skladu z NCP, kot je opredeljena v ETSI EN 319 411-1 [2];
 - (e) druga sredstva, ki zagotavljajo avtentikacijo pošiljatelja, katerega identiteta je ugotovljena. Skladnost obvezujoče zaveze potrdi organ za ugotavljanje skladnosti. Primer: To lahko vključuje uporabo enega od zgoraj navedenih sredstev iz točk (a), (b) in (d) za registracijo potrdila odjemalca za varnost transportne plasti (TLS) za avtomatizirano pošiljanje prek vzajemnega TLS ali za registracijo digitalnega potrdila o žigu, ki se uporablja za žigosanje izjav za avtentikacijo s storitvijo elektronske priporočene dostave. Uporabijo se lahko tudi drugi mehanizmi, pri katerih identificirani pošiljatelji uporabljajo prenesene storitve tretjih oseb.
- REQ-QERDS-5.2.2-03A [POGOJNO] Kadar ponudnik kvalificiranih storitev elektronske priporočene dostave povezuje sredstva za avtentikacijo z identiteto prejemnika, preverjeno v skladu z določbo 5.2.1, mora biti to eno od naslednjega, če sredstva ali katera koli kombinacija sredstev zagotavljajo zelo visoko raven zaupanja v identiteto overjenega prejemnika:
 - (a) večfaktorska avtentikacija
 - (b) evropska denarnica za digitalno identiteto ali priglašeno sredstvo elektronske identifikacije, ki izpolnjuje zahteve iz člena 8 Uredbe (EU) št. 910/2014 [i.1] glede „visoke“ ali „znatne“ ravni zanesljivosti;
 - (c) potrdilo kvalificiranega elektronskega podpisa ali kvalificiranega elektronskega žiga;
 - (d) druga sredstva, ki zagotavljajo avtentikacijo prejemnika, katerega identiteta je ugotovljena. Skladnost obvezujoče zaveze potrdi organ za ugotavljanje skladnosti. Primer: To lahko vključuje uporabo enega od zgoraj navedenih sredstev iz točk (a) do (c) za registracijo potrdila odjemalca za varnost transportne plasti (TLS) za avtomatizirano pošiljanje prek vzajemnega TLS ali za registracijo digitalnega potrdila o žigu, ki se uporablja za žigosanje izjav za avtentikacijo s storitvijo elektronske priporočene dostave. Uporabijo se lahko tudi drugi mehanizmi, pri katerih identificirani pošiljatelji uporabljajo prenesene storitve tretjih oseb.

- REQ-QERDS-5.2.2-04 [POGOJNO] Če se pošiljatelj poveže s QERDS prek varne povezave, ki zahteva medsebojno avtentikacijo stroj-stroj med pošiljateljevim računalnikom in strežnikom QERDS na podlagi potrdil, izdanih v skladu z NCP, kot je opredeljena v ETSI EN 319 411-1 [2], se lahko po vzpostavitvi te varne povezave sprejme mehanizem za enofaktorsko avtentikacijo za drugo fazo avtentikacije pošiljatelja, če vzpostavljeni organizacijski postopki in varnostni ukrepi zagotavljajo zaupanje v avtentikacijo pošiljatelja.

(7) 5.4.1 Skupne določbe

- REQ-ERDS-5.4.1-06 S storitvami elektronske priporočene dostave je treba ustvariti in dati na voljo upravičenim zainteresiranim stranem dokaze storitev elektronske priporočene dostave o dogodkih elektronske priporočene dostave, kot so opredeljeni v določbi 6 standarda ETSI EN 319 522-1 [3].
- REQ-ERDS-5.4.1-07 Ponudnik storitev elektronske priporočene dostave mora arhivirati dokaze in/ali povzetke dokazov za vsak dokaz, ki ga je izdal.
- REQ-ERDS-5.4.1-08 Dokazi storitev elektronske priporočene dostave, ki so bili ustvarjeni s storitvami elektronske priporočene dostave, morajo biti skladni s semantiko dokazov, opredeljeno v klavzuli 8 ETSI EN 319 522-2 [4].

(8) 7.2.1 Skupne določbe

- REQ-ERDS-7.2.1-02 Osebe ponudnika storitev elektronske priporočene dostave 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.
- REQ-ERDS-7.2.1-03 Skladnost z REQ-ERDS-7.2.1-02 vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

(9) 7.3.2 Ravnanje z nosilci

- REQ-ERDS-7.3.1-02 Uporabljajo se vse zahteve iz določbe 7.3.3 ETSI EN 319 401 [1].

(10) 7.5 Kriptografski nadzor

- REQ-ERDS-7.5-01 Storitve elektronske priporočene dostave izberejo in uporabljajo ustrezne kriptografske tehnike, skladne z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [5].
- REQ-ERDSP-7.5-03 Zasebni ključ za podpisovanje storitve elektronske priporočene dostave se shranjuje 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 [6] 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 meril na področju varnosti IT, in po EAL 4 ali višje; ali
 - (b) evropsko certifikacijsko shemo za kibernetsko varnost, ki temelji na skupnih merilih (EUC) [7][8], in po EAL 4 ali višje; ali
 - (c) do 31. decembra 2030, FIPS PUB 140-3 [9] stopnja 3.

To certificiranje se izvede za varnostni cilj ali profil zaščite ali zasnovano 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 EUC [7][8], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

(11) 7.8 Varnost omrežja

- REQ-ERDSP-7.8-04 Ponudnik storitev elektronske priporočene dostave uporablja najsodobnejše protokole in algoritme za šifriranje na ravni transportne plasti v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [5].

- REQ-ERDSP-7.8-06 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtoletje.
 - REQ-ERDSP-7.8-07 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.
 - REQ-ERDSP-7.8-08 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje TSP.
- (12) 7.12 Prenehanje in načrti za prenehanje ERDSP
- REQ-ERDS-7.12-03 Načrt za prenehanje ERDSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.1].
- (13) 7.14 Dobavna veriga
- REQ-ERDS-7.14-01 Uporabljajo se naslednje zahteve, določene v določbi 7.14 ETSI EN 319 401 [1].
-

*PRILOGA II***Seznam referenčnih standardov in specifikacij iz člena 2**

Uporabljajo se standardi ETSI EN 319 522-1 V1.2.1 (2024-01) („ETSI EN 319 522-1“), ETSI EN 319 522-2 V1.2.1 (2024-01) („ETSI EN 319 522-2“), ETSI EN 319 522-3 V1.2.1 (2024-01) („ETSI EN 319 522-3“), ETSI EN 319 522-4-1 V1.2.1 (2019-01) („ETSI EN 319 522-4-1“), ETSI EN 319 522-4-2 V1.1.1 (2018-09) („ETSI EN 319 522-4-2“) in ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3“).
