2025/1944

30.9.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1944

od 29. rujna 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu referentnih normi za postupke slanja i primanja podataka u kvalificiranim uslugama elektroničke preporučene dostave te u pogledu interoperabilnosti tih usluga

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 44. stavak 2. i članak 44. stavak 2.b,

budući da:

(1) Kvalificirane usluge elektroničke preporučene dostave pružaju siguran kanal za prijenos dokumenata, uključujući dokaze slanja i primanja podataka. Svrha im je pružiti sigurnost u identificiranje adresata i osigurati visoku razinu povjerenja u identifikaciju pošiljatelja.

(2) Pretpostavka sukladnosti utvrđena u članku 44. stavku 1.a Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge povjerenja za pružanje kvalificiranih usluga elektroničke preporučene dostave 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 kvalificirane usluge povjerenja.

(3) Ako pružatelj usluga povjerenja ispunjava zahtjeve utvrđene u Prilogu I. 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) Prema članku 44. stavku 2.a Uredbe (EU) br. 910/2014, ako se kvalificirani pružatelji usluga povjerenja dogovore da njihove usluge budu interoperabilne, važno je da se pridržavaju odgovarajućih normi i specifikacija utvrđenih u Prilogu II. ovoj Provedbenoj uredbi kako bi lako prenosili elektroničke preporučene podatke između dva ili više kvalificiranih pružatelja usluga povjerenja i podržali poštene prakse na unutarnjem tržištu.

(5) 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.

([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).

(6) Na sve 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]).

(7) 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.

(8) 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 usluge elektroničke preporučene dostave

Referentne norme i specifikacije iz članka 44. stavka 2. Uredbe (EU) br. 910/2014 utvrđene su u Prilogu I. ovoj Uredbi.

Članak 2.

Referentne norme i specifikacije za interoperabilnost kvalificiranih usluga elektroničke preporučene dostave

Referentne norme i specifikacije iz članka 44. stavka 2.b Uredbe (EU) br. 910/2014 utvrđene su u Prilogu II. ovoj Uredbi.

Članak 3.

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

([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).

([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 iz članka 1.

Primjenjuje se norma ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521”) uz sljedeće prilagodbe:

1. Za ETSI EN 319 521

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”.

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) – „Elektronički potpisi i infrastrukture (ESI) – Usluge isporuke elektronički registriranih poruka – 1. dio: Okvir i arhitektura”.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) – „Elektronički potpisi i infrastrukture (ESI) – Usluge isporuke elektronički registriranih poruka – 2. dio: Semantički sadržaji”.

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

— [6] ISO/IEC 15408-1:2022 – Sigurnost informacija, kibernetička sigurnost i zaštita privatnosti – Kriteriji za evaluaciju informatičke sigurnosti.

— [7] Provedbena uredba Komisije (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) ([2]).

— [8] 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.

— [9] FIPS PUB 140-3 (2019.) „Sigurnosni zahtjevi za kriptografske module”.

2. 3.1. Pojmovi

— napredan elektronički pečat: kako je definiran u Uredbi (EU) br. 910/2014 [i.1].

— napredan elektronički potpis: kako je definiran u Uredbi (EU) br. 910/2014 [i.1].

— kvalificirani elektronički pečat: kako je definiran u Uredbi (EU) br. 910/2014 [i.1].

— kvalificirani elektronički potpis: kako je definiran u Uredbi (EU) br. 910/2014 [i.1].

— sigurni kriptografski uređaj: uređaj koji čuva privatni ključ korisnika, štiti taj ključ od ugrožavanja i obavlja funkcije potpisivanja ili dešifriranja u ime korisnika.

([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.

3. 5.1.1. Zajedničke odredbe

— REQ-ERDS-5.1.1-01 ERDS osigurava da su dostupnost, cjelovitost i povjerljivost korisničkog sadržaja primjereno zajamčene dok ga ERDS obrađuje tako da odabere odgovarajuće kriptografske tehnike za održavanje cjelovitosti i povjerljivosti koje su sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [5].

4. 5.2.1.1. Općenito

— REQ-QERDS-5.2.1.1-01 QERDSP je obvezan s vrlo visokom pouzdanošću provjeriti identitet primatelja bilo izravno bilo preko treće strane jednim od sljedećih načina ili, prema potrebi, njihovom kombinacijom:

(a) na temelju fizičke prisutnosti fizičke osobe ili ovlaštenog predstavnika pravne osobe, odgovarajućim dokazima i postupcima, u skladu s nacionalnim pravom;

(b) na daljinu, pomoću sredstava elektroničke identifikacije koja ispunjavaju zahtjeve iz članka 8. Uredbe (EU) br. 910/2014 [i.1] u pogledu visoke razine osiguranja identiteta ili pomoću europske lisnice za digitalni identitet;

(c) pomoću certifikata kvalificiranog elektroničkog potpisa ili kvalificiranog elektroničkog pečata;

(d) primjenom drugih metoda identifikacije kojima se osigurava da se fizička osoba ili ovlašteni zastupnik pravne osobe može identificirati s vrlo visokom razinom pouzdanosti. Tijelo za ocjenjivanje sukladnosti potvrđuje jamstvo da se ta identifikacija provodi s vrlo visokom razinom pouzdanosti.

— REQ-QERDS-5.2.1.1-01A QERDSP provjerava identitet pošiljatelja odgovarajućim sredstvima, bilo izravno bilo preko treće strane, jednom od sljedećih metoda ili njihovom kombinacijom:

(a) na temelju fizičke prisutnosti fizičke osobe ili ovlaštenog predstavnika pravne osobe, odgovarajućim dokazima i postupcima, u skladu s nacionalnim pravom;

(b) na daljinu, pomoću europske lisnice za digitalni identitet ili prijavljenog sredstva elektroničke identifikacije koje ispunjava zahtjeve iz članka 8. Uredbe (EU) br. 910/2014 [i.1] u pogledu značajne razine sigurnosti, pod uvjetom da su izdani na temelju prethodne fizičke prisutnosti fizičke osobe ili ovlaštenog predstavnika pravne osobe;

(c) pomoću certifikata naprednog elektroničkog potpisa ili naprednog elektroničkog pečata, pod uvjetom da je taj certifikat izdan fizičkoj osobi ili ovlaštenom predstavniku pravne osobe na temelju politike normaliziranih certifikata (NCP) kako je definirana u normi ETSI EN 319 411-1 [2]; ili

(d) primjenom drugih metoda identifikacije kojima se osigurava da se fizička osoba ili ovlašteni zastupnik pravne osobe može identificirati s vrlo visokom razinom pouzdanosti. Tijelo za ocjenjivanje sukladnosti potvrđuje jamstvo da se ta identifikacija provodi s vrlo visokom razinom pouzdanosti.

— NAPOMENA: Treća strana koja provjerava identitet pošiljatelja i primatelja može biti drugi QERDSP ako su pošiljatelj i primatelj ugovaratelji usluga različitih QERDSP-ova.

5. 5.2.1.2. Identifikacija primatelja i predaja korisničkog sadržaja

— REQ-QERDS-5.2.1.2-03 Ako se identifikacija primatelja temelji na internom postupku QERDS-a, QERDSP provodi cijeli postupak u sigurnom i kontroliranom okruženju.

6. 5.2.2. Odredbe za autentifikaciju EU QERDS-a

— REQ-QERDS-5.2.2-03 [UVJETNO] Kad QERDSP povezuje sredstvo autentifikacije s identitetom pošiljatelja provjerenim u skladu s točkom 5.2.1., ono mora biti jedno od sljedećeg:

(a) mehanizam dvofaktorske autentifikacije;

(b) europska lisnica za digitalni identitet ili prijavljeno sredstvo elektroničke identifikacije koje ispunjava zahtjeve iz članka 8. Uredbe (EU) br. 910/2014 [i.1] u pogledu visoke ili značajne razine osiguranja identiteta;

(c) uzajamna TLS autentifikacija, koja uključuje certifikat izdan pošiljatelju na temelju NCP-a kako je definiran u normi ETSI EN 319 411-1 [2];

(d) digitalni potpis poduprt certifikatom izdanim na temelju NCP-a kako je definiran u normi ETSI EN 319 411-1 [2];

(e) drugo sredstvo kojim se postiže autentifikacija identificiranog pošiljatelja. Sukladnost veze potvrđuje tijelo za ocjenjivanje sukladnosti. Primjer: To može uključivati korištenje jednog od sredstava iz točaka (a), (b) i (d) za registraciju TLS certifikata klijenta za automatsko slanje putem uzajamnog TLS-a ili za registraciju certifikata digitalnog pečata kojim se ovjeravaju izjave za autentifikaciju kod ERDS-a. Mogu se primjenjivati i drugi mehanizmi u kojima identificirani pošiljatelji koriste delegirane usluge trećih strana.

— REQ-QERDS-5.2.2-03A [UVJETNO] Ako QERDSP povezuje sredstvo autentifikacije s identitetom primatelja provjerenim u skladu s klauzulom 5.2.1., ono mora biti jedno od sljedećeg, pod uvjetom da to sredstvo ili bilo koja kombinacija tih sredstava daju vrlo visoku razinu povjerenja u identitet autentificiranog primatelja:

(a) mehanizam višefaktorske autentifikacije;

(b) europska lisnica za digitalni identitet ili prijavljeno sredstvo elektroničke identifikacije koje ispunjava zahtjeve iz članka 8. Uredbe (EU) br. 910/2014 [i.1] u pogledu visoke ili značajne razine osiguranja identiteta;

(c) certifikat kvalificiranog elektroničkog potpisa ili kvalificiranog elektroničkog pečata;

(d) drugo sredstvo kojima se postiže autentifikacija identificiranog primatelja. Sukladnost veze potvrđuje tijelo za ocjenjivanje sukladnosti. Primjer: To može uključivati korištenje jednog od sredstava iz točaka od (a) do (c) za registraciju TLS certifikata klijenta za automatsko slanje putem uzajamnog TLS-a ili za registraciju certifikata digitalnog pečata kojim se ovjeravaju izjave za autentifikaciju kod ERDS-a. Mogu se primjenjivati i drugi mehanizmi u kojima identificirani pošiljatelji koriste delegirane usluge trećih strana.

— REQ-QERDS-5.2.2-04 [UVJETNO] Ako se pošiljatelj spoji na QERDS sigurnom vezom za koju je potrebna uzajamna autentifikacija stroj-stroj između pošiljateljeva stroja i poslužitelja QERDS-a na temelju certifikata izdanih prema NCP-u kako je definiran u normi ETSI EN 319 411-1 [2], onda se, nakon što se uspostavi ta sigurna veza, za drugu fazu autentifikacije pošiljatelja mogu primijeniti mehanizmi jednostruke autentifikacije, pod uvjetom da uspostavljeni organizacijski postupci i sigurnosne mjere jamče pouzdanost autentifikacije pošiljatelja.

7. 5.4.1. Zajedničke odredbe

— REQ-ERDS-5.4.1-06 ERDS generira i stavlja na raspolaganje legitimnim zainteresiranim stranama ERDS dokaze o ERD događajima kako su definirani u točki 6. norme ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 ERDSP arhivira dokaze i/ili sažetke dokaza za svaki dokaz koji je izdao.

— REQ-ERDS-5.4.1-08 ERDS dokazi koje generira ERDS moraju biti u skladu sa semantikom dokaza definiranom u točki 8. norme ETSI EN 319 522-2 [4].

8. 7.2.1. Zajedničke odredbe

— REQ-ERDS-7.2.1-02 Osoblje ERDSP-a na pouzdanim funkcijama mora 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.

— REQ-ERDS-7.2.1-03 Sukladnost s REQ-ERDS-7.2.1-02 uključuje redovita informiranja (barem svakih 12 mjeseci) o novim prijetnjama i aktualnim sigurnosnim praksama.

9. 7.3.2. Postupanje s medijima

— REQ-ERDS-7.3.1-02 Primjenjuju se svi zahtjevi iz točke 7.3.3. norme ETSI EN 319 401 [1].

10. 7.5. Kriptografske mjere

— REQ-ERDS-7.5-01A ERDS odabire i primjenjuje odgovarajuće kriptografske tehnike sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [5].

— REQ-ERDSP-7.5-03 Potpisni privatni ključ ERDS-a čuva se i upotrebljava unutar sigurnog kriptografskog uređaja koji je pouzdan sustav certificiran u skladu:

(a) sa zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normi ISO/IEC 15408 [6] 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

(b) s europskim programom kibernetičkosigurnosne certifikacije temeljenom na zajedničkim kriterijima (EUCC) [7][8] i certificiran na razini EAL 4 ili višoj; ili

(c) do 31.12.2030. normom FIPS PUB 140-3 [9] 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 [7][8] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

11. 7.8. Mrežna sigurnost

— REQ-ERDSP-7.8-04 ERDSP upotrebljava najsuvremenije protokole i algoritme za šifriranje na razini transportnog sloja sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [5].

— REQ-ERDSP-7.8-06 Potraga za ranjivim točkama koja je obvezna prema REQ-7.8-13 norme ETSI EN 319 401 [1] obavlja se najmanje svaka tri mjeseca.

— REQ-ERDSP-7.8-07 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319 401 [1] obavlja se najmanje jedanput u godini.

— REQ-ERDSP-7.8-08 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad TSP-a.

12. 7.12. Prekid rada ERDSP-a i planovi prekida ERDS-a

— REQ-ERDS-7.12-03 ERDSP-ov plan prekida mora ispunjavati zahtjeve utvrđene u provedbenim aktima donesenima na temelju članka 24. stavka 5. Uredbe (EU) br. 910/2014 [i.1].

13. 7.14. Lanac opskrbe

— REQ-ERDS-7.14-01 Primjenjuju se zahtjevi iz točke 7.14. norme ETSI EN 319 401 [1].

PRILOG II.

Popis referentnih normi i specifikacija iz članka 2.

Primjenjuju se norme 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”) i ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3”).