2025/2531

17.12.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/2531

od 16. prosinca 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu referentnih normi i specifikacija za kvalificirane elektroničke evidencije

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 45.l stavak 3.,

budući da:

(1) Uredbom (EU) 2024/1183 Europskog parlamenta i Vijeća ([2]) u Uredbu (EU) br. 910/2014 uvršten je popis novih usluga povjerenja i kvalificiranih usluga povjerenja, uključujući bilježenje elektroničkih podataka u kvalificiranu elektroničku evidenciju. Komisija treba sastaviti popis referentnih normi i, prema potrebi, utvrditi specifikacije za takve usluge.

(2) Elektronička evidencija je slijed elektroničkih zapisa podataka kojim se osigurava cjelovitost tih zapisa podataka i točnost njihova kronološkog reda. Da bi se podaci u kvalificiranu elektroničku evidenciju bilježili kronološkim redom, dosljedno i pouzdano, potrebno je utvrditi zajednički skup specifikacija za bilježenje elektroničkih podataka u kvalificiranu elektroničku evidenciju.

(3) Pretpostavka sukladnosti utvrđena u članku 45.l stavku 2. Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge povjerenja za bilježenje elektroničkih podataka u kvalificiranu elektroničku evidenciju 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.

(4) Ako pružatelj usluga povjerenja ispunjava zahtjeve utvrđene u Prilogu 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.

(5) Komisija redovito ocjenjuje nove tehnologije, prakse, norme i tehničke specifikacije. U skladu s uvodnom izjavom 75. Uredbe (EU) 2024/1183 Komisija bi ovu Uredbu trebala preispitivati i prema potrebi ažurirati kako bi bila u skladu s globalnim kretanjima, novim tehnologijama, praksama, 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 aktivnosti obrade osobnih podataka na temelju ove Uredbe primjenjuju se Uredba (EU) 2016/679 ([3]) Europskog parlamenta i Vijeća i, ako je relevantno, Direktiva 2002/58/EZ Europskog parlamenta i Vijeća ([4]), pri čemu se u obzir uzimaju i Smjernice 02/2025 za obradu osobnih podataka pomoću tehnologije ulančanih blokova ([5]) Europskog odbora za zaštitu podataka.

(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 ([6]) te je on dao mišljenje 21. listopada 2025. ([7])

(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

Referentne norme i specifikacije iz članka 45.l stavka 3. Uredbe (EU) br. 910/2014 za kvalificirane elektroničke evidencije utvrđene su u Prilogu ovoj Uredbi.

Članak 2.

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 16. prosinca 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) Službene primjedbe Europskog nadzornika za zaštitu podataka na nacrt Provedbene uredbe o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 u pogledu referentnih normi i specifikacija za kvalificirane elektroničke evidencije.

PRILOG

Popis tehničkih specifikacija i referentnih normi za kvalificirane distribuirane elektroničke evidencije

1. Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

   (a) „konačnost” znači stanje zapisa podataka u elektroničkoj evidenciji u kojem je taj zapis postao nepovratan i ne može se izmijeniti ili ukloniti;

   (b) „distribuirana elektronička evidencija” znači elektronička evidencija koja je podijeljena među nizom čvorova distribuirane elektroničke evidencije i koja se sinkronizira među tim čvorovima mehanizmom konsenzusa;

   (c) „čvor distribuirane elektroničke evidencije” znači uređaj ili proces koji je dio mreže distribuirane elektroničke evidencije u kojem se pohranjuje potpuna ili djelomična kopija zapisa podataka iz elektroničke evidencije;

   (d) „mreža distribuirane elektroničke evidencije” znači mreža čvorova distribuirane elektroničke evidencije koja čini sustav distribuirane elektroničke evidencije;

   (e) „sustav distribuirane elektroničke evidencije” znači sustav u kojem je implementirana distribuirana elektronička evidencija;

   (f) „konsenzus” znači dogovor među čvorovima distribuirane elektroničke evidencije o valjanosti transakcija i održavanju dosljednog i uređenog skupa validiranih transakcija u cijelom sustavu distribuirane elektroničke evidencije;

   (g) „mehanizam konsenzusa” znači skup pravila i procedura za postizanje konsenzusa;

   (h) „važeća pravila” znači skup protokola, politika i mehanizama koji određuju način rada sustava distribuirane elektroničke evidencije, način na koji se podaci validiraju i dodaju u elektroničku evidenciju te način interakcije sudionika;

   (i) „transakcija” znači najmanja jedinica radnog procesa u elektroničkoj evidenciji;

   (j) „radni proces” znači jedan ili više slijedova radnji potrebnih za postizanje ishoda koji je u skladu s važećim pravilima za određenu elektroničku evidenciju;

   (k) „validirana transakcija” znači transakcija čija su potrebna cjelovitost, autentičnost i uvjeti specifični za protokol provjereni u skladu s važećim pravilima za sustav distribuirane elektroničke evidencije;

   (l) „kriptografska veza” znači upućivanje na podatke koje se uspostavlja primjenom odgovarajućih kriptografskih tehnika radi osiguravanja cjelovitosti, autentičnosti ili sljedivosti podataka na koje se upućuje te ispravnog slijeda zapisa podataka;

   (m) „izvješće o evidenciji” znači strukturirani prikaz provjerljivih informacija izdvojenih iz zapisa podataka elektroničke evidencije koji daje uvid u određene aktivnosti, stanja ili sukladnost s unaprijed definiranim pravilima;

   (n) „pružatelj kvalificirane elektroničke evidencije” znači kvalificirani pružatelj usluga povjerenja koji pruža kvalificiranu uslugu povjerenja koja se sastoji od bilježenja podataka u kvalificiranu elektroničku evidenciju;

   (o) „kvalificirana distribuirana elektronička evidencija” znači distribuirana elektronička evidencija koja ispunjava zahtjeve za kvalificiranu elektroničku evidenciju.

2. Ako kvalificirani pružatelj usluga povjerenja treba izraditi izvješće o evidenciji, ono se mora izrađivati automatski.

3. Pružatelji kvalificiranih elektroničkih evidencija izrađuju, ažuriraju i održavaju kvalificiranu elektroničku evidenciju te u nju bilježe elektroničke podatke u skladu sa specifikacijama utvrđenima u dokumentima navedenima u nastavku.

   (a) Za sve pružatelje kvalificiranih elektroničkih evidencija vrijedi norma ETSI EN 319 401 v3.1.1 (2024-06), uz sljedeće prilagodbe:

      — 2.1. Normativna upućivanja:

         [1] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, publikacija Agencije Europske unije za mrežnu i informacijsku sigurnost („ENISA”).

[2] IETF RFC 7515 (svibanj 2015.): „JSON web-potpis (JWS)”.

[3] FIPS PUB 140 – 3 (2019.), „Sigurnosni zahtjevi za kriptografske module”.

[4] Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. 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).

[5] Provedbena uredba Komisije (EU) 2024/3144 od 18. prosinca 2024. o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe.

[6] ISO/IEC 15408:2022 (od 1. do 5. dijela): „Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Kriteriji za vrednovanje sigurnosti IT-a”.

— 6.1. Izjava o praksi usluge povjerenja:

  — REQ-6.1-12 Izjava o praksi za elektroničku evidenciju mora sadržavati barem sljedeće informacije:

    — funkcionalne i tehničke mogućnosti platforme za elektroničku evidenciju i njihovo korištenje za cijelo vrijeme pružanja bilježenja podataka u kvalificiranoj elektroničkoj evidenciji kao kvalificirane usluge povjerenja,

    — konkretne mehanizme za autentifikaciju podrijetla podataka koji se koriste pri pružanju usluge,

    — konkretne mehanizme za uspostavu sekvencijskog kronološkog reda koji se koriste pri pružanju usluge,

    — prema potrebi, kriptografsku vezu koja se koristi za osiguravanje slijeda zapisa podataka,

    — prema potrebi, mehanizam konsenzusa za osiguravanje konačnosti i cjelovitosti zapisa podataka i transakcija pohranjenih u evidenciji, uključujući eventualno razdoblje povećanog opreza dok se ne postignu konačnost i cjelovitost;

    — konkretne mehanizme za cjelovitost podataka koji se koriste pri pružanju usluge.

  — 6.2. Uvjeti poslovanja:

    — REQ-6.2-03 Prije stupanja u ugovorni odnos, ugovarateljima usluge i stranama koje se oslanjaju na uslugu povjerenja na jasan se, sveobuhvatan i lako dostupan način, na javno dostupnom mjestu i pojedinačno, priopćavaju uvjeti poslovanja, uključujući prethodno navedene pojedinosti.

  — 6.3. Politika informacijske sigurnosti:

    — REQ-6.3-04X TSP uspostavlja postupke za obavješćivanje nadzornog tijela o svim promjenama u pružanju usluge povjerenja, u skladu s poslovnim zahtjevima i relevantnim zakonima i propisima. TSP obavijest nadzornom tijelu dostavlja barem:

      — mjesec dana prije uvođenja bilo kakvih promjena,

      — tri mjeseca prije planiranog prestanka pružanja usluga povjerenja.

  — 7.2. Ljudski resursi:

    — REQ-7.2.-04 Osoblje TSP-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-7.2-05X To uključuje redovita (najmanje svakih 12 mjeseci) informiranja o novim prijetnjama i aktualnim sigurnosnim praksama.

— 7.5. Kriptografske mjere:

— REQ-7.5-01X Odgovarajuće sigurnosne kontrole uspostavljaju se za upravljanje svim kriptografskim ključevima, kriptografskim algoritmima i kriptografskim uređajima tijekom njihova životnog ciklusa, prema potrebi u skladu s pristupom kriptografske agilnosti.

— REQ-7.5-02 Za potrebe pružanja svojih usluga povjerenja TSP odabire i primjenjuje odgovarajuće kriptografske tehnike sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1].

Konkretno:

— REQ-7.5-03 Pružatelji kvalificiranih elektroničkih evidencija utvrđuju podrijetlo zapisa podataka u elektroničkoj evidenciji. U tu svrhu koriste napredne elektroničke potpise koji se temelje na kvalificiranim certifikatima ili napredne elektroničke pečate koji se temelje na kvalificiranim certifikatima koje su korisnici usluge izradili u skladu sa sljedećim normama i specifikacijama:

(a) ETSI EN 319 122-1 V1.3.1 (2023-06) Elektronički potpisi i infrastrukture (ESI) – CAdES digitalni potpisi – 1. dio: Gradbeni blokovi i CAdES osnovni potpisi.

(b) ETSI EN 319 132-1 V1.3.1 (2024-07) Elektronički potpisi i infrastruktura povjerenja (ESI) – XAdES digitalni potpisi – 1. dio: Gradbeni blokovi i PAdES osnovni potpisi.

(c) ETSI TS 119 182-1 V1.2.1 (2024-07). Elektronički potpisi i infrastruktura povjerenja (ESI) – JAdES digitalni potpisi – 1. dio: Gradbeni blokovi i JAdES osnovni potpisi, uz sljedeću prilagodbu:

— 5.1.8. Parametar zaglavlja x5c (lanac certifikata X.509):

— Parametar zaglavlja x5c, kako je definiran u točki 4.1.6. norme IETF RFC 7515 [2], mora biti prisutan u JAdES potpisu kao potpisani ili nepotpisani parametar zaglavlja.

— Parametar zaglavlja x5c mora imati semantiku iz točke 4.1.6. norme IETF RFC 7515 [2].

— Parametar zaglavlja x5c mora imati sintaksu iz točke 4.1.6. norme IETF RFC 7515 [2].

— REQ-7.5-04: Pružatelji kvalificiranih elektroničkih evidencija osiguravaju jedinstven sekvencijalni kronološki red zapisa podataka u elektroničkoj evidenciji. U tu svrhu koriste kriptografske veze koje se temelje na *hash* listama ili *hash* stablima, uz upotrebu kriptografskih *hash* funkcija, u skladu sa sljedećim specifikacijama i normama:

(a) SHA-256 ili veća izlazna *hash* vrijednost, u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1];

(b) SHA3-256 ili veća izlazna *hash* vrijednost, u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1].

Druga mogućnost je da, ako se za osiguravanje jedinstvenog sekvencijalnog kronološkog reda zapisa podataka u elektroničkoj evidenciji služe bilježenjem vremena, pružatelji kvalificiranih elektroničkih evidencija koriste kvalificirane vremenske žigove.

— REQ-7.5-05 Pružatelji kvalificiranih elektroničkih evidencija osiguravaju cjelovitost zapisa podataka zabilježenih u kvalificiranoj elektroničkoj evidenciji. U tu svrhu koriste napredne elektroničke potpise koji se temelje na kvalificiranim certifikatima ili napredne elektroničke pečate koji se temelje na kvalificiranim certifikatima u skladu sa sljedećim normama i specifikacijama:

(a) bilo koji format potpisa ili pečata koji je u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1];

(b) SHA-256 ili veća izlazna *hash* vrijednost, u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1];

(c) SHA3-256 ili veća izlazna *hash* vrijednost, u skladu s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [1];

(d) Pružatelji kvalificiranih elektroničkih evidencija osiguravaju da svaka naknadna promjena podataka zabilježenih u kvalificiranoj elektroničkoj evidenciji bude odmah uočljiva.

— REQ-7.5-06 Ako se upotrebljavaju mehanizmi digitalnog potpisa, potpisni privatni ključevi pružatelja kvalificirane elektroničke evidencije čuvaju se i upotrebljavaju 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 ([1]) [6] ili u zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije, verzija CC:2022, 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 temeljenim na zajedničkim kriterijima (EUCC) ([2]) ([3]) [4][5] i certificiran na razini EAL 4 ili višoj; ili

(c) do 31.12.2030. s normom FIPS PUB 140-3 ([4]) [3] 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 certifikacija [4][5], taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

([1]) ISO/IEC 15408:2022 (od 1. do 5. dijela): „Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Kriteriji za vrednovanje sigurnosti IT-a”.

([2]) Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. 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) (SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Provedbena uredba Komisije (EU) 2024/3144 od 18. prosinca 2024. o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe (SL L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

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

— 7.8. Mrežna sigurnost:

— REQ-7.8-14X Potraga za ranjivim točkama koja je obvezna prema REQ-7.8-13 norme obavlja se najmanje svaka tri mjeseca.

— REQ-7.8-18X Penetracijski test koji je obvezan prema REQ-7.8-17X obavlja se najmanje jedanput u godini.

— REQ-7.8-21X Vatrozidovi se također konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad TSP-a.

— 7.9.1. Praćenje i evidentiranje:

— REQ-7.9.1-02X U aktivnostima praćenja uzima se u obzir osjetljivost svih prikupljenih ili analiziranih informacija.

— 7.12. Prekid rada i planovi prekida TSP-a:

— REQ-7.12-02 A TSP-ov plan prekida mora ispunjavati zahtjeve utvrđene u provedbenim aktima donesenima na temelju članka 24. stavka 5. Uredbe (EU) br. 910/2014 [i.1].

(b) Uz to, za sve pružatelje kvalificiranih elektroničkih evidencija koji koriste tehnologije distribuirane elektroničke evidencije vrijede norme:

1. ISO 23257:2022 – Ulančani blokovi i tehnologija distribuirane glavne knjige – Referentna arhitektura, točka 9., s potpunim opisom sustava tehnologije distribuirane elektroničke evidencije, odgovarajuće mreže tehnologije distribuirane elektroničke evidencije i čvorova tehnologije distribuirane elektroničke evidencije;
2. ISO/TS 23635:2022 – Ulančani blokovi i tehnologija distribuirane glavne knjige – Smjernice za upravljanje koje se odnose na pisane i javno dostupne politike i prakse povezane s upravljačkom strukturom za uslugu elektroničke evidencije koju pružaju.