Uradni list
Evropske unije

SL
Serija L

2025/1929

30.9.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/1929

z dne 29. septembra 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta v zvezi z vezavo datuma in časa na podatke ter določitvi točnosti časovnih virov za zagotavljanje kvalificiranih elektronskih časovnih 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 42(2) Uredbe,

ob upoštevanju naslednjega:

(1) Kvalificirani elektronski časovni žigi imajo ključno vlogo v digitalnem okolju, saj spodbujajo prehod s tradicionalnih papirnih postopkov na enakovredne elektronske postopke. Kvalificirani elektronski časovni žigi z zavezujočimi informacijami o datumu in času za elektronske podatke pomagajo zagotoviti točnost datuma in časa, ki ju navajajo, ter celovitost digitalnih dokumentov, na katere sta datum in čas vezana.

(2) Domneva o skladnosti iz člena 42(1a) Uredbe (EU) št. 910/2014 bi se morala uporabljati samo, kadar so kvalificirane storitve zaupanja za izdajo kvalificiranih časovnih žigov skladne s standardi iz te uredbe. Ti standardi bi morali odražati uveljavljene prakse in biti splošno priznani v ustreznih sektorjih. Te standarde bi bilo treba prilagoditi tako, da bi vključevali dodatne kontrole, ki bi zagotavljale varnost in zanesljivost kvalificirane storitve zaupanja ter vezavo datuma in časa na podatke in točnost časovnega vira.

(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.

(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.

([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).

([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).

(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 iz člena 42(2) Uredbe (EU) št. 910/2014 so določeni v Prilogi k tej uredbi.

Člen 2

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

([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 časovnega žigosanja

Standarda ETSI EN 319 421 V1.3.1 ([1]) („ETSI EN 319 421“) in ETSI EN 319 422 V1.1.1 ([2]) („ETSI EN 319 422“) se uporabljata z naslednjimi prilagoditvami:

1. Za ETSI EN 319 421

(1) 2.1 Normativne reference:

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) „Elektronski podpisi in infrastrukture zaupanja (ESI) – Protokol časovnega žigosanja in profili žetonov časovnega žiga“.

— [6] neveljavno.

— [9] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“, ki jih je objavila Agencija Evropske unije za kibernetsko varnost (ENISA) ([3]).

— [10] Izvedbena uredba Komisije (EU) 2024/482 ([4]) 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.

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

(2) 3.1 Pogoji

— obdobje veljavnosti potrdila: [časovni interval od notBefore do vključno z notAfter, v katerem certifikacijski organ („CA“) jamči, da bo hranil informacije o statusu potrdila.

(3) 3.3 Kratice

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

(4) 6.2 Izjava o praksi storitev zaupanja

— OVR-6.2-03 TSA v svojo izjavo o razkritju TSA vključi izjave o razpoložljivosti svoje storitve časovnega žigosanja.

(5) 7.3 Osebna varnost

— OVR-7.3-02 Osebje TSA 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-7.3-03 Skladnost z OVR-7.3-02 vključuje redne posodobitve (vsaj na vsakih 12 mesecev) v zvezi z novimi grožnjami in trenutnimi varnostnimi praksami.

([1]) EN 319 421 – Elektronski podpisi in infrastrukture zaupanja (ESI) – Politične in varnostne zahteve za ponudnike storitev zaupanja, ki izdajajo časovne žige, V1.3.1.
([2]) EN 319 422 – Elektronski podpisi in infrastrukture zaupanja (ESI) – Protokol časovnega žigosanja in profili žetonov časovnega žiga, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) UL L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(6) 7.6.2 Ustvarjanje ključev za enoto za časovno žigosanje

— TIS-7.6.2-03 Ustvarjanje ključev za enoto za časovno žigosanje se izvede 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 [3] 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 [10][11] in po EAL 4 ali višje; ali

(c) do 31. decembra 2030, FIPS PUB 140-3 [7] 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 [10][11], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— TIS-7.6.2-04 neveljavno.

— OPOMBA 3 neveljavna.

— TIS-7.6.2-05A Algoritem za ustvarjanje ključev za enoto za časovno žigosanje, dobljeni algoritem za dolžino ključa za podpisovanje in algoritem za podpis, ki se uporablja za podpisovanje časovnih žigov oziroma za podpisovanje potrdil javnih ključev za enoto za časovno žigosanje, v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost [9] in objavila ENISA.

— OPOMBA 4 neveljavna.

— TIS-7.6.2-06 Ključ za podpisovanje za enoto za časovno žigosanje 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.

(7) 7.6.3 Zaščita zasebnega ključa za enoto za časovno žigosanje

— TIS-7.6.3-02 Zasebni ključ za enoto za časovno žigosanje 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 [3] 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 merilih na področju varnosti IT, in po EAL 4 ali višje; ali

(b) EUCC [10][11] in po EAL 4 ali višje; ali

(c) do 31. decembra 2030, FIPS PUB 140-3 [7] 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 [10][11], se ta naprava konfigurira in uporablja v skladu s tem certificiranjem.

— TIS-7.6.3-03 neveljavno.

— OPOMBA 2 neveljavna.

(8) 7.6.7 Konec življenjskega cikla ključa enote za časovno žigosanje

— TIS-7.6.7-03A Datum poteka veljavnosti zasebnih ključev za enoto za časovno žigosanje je v skladu z dogovorjenimi kriptografskimi mehanizmi [9].

— OPOMBA 1 neveljavna.

(9) 7.10 Varnost omrežja

— OVR-7.10-05 Pregled ranljivosti, ki ga zahteva REQ-7.8-13 iz ETSI EN 319 401 [1], se izvede vsaj enkrat na četrtletje.

— OVR-7.10-06 Penetracijsko testiranje, ki ga zahteva REQ-7.8-17X iz ETSI EN 319 401 [1], se izvede vsaj enkrat na leto.

— OVR-7.10-07 Požarni zidovi se konfigurirajo tako, da se preprečijo vsi protokoli in dostopi, ki niso potrebni za delovanje TSA.

(10) 7.14 Prenehanje in načrti za prenehanje TSA

— OVR-7.14-01A Načrt za prenehanje TSP mora izpolnjevati zahteve iz izvedbenih aktov, sprejetih na podlagi člena 24(5) Uredbe (EU) št. 910/2014 [i.4].

2. Za ETSI EN 319 422

(1) 2.1 Normativne reference

— [5] neveljavno.

— [6] neveljavno.

— [8] Evropska certifikacijska skupina za kibernetsko varnost, podskupina za kriptografijo: „Dogovorjeni kriptografski mehanizmi“.

— [9] RFC 9110 Semantika HTTP.

(2) 4.1.3 Zgoščevalni algoritmi, ki se uporabljajo

— Uporablja se naslednja določba:

Zgoščevalni algoritmi za zgoščevanje informacij, ki jih je treba časovno ožigosati, pričakovano trajanje časovnega žiga in izbrane funkcije zgoščevanja glede na čas so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA neveljavna.

(3) 4.2.3 Algoritmi, ki jih je treba podpreti

— Uporablja se naslednja določba:

Algoritmi za podpis s časovnim žigom, ki jih je treba podpreti, so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].“

— OPOMBA neveljavna.

(4) 4.2.4 Dolžine ključev, ki jih je treba podpreti

— Uporablja se naslednja določba:

Dolžine ključev algoritma za podpis izbranega algoritma za podpis so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA.

— OPOMBA neveljavna.

(5) 5.1.3 Algoritmi, ki jih je treba podpreti

— Uporablja se naslednja določba:

Zgoščevalni algoritmi za informacije o časovnem žigosanju, ki jih je treba podpreti, pričakovano trajanje časovnega žiga in izbrane funkcije zgoščevanja glede na čas so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA neveljavna.

(6) 5.2.3 Algoritmi, ki se uporabljajo

— Uporablja se naslednja določba:

Zgoščevalni algoritmi za zgoščevanje informacij, ki jih je treba časovno ožigosati, in algoritmi za podpis žetona časovnega žiga so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA neveljavna.

(7) 6.3 Zahteve glede dolžin ključev

— Uporablja se naslednja določba:

Dolžine ključev izbranega algoritma za podpis za enoto za časovno žigosanje so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA neveljavna.

(8) 6.5 Zahteve glede algoritmov

— Uporablja se naslednja določba:

Javni ključ za enoto za časovno žigosanje in podpis potrdila enote za časovno žigosanje uporabljata algoritme, ki so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

— OPOMBA neveljavna.

(9) 7 Profili za protokole prenosa, ki jih je treba podpreti

— Odjemalec in strežnik za časovno žigosanje podpirata protokol za časovno žigosanje prek HTTPS [9], kot je opredeljeno v določbi 3.4 IETF RFC 3161 [1].

(10) 8 Identifikatorji objektov kriptografskih algoritmov

— Uporablja se naslednja določba:

Javni ključ za enoto za časovno žigosanje in podpis potrdila enote za časovno žigosanje uporabljata algoritme, ki so v skladu z dogovorjenimi kriptografskimi mehanizmi, ki jih je podprla evropska certifikacijska skupina za kibernetsko varnost in objavila ENISA [8].

(11) 9.1 Izjava o skladnosti s predpisi

— Če TSA žeton časovnega žiga razglasi za kvalificirani elektronski časovni žig v skladu z Uredbo (EU) št. 910/2014 [i.2], mora vsebovati en primerek razširitve izjav QC v polju za razširitve žetona časovnega žiga s sintakso, kot je opredeljena v določbi 3.2.6 IETF RFC 3739 [i.3].

— Razširitev izjav QC mora vsebovati en primerek izjave „esi4-qtstStatement-1“, kot je opredeljeno v Prilogi B.

— Razširitev izjav QC se ne označi kot kritična.