2025/1929

30.9.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1929

od 29. rujna 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu povezivanja datuma i vremena s podacima i utvrđivanja točnosti izvora vremena za pružanje kvalificiranih elektroničkih vremenskih žigova

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 42. stavak 2.,

budući da:

(1) Kvalificirani elektronički vremenski žigovi imaju bitnu ulogu u digitalnom okruženju jer pospješuju prelazak s tradicionalnih postupaka koji koriste papir na elektroničke ekvivalente. Povezujući podatke o datumu i vremenu s elektroničkim podacima, kvalificirani elektronički vremenski žigovi pomažu osigurati točnost datuma i vremena koje prikazuju te cjelovitost digitalnih dokumenata povezanih s određenim datumom i vremenom.

(2) Pretpostavka sukladnosti utvrđena u članku 42. stavku 1.a Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge povjerenja za izdavanje kvalificiranih vremenskih žigova pridržavaju normi utvrđenih u ovoj Uredbi. Te bi norme trebale odražavati ustaljenu praksu i biti općepriznate u relevantnim sektorima. Norme bi trebalo prilagoditi tako da uključuju dodatne kontrole kako bi se zajamčile sigurnost i vjerodostojnost kvalificirane usluge povjerenja i povezivanja datuma i vremena s podacima i točnošću izvora vremena.

(3) 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.

(4) 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 provedbenu 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.

(5) Na 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]).

([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).
([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).

(6) 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.

(7) 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 iz članka 42. stavka 2. Uredbe (EU) br. 910/2014 utvrđene su u Prilogu ovoj Uredbi.

Članak 2.

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

([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

Popis referentnih normi i specifikacija za kvalificirane usluge vremenskih žigova

Primjenjuju se norme ETSI EN 319 421 V1.3.1 ([1]) („ETSI EN 319 421”) i ETSI EN 319 422 V1.1.1 ([2]) („ETSI EN 319 422”) uz sljedeće prilagodbe:

1. Za ETSI EN 319 421

1. 2.1. Normativna upućivanja:

— [3] ISO/IEC 15408:2022 (od 1. do 5. dijela) „Sigurnost informacija, kibernetička sigurnost i zaštita privatnosti – Kriteriji za evaluaciju informatičke sigurnosti”.

— [4] ETSI EN 319 401 V3.1.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Zahtjevi općih pravila za pružatelje usluga povjerenja”.

— [5] ETSI EN 319 422 V1.1.1 (2016-03) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Protokol izdavanja vremenskih žigova i profili tokena vremenskog žiga”.

— [6] nevažeće.

— [9] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, publikacija Agencije Europske unije za kibersigurnost („ENISA”) ([3]).

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

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

2. 3.1. Pojmovi

— razdoblje valjanosti certifikata: interval od „notBefore” do i uključujući „notAfter” u kojem certifikacijsko tijelo („CA”) jamči čuvati informacije o statusu certifikata.

3. 3.3. Pokrate

— EUCC europski program kibernetičkosigurnosne certifikacije temeljen na zajedničkim kriterijima

4. 6.2. Izjava o praksi usluge povjerenja

— OVR-6.2-03 TSA u svoju izjavu o pružanju usluga uključuje izjave o dostupnosti svoje usluge vremenskih žigova.

5. 7.3. Sigurnost osoblja

— OVR-7.3-02 Osoblje TSA-a na pouzdanim funkcijama i, ako je primjenjivo, njegovi podugovaratelji na pouzdanim funkcijama, moraju 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.

— OVR-7.3-03 Sukladnost s OVR-7.3-02 uključuje redovita informiranja (barem svakih 12 mjeseci) o novim prijetnjama i aktualnim sigurnosnim praksama.

([1]) EN 319 421 – Elektronički potpisi i infrastrukture (ESI) – Zahtjevi općih i sigurnosnih pravila za vjerodostojne davatelje usluga izdavanja vremenskih žigova, V1.3.1.
([2]) EN 319 422 – Elektronički potpisi i infrastrukture (ESI) – Protokol izdavanja vremenskih žigova i profili tokena vremenskog 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]) SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) SL L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6. 7.6.2. Generiranje ključeva TSU-a

— TIS-7.6.2-03 Generiranje ključeva TSU-a radi se 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 [3] 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 EUCC-om [10][11] i certificiran na razini EAL 4 ili višoj; ili

(c) do 31.12.2030. normom FIPS PUB 140-3 [7] 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 [10][11] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

— TIS-7.6.2-04 nevažeće.

— NAPOMENA 3. nevažeća.

— TIS-7.6.2-05 A Algoritam generiranja ključa TSU-a, dobivena duljina potpisnog ključa i potpisni algoritam koji se koristi za potpisivanje vremenskih žigova odnosno za potpisivanje certifikata TSU javnog ključa moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju [9] i objavila ENISA.

— NAPOMENA 4. nevažeća.

— TIS-7.6.2-06 Potpisni ključ TSU-a smije se uvesti u drugi sigurni kriptografski uređaj i izvesti iz njega samo ako se taj izvoz i uvoz obavljaju na siguran način i u skladu s certifikacijom tih uređaja.

7. 7.6.3. Zaštita privatnog ključa TSU-a

— TIS-7.6.3-02 Privatni ključ TSU-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 [3] 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 temeljenim na zajedničkim kriterijima (EUCC) [10][11] i certificiran na razini EAL 4 ili višoj, ili

(c) do 31.12.2030. normom FIPS PUB 140-3 [7] 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 [10][11] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

— TIS-7.6.3-03 nevažeće.

— NAPOMENA 2. nevažeća.

8. 7.6.7. Kraj životnog ciklusa ključa TSU-a

— TIS-7.6.7-03 A Datum isteka privatnih ključeva TSU-a mora biti sukladan s Dogovorenim kriptografskim mehanizmima [9].

— Napomena 1. nevažeća.

9. 7.10. Mrežna sigurnost

— OVR-7.10-05 Potraga za ranjivim točkama koja je obvezna prema REQ-7.8-13 norme ETSI EN 319 401 [1] obavlja se najmanje svaka tri mjeseca.

— OVR-7.10-06 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319 401 [1] obavlja se najmanje jedanput u godini.

— OVR-7.10-07 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad TSA-a.

10. 7.14. Prekid rada i planovi prekida TSA-a

— OVR-7.14-01 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.4].

2. Za ETSI EN 319 422

1. 2.1. Normativna upućivanja

— [5] nevažeće.

— [6] nevažeće.

— [8] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”.

— [9] RFC 9110 Semantika HTTP-a.

2. 4.1.3. Zahtjevi za algoritme za izračunavanje sažetka (*hash* algoritmi)

— Primjenjuje se sljedeća klauzula:

Algoritmi za izračunavanje sažetka koji se koriste za izradu sažetka informacija na koje se stavlja vremenski žig, očekivano trajanje vremenskog žiga i rok korištenja odabranih *hash* funkcija moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

3. 4.2.3. Zahtjevi za algoritme

— Primjenjuje se sljedeća klauzula:

Algoritmi za potpisivanje tokena vremenskog žiga moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

4. 4.2.4. Zahtjevi za duljine ključeva

— Primjenjuje se sljedeća klauzula:

Duljine ključeva potpisnog algoritma za odabrani potpisni algoritam moraju biti sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA.

— NAPOMENA nevažeća.

5. 5.1.3. Zahtjevi za algoritme

— Primjenjuje se sljedeća klauzula:

Algoritmi za izračunavanje sažetka podataka vremenskog žiga, očekivano trajanje vremenskog žiga i rok korištenja odabranih *hash* funkcija moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

6. 5.2.3. Zahtjevi za algoritme

— Primjenjuje se sljedeća klauzula:

Algoritmi za izračunavanje sažetka koji se koriste za izradu sažetka informacija na koje se stavlja vremenski žig i algoritmi za potpisivanje tokena vremenskog žiga moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

7. 6.3. Zahtjevi za duljinu ključa

— Primjenjuje se sljedeća klauzula:

Duljina ključa za odabrani potpisni algoritam certifikata TSU-a mora biti sukladna s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

8. 6.5. Zahtjevi za algoritme

— Primjenjuje se sljedeća klauzula:

Javni ključ TSU-a i potpisni certifikat TSU-a moraju koristiti algoritme sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

9. 7. Zahtjevi za profile za transportne protokole

— Klijent za vremenski žig i poslužitelj za vremenski žig moraju omogućivati protokol stavljanja vremenskog žiga putem HTTPS-a [9] kako je definiran u točki 3.4. norme IETF RFC 3161 [1].

10. 8. Identifikatori objekta kriptografskih algoritama

— Primjenjuje se sljedeća klauzula:

Javni ključ TSU-a i potpisni certifikat TSU-a moraju koristiti algoritme sukladne s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

11. 9.1. Izjava o sukladnosti s uredbom

— Ako TSA deklarira da je token vremenskog žiga kvalificirani elektronički vremenski žig u skladu s Uredbom (EU) br. 910/2014 [i.2], on mora sadržavati jednu ekstenziju „qcStatements” u polju za ekstenziju tokena vremenskog žiga sa sintaksom kako je definirana u točki 3.2.6. norme IETF RFC 3739 [i.3].

— Ekstenzija „qcStatements” mora sadržavati jednu izjavu „esi4-qtstStatement-1” kako je definirana u Prilogu B.

— Ekstenzija „qcStatements” ne označava se kao kritična.