2025/1942

30.9.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/1942

od 29. rujna 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu kvalificiranih usluga validacije kvalificiranih elektroničkih potpisa i kvalificiranih usluga validacije 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 33. stavak 2. i članak 40.,

budući da:

(1) Kvalificiranim uslugama validacije kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata osiguravaju se cjelovitost, autentičnost i točnost postupka i rezultata validacije kvalificiranih elektroničkih potpisa odnosno kvalificiranih elektroničkih pečata. Te kvalificirane usluge povjerenja imaju bitnu ulogu u digitalnom poslovnom okruženju jer pospješuju prelazak s tradicionalnih postupaka koji koriste papir na elektroničke ekvivalente.

(2) Pretpostavka sukladnosti utvrđena u članku 33. stavku 2. i članku 40. Uredbe (EU) br. 910/2014 trebala bi vrijediti samo ako se kvalificirane usluge validacije kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata pridržavaju tehničkih 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 kvalificiranih usluga povjerenja te sposobnost provjere kvalificiranog statusa i tehničke valjanosti kvalificiranih elektroničkih potpisa i kvalificiranih elektroničkih pečata.

(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 33. 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 za kvalificirane usluge validacije kvalificiranih elektroničkih potpisa i za kvalificirane usluge validacije kvalificiranih elektroničkih pečata

Primjenuju se norme ETSI TS 119 441 V1.2.1 (2023-10) ([1]) („ETSI TS 119 441”) i ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) („ETSI TS 119 172-4”) uz sljedeće prilagodbe:

1. Za ETSI TS 119 441

1. 2.1. Normativna upućivanja

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

— [3] 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”.

— [4] ISO/IEC 15408-1:2022 – Sigurnost informacija, kibernetička sigurnost i zaštita privatnosti – Kriteriji za evaluaciju informatičke sigurnosti.

— [5] nevažeće.

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

— [7] Provedbena uredba Komisije (EU) 2024/482.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) ([3]).

— [8] 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”.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) – „Elektronički potpisi i infrastrukture (ESI) – Postupci za stvaranje i validaciju naprednih elektroničkih potpisa (AdES) – 2. dio: Izvješće o validaciji potpisa”.

— [10] Europska skupina za kibernetičkosigurnosnu certifikaciju, podskupina za kriptografiju: „Dogovoreni kriptografski mehanizmi”, publikacija Agencije Europske unije za kibersigurnost („ENISA”) ([4]).

— [11] Provedbena uredba Komisije (EU) 2024/3144 o izmjeni Provedbene uredbe (EU) 2024/4822 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe ([5]).

— [12] ETSI EN 319 411-1 – „Elektronički potpisi i vjerodostojne infrastrukture (ESI) – Zahtjevi za opća pravila i za sigurnost za vjerodostojne davatelje usluga certificiranja – 1. dio: Opći zahtjevi”.

([1]) ETSI TS 119 441 – „Elektronički potpisi i infrastrukture (ESI) – Zahtjevi politike za TSP koji pruža usluge validacije potpisa, V1.2.1 (2023-10)”.
([2]) ETSI TS 119 172-4 – „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, V1.1.1 (2021-05)”.
([3]) SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) SL L, 2024/3144, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2. 2.2. Normativna upućivanja

— [i.11] nevažeće.

3. 3.3. Pokrate

— EUCC europski program kibernetičkosigurnosne certifikacije temeljen na zajedničkim kriterijima

4. 4.3.3. Postupak

— NAPOMENA 10. Vidjeti ETSI EN 319 102-1 [3] za upute i ETSI TS 119 172-4 [8] za dodatne upute u slučaju EU kvalificiranog potpisa ili pečata.

5. 6.1. Izjava o praksi uluge validacije potpisa

— OVR-6.1-02 Izjava o praksi SVS-a mora biti strukturirana u skladu s Prilogom A.

— OVR-6.1-03 U izjavi o praksi SVS-a navode se podržane politike SVS-a ili se upućuje na njih (npr. pomoću OID-ova) te ih se ukratko opisuje.

6. 6.3. Politika informacijske sigurnosti

— OVR-6.3-02 U okviru sigurnosne politike dokumentiraju se mjere sigurnosti i kontrole privatnosti implementirane radi zaštite osobnih podataka.

7. 7.2. Ljudski resursi

— OVR-7.2-02 Osoblje SVSP-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.

8. 7.5. Kriptografske mjere

— OVR-7.5-02 [UVJETNO] Nakon potpisivanja izvješća o validaciji pouzdani CA izdaje javni potpisni certifikat SVSP-a koji odgovara privatnom potpisnom ključu SVSP-a u skladu s certifikatskom politikom NCP+ kako je specificirana u ETSI EN 319 411-1 [12]. Trebalo bi ga izdavati u skladu s odgovarajućom certifikatskom politikom specificiranom u ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [UVJETNO] Nakon potpisivanja izvješća o validaciji privatni potpisni ključ SVSP-a čuva se i upotrebljava unutar sigurnog kriptografskog uređaja koji je pouzdan sustav certificiran u skladu:

(a) zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normi ISO/IEC 15408 [4] 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) EUCC-om [7][11] i certificiran na razini EAL 4 ili višoj; ili

(c) do 31.12.2030. normom FIPS PUB 140-3 [6] 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 [7][11] certifikacija, taj se uređaj konfigurira i upotrebljava u skladu s tom certifikacijom.

— OVR-7.5-04 nevažeće.

— OVR-7.5-06 Privatni potpisni ključ SVSP-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.

9. 7.7. Sigurnost rada

— OVR-7.7-02 Kako bi se osiguralo da sustavi na kojima je aplikacija razvijena primjenjuju odgovarajuće sigurnosne mjere i prilagođavaju se specifičnim okruženjima primjene, SVA koristi okruženje primjene koje se održava aktualnim sigurnosnim zakrpama.

— OVR-7.7-03 Na SVA se primjenjuju sljedeći zahtjevi iz točke 5.2. norme ETSI EN 119 101 [1]: GSM 1.3.

10. 7.8. Mrežna sigurnost

— OVR-7.8-02 Ako je dopušten daljinski pristup sustavima za pohranu ili obradu povjerljivih podataka, donosi se formalna politika i opisuje se kao dio elemenata koji se zahtijevaju OVR-6.3 – 02.

— OVR-7.8-04 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-7.8-05 Penetracijski test koji je obvezan prema REQ-7.8-17X norme ETSI EN 319.401 [1] obavlja se najmanje jedanput u godini.

— OVR-7.8-06 Vatrozidovi se konfiguriraju tako da sprečavaju sve protokole i pristupe koji nisu potrebni za rad SVSP-a.

11. 7.12. Prekid pružanja usluga validacije potpisa i planovi za prekid

— OVR-7.12-02 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].

12. 7.14. Lanac opskrbe

— OVR-7.14-01 Primjenjuju se zahtjevi iz točke 7.14. norme ETSI EN 319 401 [2].

13. 8.1. Postupak validacije potpisa

— VPR-8.1-07 Validacijska aplikacija (SVA) mora biti sukladna sa zahtjevima iz točke 7.4., od SIA 1 do SIA 4, norme ETSI TS 119 101 [1].

— VPR-8.1-11 [UVJETNO] Ako SVS namjerava validirati kvalificirane elektroničke potpise ili kvalificirane elektroničke pečate u skladu s člankom 32. stavkom 1. (odnosno člankom 40.) Uredbe (EU) br. 910/2014 [i.1], postupak validacije mora biti u skladu sa zahtjevima iz ETSI TS 119 172-4 [8].

14. 8.2. Protokol validacije potpisa

— SVP-8.2-03 Odgovor za validaciju potpisa mora sadržavati OID politike SVS-a.

15. 8.4. Izvješće o validaciji potpisa

— SVR-8.4-02 Izvješće o validaciji mora biti sukladno s ETSI TS 119 102-2 [9].

— SVR-8.4-07 [UVJETNO] Ako SVS ne obrađuje politiku validacije potpisa u cijelosti, u izvješću se, uz izvješćivanje o potvrđenim ograničenjima, izvješćuje o ograničenjima koja su zanemarena ili poništena.

— SVR-8.4-15 U izvješću o validaciji jasno se navodi podrijetlo svakog PoE-a (potpis, klijent, poslužitelj).

— SVR-8.4-16 Izvješće o validaciji sadržava potpis izvješća o validaciji, koji mora biti digitalni potpis SVSP-a.

— SVR-8.4-17 [UVJETNO] Pri potpisivanju izvješća o validaciji format i cilj potpisa moraju biti sukladni s ETSI TS 119 102-2 [9].

16. 9. Okvir za definiranje politika usluge validacije na temelju politike usluge povjerenja definirane u ovom dokumentu:

— OVR-9-05 [UVJETNO] Pri izradi politike SVS-a na temelju politike usluge povjerenja definirane u ovom dokumentu provodi se procjena rizika kako bi se ocijenili poslovni zahtjevi i odredili sigurnosni zahtjevi koje treba uključiti u politiku za navedenu zajednicu i primjenjivost.

— OVR-9-06 [UVJETNO] Pri izradi politike SVS-a na temelju politike usluge povjerenja definirane u ovom dokumentu, ta se politika odobrava i mijenja u skladu s utvrđenim postupkom preispitivanja, uključujući odgovornosti za održavanje politike.

— OVR-9-07 [UVJETNO] Pri izradi politike SVS-a na temelju politike usluge povjerenja definirane u ovom dokumentu mora postojati utvrđeni postupak preispitivanja kako bi se osiguralo da se politika temelji na izjavama o praksi.

— OVR-9-08 [UVJETNO] Pri izradi politike SVS-a na temelju politike usluge povjerenja definirane u ovom dokumentu TSP svojoj zajednici korisnika stavlja na raspolaganje politike koje podržava.

— OVR-9-09 [UVJETNO] Pri izradi politike SVS-a na temelju politike usluge povjerenja definirane u ovom dokumentu TSP ugovarateljima usluge stavlja na raspolaganje revizije politika koje podržava.

17. Prilog B (normativno) Kvalificirana usluga validacije QES-a kako je definirana u članku 33. Uredbe (EU) br. 910/2014.

— VPR-B-02 [UVJETNO] Ako je SVSP QSVSP, implementacija mora biti sukladna s normom ETSI TS 119 172-4 [8].

— NAPOMENA 2. nevažeća.

— OVR-B-04 [UVJETNO] Ako je SVSP QSVSP, testovima u OVR-B-03 provjeravaju se različiti slučajevi upotrebe, pozitivni i negativni.

— VPR-B-11 [UVJETNO] Ako je SVSP QSVSP, SVSP kontrolira izračunavanje sažetka (ili ga obavlja na strani poslužitelja ili upravlja klijentom ako je ono dopušteno na strani klijenta).

— NAPOMENA 5. nevažeća.

— NAPOMENA 6. nevažeća.

— VPR-B-15 [UVJETNO] Ako je SVSP QSVSP, izvješće o validaciji mora biti sukladno s normom ETSI TS 119 102-2 [9] kako bi se ispunili uvjeti od VPR-B-13 do VPR-B-14.

— VPR-B-16 [UVJETNO] Ako je SVSP QSVSP, implementacija mora biti sukladna s Dogovorenim kriptografskim mehanizmima koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju i objavila ENISA [10] za upotrebu odgovarajućih kriptografskih tehnika pri pružanju kvalificiranih usluga validacije QES-a.

18. Prilog C (informativno) Korelacija zahtjeva s Uredbom (EU) br. 910/2014, odjeljak „Pružanje validacije u skladu s člankom 32. stavkom 1.” drugi stavak:

— Kako bi se osiguralo da se provjere svi uvjeti propisani člankom 32. stavkom 1. i člankom 40. Uredbe (EU) br. 910/2014 [i.1], nužan je pravilan validacijski algoritam. On daje isti deterministički rezultat za potpis ili pečat dan na validaciju. U tu je svrhu ključna politika validacije potpisa. U tu svrhu norma ETSI TS 119 172-4 [8] izdana je na temelju validacijskog algoritma specificiranog u ETSI EN 319 102-1 [3].

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 (2024-11) – „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].

— 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 od 24 sata za potpisni certifikat. Za certifikate koji nisu potpisni certifikati, uključujući certifikate s vremenskim žigovima, ne postavlja se nikakva vrijednost za „RevocationFreshness-Constraints”.

3. 4.4. Postupak provjere tehničke primjenjivosti (pravila)

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

(a) postupak se prekida;

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

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