Uradni list
Evropske unije

SL
Serija L

2025/2531

17.12.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/2531

z dne 16. decembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede referenčnih standardov in specifikacij za kvalificirane elektronske evidence

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 45l(3) Uredbe,

ob upoštevanju naslednjega:

(1) Z Uredbo (EU) 2024/1183 Evropskega parlamenta in Sveta ([2]) je bil v Uredbi (EU) št. 910/2014 uveden seznam novih storitev zaupanja in kvalificiranih storitev zaupanja, vključno z beleženjem elektronskih podatkov v kvalificirani elektronski evidenci. Komisija pripravi seznam referenčnih standardov in po potrebi določi specifikacije za take storitve.

(2) Elektronska evidenca je zaporedje elektronskih podatkovnih zapisov, ki zagotavlja celovitost teh zapisov in točnost kronološkega zaporedja teh zapisov. Za zagotovitev kronološkega, doslednega in zanesljivega beleženja podatkov v kvalificirani elektronski evidenci je treba določiti skupni sklop specifikacij za beleženje elektronskih podatkov v kvalificirani elektronski evidenci.

(3) Domneva o skladnosti iz člena 45l(2) Uredbe (EU) št. 910/2014 bi se morala uporabljati samo, kadar so kvalificirane storitve zaupanja za beleženje elektronskih podatkov v kvalificirani elektronski evidenci 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.

(4) 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.

(5) Komisija redno ocenjuje nove tehnologije, prakse, standarde in tehnične specifikacije. V skladu z uvodno izjavo 75 Uredbe (EU) 2024/1183 bi morala Komisija pregledovati in po potrebi posodabljati to uredbo, da bi bila usklajena s svetovnim razvojem, novimi tehnologijami, praksami, 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]) ter, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([4]) se uporabljata za dejavnosti obdelave osebnih podatkov na podlagi te uredbe, pri čemer se upoštevajo tudi Smernice 02/2025 Evropskega odbora za varstvo podatkov o obdelavi osebnih podatkov s tehnologijo veriženja blokov ([5]).

(7) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([6]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 21. oktobra 2025 ([7]).

(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

Referenčni standardi in specifikacije iz člena 45l(3) Uredbe (EU) št. 910/2014 za kvalificirane elektronske evidence 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, 16. decembra 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) Uradne pripombe ENVP k osnutku izvedbene uredbe o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 glede referenčnih standardov in specifikacij za kvalificirane elektronske evidence.

PRILOGA

Seznam tehničnih specifikacij in referenčnih standardov za kvalificirane razpršene elektronske evidence

1. V tej uredbi se uporabljajo naslednje opredelitve pojmov:

   (a) „dokončnost“ pomeni stanje podatkovnega zapisa v elektronski evidenci, ko postane nepovraten in ga ni mogoče spremeniti ali odstraniti;

   (b) „razpršena elektronska evidenca“ pomeni elektronsko evidenco, ki je porazdeljena med več vozlišči razpršene elektronske evidence in sinhronizirana med temi vozlišči z uporabo mehanizma soglasja;

   (c) „vozlišče razpršene elektronske evidence“ pomeni napravo ali postopek, ki je del omrežja razpršene elektronske evidence in shranjuje popolno ali delno kopijo podatkovnih zapisov elektronske evidence;

   (d) „omrežje razpršene elektronske evidence“ pomeni omrežje vozlišč razpršene elektronske evidence, ki sestavlja sistem razpršene elektronske evidence;

   (e) „sistem razpršene elektronske evidence“ pomeni sistem, ki izvaja razpršeno elektronsko evidenco;

   (f) „soglasje“ pomeni dogovor med vozlišči razpršene elektronske evidence o veljavnosti transakcij ter vzdrževanju doslednega in urejenega sklopa potrjenih transakcij v celotnem sistemu razpršene elektronske evidence;

   (g) „mehanizem soglasja“ pomeni sklop pravil in postopkov, s katerimi se doseže soglasje;

   (h) „pravila upravljanja“ pomenijo sklop protokolov, politik in mehanizmov, ki določajo, kako deluje sistem razpršene elektronske evidence, kako se podatki potrjujejo in dodajajo v elektronsko evidenco ter kako poteka interakcija med udeleženci;

   (i) „transakcija“ pomeni najmanjšo enoto delovnega procesa v elektronski evidenci;

   (j) „delovni postopek“ pomeni eno ali več zaporedij ukrepov, potrebnih za dosego rezultata, ki je skladen s pravili upravljanja elektronske evidence;

   (k) „potrjena transakcija“ pomeni transakcijo, za katero so bili v skladu s pravili upravljanja sistema razpršene elektronske evidence preverjeni zahtevani pogoji celovitosti in avtentičnosti ter pogoji, specifični za protokol;

   (l) „kriptografska povezava“ pomeni sklic na podatke, ki se vzpostavi z uporabo ustreznih kriptografskih tehnik za zagotovitev celovitosti, avtentičnosti ali sledljivosti teh podatkov ter pravilnega zaporedja podatkovnih zapisov;

   (m) „evidenčno poročilo“ pomeni strukturirano predstavitev preverljivih informacij, pridobljenih iz podatkovnih zapisov elektronske evidence, ki zagotavlja vpogled v določene dejavnosti, stanja ali skladnost z vnaprej določenimi pravili;

   (n) „ponudnik kvalificirane elektronske evidence“ pomeni ponudnika kvalificirane storitve zaupanja, ki zajema beleženje podatkov v kvalificirani elektronski evidenci;

   (o) „kvalificirana razpršena elektronska evidenca“ pomeni razpršeno elektronsko evidenco, ki izpolnjuje zahteve za kvalificirano elektronsko evidenco.

2. Kadar mora ponudnik kvalificiranih storitev zaupanja pripraviti evidenčno poročilo, se to poročilo pripravi avtomatizirano.

3. Ponudniki kvalificiranih elektronskih evidenc ustvarijo elektronsko evidenco, evidentirajo elektronske podatke v njej, jo posodabljajo in vzdržujejo v skladu s specifikacijami, določenimi:

   (a) za vse ponudnike kvalificiranih elektronskih evidenc v standardu ETSI EN 319 401 v3.1.1 (2024-06) z naslednjimi prilagoditvami:

      — 2.1 Normativne reference:

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

[2] IETF RFC 7515 (maj 2015): „Spletni podpis JSON (JWS)“.

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

[4] Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 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.

[5] Izvedbena uredba Komisije (EU) 2024/3144 z dne 18. decembra 2024 o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe.

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

— 6.1 Izjava o praksi storitev zaupanja:

  — REQ-6.1-12 Izjava o praksi elektronske evidence vsebuje vsaj naslednje informacije:

    — funkcionalne in tehnične zmogljivosti platforme elektronske evidence in njena uporaba med celotnim zagotavljanjem evidentiranja podatkov v kvalificirani elektronski evidenci kot kvalificirane storitve zaupanja;

    — specifični mehanizmi za avtentikacijo izvora podatkov, ki se uporabljajo pri zagotavljanju storitve;

    — specifični mehanizmi za kronološko zaporedje, ki se uporabljajo pri zagotavljanju storitve;

    — kadar je ustrezno, kriptografska povezava, ki se uporablja za zagotovitev zaporedja podatkovnih zapisov;

    — kadar je ustrezno, mehanizem soglasja, ki zagotavlja dokončnost in celovitost podatkovnih zapisov in transakcij, shranjenih v evidenci, vključno z morebitnim previdnostnim obdobjem do doseganja dokončnosti in celovitosti;

    — specifični mehanizmi za celovitost podatkov, ki se uporabljajo pri zagotavljanju storitve.

— 6.2 Pogoji:

  — REQ-6.2-03 Naročniki in stranke, ki se zanašajo na storitev zaupanja, so pred sklenitvijo pogodbenega razmerja na jasen, celovit in lahko dostopen način na javno dostopnem mestu ter posamično obveščeni o natančnih pogojih, vključno z zgoraj naštetimi postavkami.

— 6.3 Informacijska varnostna politika:

  — REQ-6.3-04X Ponudnik storitev zaupanja vzpostavi postopke za obveščanje nadzornega organa o vseh spremembah pri zagotavljanju storitve zaupanja v skladu s poslovnimi zahtevami ter ustreznimi zakoni in predpisi. Ponudnik storitve zaupanja obvesti nadzorni organ najmanj:

    — en mesec pred uvedbo kakršne koli spremembe;

    — tri mesece pred načrtovanim prenehanjem zagotavljanja storitev zaupanja.

— 7.2 Človeški viri:

  — REQ-7.2-04X Osebje ponudnika storitev zaupanja 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-7.2-05X To vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

— 7.5 Kriptografski nadzor:

— REQ-7.5-01X Vzpostavi se ustrezen varnostni nadzor za upravljanje vseh kriptografskih ključev, kriptografskih algoritmov in kriptografskih naprav v njihovem celotnem življenjskem ciklu, po potrebi po pristopu kriptografske prožnosti.

— REQ-7.5-02 Ponudnik storitev zaupanja za namene zagotavljanja svojih storitev zaupanja izbere in uporablja ustrezne kriptografske tehnike, skladne z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1].

Zlasti:

— REQ-7.5-03 Ponudniki kvalificiranih elektronskih evidenc določijo izvor podatkovnih zapisov v elektronski evidenci. V ta namen uporabljajo napredne elektronske podpise, ki temeljijo na kvalificiranih potrdilih, ali napredne elektronske žige, ki temeljijo na kvalificiranih potrdilih, ki jih ustvarijo uporabniki storitve v skladu z naslednjimi standardi in specifikacijami:

(a) ETSI EN 319 122-1 V1.3.1 (2023-06); Elektronski podpisi in infrastruktura (ESI) – Digitalni podpisi CAdES – 1. del: Gradniki in izhodiščni podpisi CAdES;

(b) ETSI EN 319 132-1 V1.3.1 (2024-07); Elektronski podpisi in infrastrukture zaupanja (ESI) – Digitalni podpisi XAdES – 1. del: Gradniki in izhodiščni podpisi XAdES;

(c) ETSI TS 119 182-1 V1.2.1 (2024-07); Elektronski podpisi in infrastrukture zaupanja (ESI) – Digitalni podpisi JAdES – 1. del: Gradniki in izhodiščni podpisi JAdES, z naslednjo prilagoditvijo:

— 5.1.8 Parameter glave x5c (veriga certifikatov X.509)

— Parameter glave x5c, kot je opredeljen v določbi 4.1.6 IETF RFC 7515 [2], je prisoten v podpisu JAdES kot parameter podpisane ali nepodpisane glave.

— Parameter glave x5c ima semantiko iz določbe 4.1.6 IETF RFC 7515 [2].

— Parameter glave x5c ima sintakso iz določbe 4.1.6 IETF RFC 7515 [2].

— REQ-7.5-04: Ponudniki kvalificiranih elektronskih evidenc zagotavljajo enolično kronološko zaporedje podatkovnih zapisov v elektronski evidenci. V ta namen uporabljajo kriptografske povezave, ki temeljijo na zgoščevalnih seznamih ali zgoščevalnih drevesih, z uporabo kriptografskih zgoščevalnih funkcij v skladu z naslednjimi specifikacijami in standardi:

(a) izhodna velikost zgoščene vrednosti SHA-256 ali več, v skladu z „dogovorjenimi kriptografskimi mehanizmi“, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1].

(b) izhodna velikost zgoščene vrednosti SHA3-256 ali več, v skladu z „dogovorjenimi kriptografskimi mehanizmi“, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1].

Alternativno ponudniki kvalificiranih elektronskih evidenc pri uporabi beleženja časa za zagotovitev enoličnega kronološkega zaporedja podatkovnih zapisov v elektronski evidenci uporabljajo kvalificirane časovne žige.

— REQ-7.5-05 Ponudniki kvalificiranih elektronskih evidenc zagotovijo celovitost podatkovnih zapisov v kvalificirani elektronski evidenci. V ta namen uporabljajo napredne elektronske podpise ali žige, ki temeljijo na kvalificiranih potrdilih, v skladu z naslednjimi standardi in specifikacijami:

  (a) katera koli oblika podpisa ali žiga, ki je skladna z „dogovorjenimi kriptografskimi mehanizmi“, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1];

  (b) izhodna velikost zgoščene vrednosti SHA-256 ali več, v skladu z „dogovorjenimi kriptografskimi mehanizmi“, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1];

  (c) izhodna velikost zgoščene vrednosti SHA3-256 ali več, v skladu z „dogovorjenimi kriptografskimi mehanizmi“, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [1].

  (d) ponudniki kvalificiranih elektronskih evidenc zagotavljajo takojšnjo zaznavnost vsake nadaljnje spremembe podatkov, zabeleženih v elektronski evidenci.

— REQ-7.5-06 Kadar se uporabljajo mehanizmi digitalnega podpisa, se zasebni ključ za podpisovanje ponudnika kvalificirane elektronske evidence 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 ([1]) [6] 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 ([2]) ([3]) [4][5] in po EAL 4 ali višje; ali

  (c) do 31. decembra 2030, FIPS PUB 140-3 ([4]) [3] 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 [4][5], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

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

([2]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 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 (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Izvedbena uredba Komisije (EU) 2024/3144 z dne 18. decembra 2024 o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe (UL L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

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

— 7.8 Varnost omrežja:

— REQ-7.8-14X Pregled ranljivosti, ki ga zahteva REQ-7.8-13, se izvede vsaj enkrat na četrtletje.

— REQ-7.8-18X Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X, se izvede vsaj enkrat na leto.

— REQ-7.8-21X Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje ponudnika storitev zaupanja.

— 7.9.1 Spremljanje in beleženje:

— REQ-7.9.1–02X Dejavnosti spremljanja upoštevajo občutljivost vseh zbranih ali analiziranih informacij.

— 7.12 Prenehanje zagotavljanja storitve ponudnika storitev zaupanja in načrti za prenehanje zagotavljanja storitve:

— REQ-7.12-02A Načrt za prenehanje zagotavljanja storitve ponudnika storitev zaupanja mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.1].

(b) dodatno za vse ponudnike kvalificiranih elektronskih evidenc, ki uporabljajo tehnologije razpršene elektronske evidence, v:

(1) standardu ISO 23257:2022 „Tehnologije veriženja blokov in razpršene evidence – Referenčna arhitektura“, določba 9, s popolnim opisom sistema tehnologije razpršene elektronske evidence, ustreznega omrežja tehnologije razpršene elektronske evidence in vozlišč tehnologije razpršene elektronske evidence;

(2) standardu ISO 23635:2022 „Tehnologije veriženja blokov in razpršene evidence – Smernice za upravljanje“ v zvezi s pisnimi in javno dostopnimi politikami in praksami, povezanimi s strukturo upravljanja za storitev elektronske evidence, ki jo zagotavljajo.