2025/1946

30.9.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1946

od 29. rujna 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu kvalificiranih usluga čuvanja kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata

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 34. stavak 2. i članak 40.,

budući da:

(1) Kvalificirane usluge čuvanja kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata dugoročno osiguravaju cjelovitost, autentičnost, dokaz postojanja i pristupačnost dokaza o čuvanju tih elektroničkih potpisa i elektroničkih pečata, što omogućuje dokazivanje njihove pravne valjanosti tijekom duljeg razdoblja i jamči da će ih biti moguće validirati neovisno o promjenama tehnologije u budućnosti. Te se usluge pružaju neovisno ili kao dio druge kvalificirane usluge povjerenja, primjerice kvalificiranih usluga elektroničkog arhiviranja.

(2) Pretpostavka sukladnosti utvrđena u članku 34. stavku 1.a i članku 40. Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge čuvanja kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata 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 obuhvate dodatne kontrole koje jamče sigurnost i pouzdanost kvalificirane usluge povjerenja te sposobnost provjere kvalificiranog statusa i tehničke valjanosti potpisa i pečata tijekom duljeg razdoblja.

(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 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).

(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]).

(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

Referentne norme i specifikacije iz članka 34. stavka 2. i članka 40. Uredbe (EU) br. 910/2014 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 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

Popis referentnih normi i specifikacija iz članka 2.

Primjenjuju se norme ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511”) i ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4”) uz sljedeće prilagodbe:

1. Za ETSI TS 119 511

    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 TS 119 612 V2.3.1 – „Elektronički potpisi i infrastrukture (ESI) – Pouzdani popisi”.

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

        — [6] Provedbena uredba Komisije (EU) 2024/482 ([1]) 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).

        — [7] Provedbena uredba Komisije (EU) 2024/3144 ([2]) o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe.

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

        — [9] ETSI TS 119 172-4 V1.1.1 (2021-05) – „Elektronički potpisi i infrastrukture (ESI) – Potpisne politike – 4. dio: Pravila o primjenjivosti potpisa (politika validacije) za europske kvalificirane elektroničke potpise/pečate koji koriste pouzdane popise”.

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

    2. 3.1. Pojmovi

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

    3. 6.4. Profili čuvanja

        — OVR-6.4-08A [WTS][WOS] Očekivano trajanje dokaza mora biti sukladno s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

        — NAPOMENA 3. nevažeća.

    4. 6.5. Politika čuvanja dokaza

        — OVR-6.5-04A Korišteni kriptografski algoritmi moraju biti sukladni s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

        — Napomena 1. nevažeća.

([1]) SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) SL L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5. 7.2. Ljudski resursi

— OVR-7.2-02 Osoblje PSP-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-7.2-03 Sukladnost s OVR-7.2-02 uključuje redovita informiranja (barem svakih 12 mjeseci) o novim prijetnjama i aktualnim sigurnosnim praksama.

6. 7.5. Kriptografske mjere

— OVR-7.5-05 [UVJETNO] Kad PSP potpiše dokaz o čuvanju (ili njegov dio), privatni potpisni ključ PSP-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 [10] 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 [6][7] i certificiran na razini EAL 4 ili višoj; ili

(c) do 31.12.2030. normom FIPS PUB 140-3 [5] 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 [6][7] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

— OVR-7.5-06 [UVJETNO] nevažeće.

— OVR-7.5-07 [UVJETNO] Kad PSP potpiše dokaz o čuvanju (ili njegov dio), sve sigurnosne kopije privatnih potpisnih ključeva PSP-a moraju se, kako bi se sačuvala njihova cjelovitost i povjerljivost, zaštititi sigurnim kriptografskim uređajem prije nego što budu pohranjene izvan tog uređaja.

— OVR-7.5-08 Privatni potpisni ključ PSP-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. 7.8. Mrežna sigurnost

— OVR-7.8-03 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-7.8-04 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319 401 [1] obavlja se najmanje jedanput u godini.

— OVR-7.8-05 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad PSP-a.

8. 7.14. Kriptografsko praćenje

— OVR-7.14-03A Evaluacija kriptografskih algoritama u točkama OVR-7.14.01 i OVR-7.14.02 mora biti sukladna s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [8].

— NAPOMENA nevažeća.

9. 7.12. Prekid rada i planovi prekida TSP-a

— OVR-7.12-01A TSP-ov plan prekida mora ispunjavati zahtjeve utvrđene u provedbenim aktima donesenima na temelju članka 24. stavka 5. Uredbe (EU) br. 910/2014 [i.2].

10. 7.17. Lanac opskrbe

— OVR-7.17-01 Primjenjuju se zahtjevi iz točke 7.14. norme ETSI EN 319 401 [1].

11. Prilog A (normativni): Kvalificirana usluga čuvanja QES-a kako je definirana u članku 34. Uredbe (EU) br. 910/2014.

— OVR-A-02 [PDS][PDS+PGD]

(a) usluga čuvanja čuva sve informacije potrebne za provjeru kvalificiranog statusa elektroničkog potpisa ili elektroničkog pečata koje ne bi bile javno dostupne do kraja razdoblja čuvanja;

(b) usluga čuvanja vodi računa da su čuvane informacije u svakom trenutku razdoblja čuvanja takve da kad se daju kao ulazni podaci za postupak iz točke 4.4. norme ETSI TS 119 172-4 [9], rezultat tog postupka jasno određuje je li digitalni potpis ili pečat u trenutku kad je sačuvan bio tehnički prikladan za implementaciju EU kvalificiranog elektroničkog potpisa ili EU kvalificiranog elektroničkog pečata.

— OVR-A-03 [PDS][PDS+PGD] Vremenski žigovi koji se koriste u dokazima o čuvanju moraju biti kvalificirani vremenski žigovi u skladu s Uredbom (EU) br. 910/2014 [i.2].

2. Za ETSI TS 119 172-4

1. 2.1. Normativna upućivanja:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) – „Elektronički potpisi i infrastruktura povjerenja (ESI) – Postupci za stvaranje i validaciju naprednih elektroničkih potpisa (AdES) – 1. dio: Stvaranje i validacija”.

— Sva upućivanja na „ETSI TS 119 102-1 [1]” tumače se kao upućivanja na „ETSI EN 319 102-1 [1]”.

— [2] ETSI TS 119 612 V2.3.1 – „Elektronički potpisi i infrastrukture (ESI) – Pouzdani popisi”.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) – „Elektronički potpisi i infrastrukture (ESI) – Zahtjevi u pogledu politike i sigurnosti za aplikacije za izradu i validaciju potpisa”.

2. 4.2. Ograničenja validacije i postupci validacije, zahtjev REQ-4.2-03, odjeljak „X.509 ograničenja validacije”, točka (c):

— (i) Ako je certifikat krajnjeg subjekta točka povjerenja, ne smije se koristiti „RevocationChecking-Constraints”.

— (ii) Ako certifikat krajnjeg subjekta nije točka povjerenja, „RevocationCheckingConstraints” postavlja se na „eitherCheck” kako je definirano u redcima (m)2.1. tablice A.2. u točki A.4.2.1. norme ETSI TS 119 172-1 [3].

— (iii) Ako je certifikat krajnjeg subjekta točka povjerenja, ne smiju se koristiti „RevocationFreshness-Constraints” definirani u redcima (m)2.2. tablice A.2. u točki A.4.2.1. norme ETSI TS 119 172-1 [3].

— iv. Ako certifikat krajnjeg subjekta nije točka povjerenja, koriste se „RevocationFreshnessConstraints” definirani u redcima (m)2.2. tablice A.2. u točki A.4.2.1. norme ETSI TS 119 172-1 [3] s najvećom vrijednošću 0 za potpisni certifikat kako bi se informacije o opozivu prihvaćale samo ako su izdane nakon „trenutka posljednje potvrđene valjanosti”. Za certifikate koji nisu potpisni certifikati, uključujući certifikate s vremenskim žigovima, ne postavlja se nikakva vrijednost za „RevocationFreshness-Constraints”.

3. 4.3. Zahtjevi u pogledu validacije potpisa i provjera pravila o primjenjivosti

— REQ-4.3-02 Aplikacije za validaciju potpisa moraju biti sukladne s ETSI TS 119 101 [13].

4. 4.4. Postupak provjere tehničke primjenjivosti (pravila)

— REQ-4.4.2-03 Ako je bilo koja provjera iz REQ-4.4.2.-01 neuspješna:

— postupak se prekida;

— potpis se tehnički određuje neodređenim, tj. da nije ni EU kvalificirani elektronički potpis ni EU kvalificirani elektronički pečat;

— taj rezultat i rezultati postupaka svih međupostupaka navode se u izvješću o provjeri pravila o primjenjivosti potpisa.