REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1946 AL COMISIEI

din 29 septembrie 2025

de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește serviciile calificate de păstrare a semnăturilor electronice calificate și a sigiliilor electronice calificate

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ([1]), în special articolul 34 alineatul (2) și articolul 40,

întrucât:

(1) Serviciile calificate de păstrarea semnăturilor electronice calificate și a sigiliilor electronice calificate asigură integritatea pe termen lung, autenticitatea, dovada existenței și accesibilitatea probelor de păstrare ale acestor semnături electronice și sigilii electronice. Acest lucru permite demonstrarea valabilității lor juridice pe perioade lungi și garantează că pot fi validate indiferent de evoluțiile tehnologice viitoare. Aceste servicii sunt furnizate în mod independent sau ca parte a unui alt serviciu de încredere calificat, cum ar fi serviciile calificate de arhivare electronică.

(2) Prezumția de conformitate prevăzută la articolul 34 alineatul (1a) și la articolul 40 din Regulamentul (UE) nr. 910/2014 ar trebui să se aplice numai în cazul în care serviciile calificate de păstrare a semnăturilor electronice calificate și a sigiliilor electronice calificate respectă standardele prevăzute în prezentul regulament. Aceste standarde ar trebui să reflecte practicile consacrate și să fie recunoscute pe scară largă în sectoarele relevante. Acestea ar trebui să fie adaptate pentru a include controale suplimentare care să asigure securitatea și credibilitatea serviciului de încredere calificat, precum și capacitatea de a verifica statutul de calificat și valabilitatea tehnică a semnăturilor și a sigiliilor de-a lungul timpului.

(3) În cazul în care un prestator de servicii de încredere aderă la cerințele prevăzute în anexa la prezentul regulament, organismele de supraveghere ar trebui să presupună conformitatea cu cerințele relevante din Regulamentul (UE) nr. 910/2014 și să ia în considerare în mod corespunzător o astfel de prezumție pentru acordarea sau confirmarea statutului de calificat al serviciului de încredere. Cu toate acestea, un prestator de servicii de încredere calificat se poate baza în continuare pe alte practici pentru a demonstra conformitatea cu cerințele Regulamentului (UE) nr. 910/2014.

(4) Comisia evaluează periodic noile tehnologii, practici, standarde sau specificații tehnice. În conformitate cu considerentul 75 din Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului ([2]), Comisia ar trebui să revizuiască și să actualizeze prezentul regulament, dacă este necesar, pentru a îl menține aliniat la evoluțiile mondiale, la noile tehnologii, standarde sau specificații tehnice, precum și pentru a respecta bunele practici de pe piața internă.

([1]) JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([3]) și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului ([4]) se aplică activităților de prelucrare a datelor cu caracter personal efectuate în temeiul prezentului regulament.

(6) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([5]) și a emis un aviz la 6 iunie 2025.

(7) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Standarde de referință și specificații

Standardele de referință și specificațiile menționate la articolul 34 alineatul (2) și la articolul 40 din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa la prezentul regulament.

Articolul 2

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 29 septembrie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

([3]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1; ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (Directiva privind viața privată și comunicațiile electronice) (JO L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXĂ

Lista standardelor de referință și a specificațiilor menționate la articolul 2

Standardele ETSI TS 119 511 V1.1.1 (2019-06) („ETSI TS 119 511”) și ETSI TS 119 172-4 V1.1.1 (2021-05) („ETSI TS 119 172-4”) se aplică cu următoarele adaptări:

1. În cazul ETSI TS 119 511:

    1. 2.1 Referințe normative:

        — [1] ETSI EN 319 401 V3.1.1 (2024-06) „Semnături electronice și infrastructuri (ESI); Cerințe de politică generală pentru prestatorii de servicii de încredere”.

        — [2] ETSI TS 119 612 (V2.3.1) „Semnături electronice și infrastructuri (ESI); Listele sigure”.

        — [5] FIPS PUB 140-3 (2019) „Cerințe de securitate pentru modulele criptografice”.

        — [6] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei [1] de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC).

        — [7] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei [2] de modificare a Regulamentului de punere în aplicare (UE) 2024/482 în ceea ce privește standardele internaționale aplicabile și de rectificare a regulamentului de punere în aplicare respectiv.

        — [8] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanismele criptografice convenite” publicate de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”) [3].

        — [9] ETSI TS 119 172-4 V1.1.1 (2021-05) „Semnături electronice și infrastructuri (ESI); Politici în materie de semnătură; Partea 4: Norme privind aplicabilitatea semnăturii (politica de validare) pentru semnăturile/sigiliile electronice calificate europene care utilizează liste sigure”.

        — [10] ISO/IEC 15408: 2022 (părțile 1-5) „Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare pentru securitatea IT”.

    2. 3.1 Termeni

        — dispozitiv criptografic securizat: dispozitiv care stochează cheia privată a utilizatorului, protejează această cheie împotriva compromiterii și îndeplinește funcții de semnare sau de decriptare în numele utilizatorului.

    3. 6.4 Profiluri de păstrare

        — OVR-6.4-08A [WTS][WOS] Durata preconizată a dovezilor trebuie să fie conformă cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

        — Nota 3 – necompletată.

    4. 6.5 Politica de păstrare a dovezilor

        — OVR-6.5-04A Algoritmii criptografici utilizați trebuie să fie conformi cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

        — Nota 1 – necompletată.

[1] JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
[2] JO 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 Resurse umane

— OVR-7.2-02 Personalul prestatorului de servicii de păstrare (PSP) cu roluri de încredere și, dacă este cazul, subcontractanții săi cu roluri de încredere trebuie să fie în măsură să îndeplinească cerința privind „cunoștințele de specialitate, experiența și calificările” prin formare și acreditări oficiale sau prin experiență efectivă sau printr-o combinație a celor două.

— OVR-7.2-03 Conformitatea cu OVR-7.2-02 include actualizări periodice (cel puțin o dată la 12 luni) privind noile amenințări și practicile actuale în materie de securitate.

6. 7.5 Comenzi criptografice

— OVR-7.5-05 [CONDIȚIONAT] Atunci când PSP semnează o dovadă de păstrare (sau o parte a acesteia), cheia de semnătură privată a PSP este păstrată și utilizată într-un dispozitiv criptografic securizat care este un sistem de încredere certificat în conformitate cu:

(a) criteriile comune de evaluare a securității IT, astfel cum sunt stabilite în ISO/IEC 15408 [10] sau în criteriile comune de evaluare a securității IT, versiunea CC: 2022, părțile 1-5, publicate de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice, certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

(b) EUCC [6] [7] și certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

(c) până la 31.12.2030, FIPS PUB 140-3 [5] nivelul 3.

Această certificare se referă la un obiectiv de securitate sau un profil de protecție sau un proiect de modul și o documentație de securitate care îndeplinesc cerințele prezentului document, pe baza unei analize a riscurilor și ținând seama de măsurile de securitate fizice și de altă natură, fără caracter tehnic.

În cazul în care dispozitivul criptografic securizat beneficiază de o certificare EUCC [6][7], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— OVR-7.5-06 [CONDIȚIONAT] – necompletat.

— OVR-7.5-07 [CONDIȚIONAT] Atunci când PSP semnează o dovadă de păstrare (sau o parte a acesteia), orice copie de rezervă a cheilor de semnătură private ale PSP trebuie protejată pentru ca integritatea și confidențialitatea acesteia să fie garantată de către dispozitivul criptografic securizat înainte de a fi stocată în afara dispozitivului respectiv.

— OVR-7.5-08A Cheia de semnătură privată a unui PSP este exportată și importată într-un alt dispozitiv criptografic securizat numai în cazul în care acest export și import sunt efectuate în condiții de siguranță și în conformitate cu certificarea dispozitivelor respective.

7. 7.8 Securitatea rețelelor

— OVR-7.8-03 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— OVR-7.8-04 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— OVR-7.8-05 Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității PSP.

8. 7.14 Monitorizare criptografică

— OVR-7.14-03A Evaluarea algoritmilor criptografici din OVR-7.14.01 și OVR-7.14.02 respectă mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

9. 7.12 Încetarea activității TSP și planul privind încetarea activității TSP

— OVR-7.12-01A Planul privind încetarea activității TSP respectă cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014 [i.2].

10. 7.17 Lanțul de aprovizionare

— OVR-7.17-01 Se aplică cerințele specificate în ETSI EN 319 401 [1] clauza 7.14.

11. Anexa A (normativă): Serviciu calificat de păstrare pentru QES, astfel cum este definit la articolul 34 din Regulamentul (UE) nr. 910/2014

— OVR-A-02 [PDS][PDS+PGD]:

(a) serviciul de păstrare păstrează toate informațiile necesare pentru verificarea statutului de calificat al semnăturii sau sigiliului electronic care nu ar fi disponibile publicului până la sfârșitul perioadei de păstrare;

(b) serviciul de păstrare trebuie să se asigure că, în orice moment al perioadei de păstrare, informațiile păstrate sunt de așa natură încât, atunci când sunt furnizate ca date de intrare pentru procesul specificat în clauza 4.4 din ETSI TS 119 172-4 [9], rezultatul acestui proces stabilește în mod clar dacă semnătura sau sigiliul digital era sau nu, la momentul conservării sale, adecvat(ă) din punct de vedere tehnic pentru implementarea unei semnături electronice calificate a UE sau a unui sigiliu electronic calificat al UE.

— OVR-A-03 [PDS][PDS+PGD] Marcajele temporale utilizate în cadrul dovezilor privind păstrarea sunt marcaje temporale calificate în conformitate cu Regulamentul (UE) nr. 910/2014 [i.2].

2. În cazul ETSI TS 119 172-4:

1. 2.1 Referințe normative:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Semnături electronice și infrastructuri de încredere (ESI); Proceduri pentru crearea și validarea semnăturilor digitale AdES; Partea 1: Creare și validare”.

— Toate trimiterile la „ETSI TS 119 102-1 [1]” se interpretează ca trimiteri la „ETSI EN 319 102-1 [1]”.

— [2] ETSI TS 119 612 (V2.3.1) „Semnături electronice și infrastructuri (ESI); Listele sigure”.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Semnături electronice și infrastructuri (ESI); Cerințe de politică și de securitate pentru cererile de creare și validare a semnăturii”.

2. 4.2 Constrângeri de validare și proceduri de validare, cerința REQ-4.2-03, secțiunea „X.509 Constrângeri de validare”, litera (c):

— (i) în cazul în care un certificat al entității finale reprezintă o ancoră de încredere, nu se utilizează RevocationCheckingConstraints;

— (ii) în cazul în care un certificat al entității finale nu reprezintă o ancoră de încredere, RevocationCheckingConstraints se setează la „eitherCheck”, astfel cum este definit în ETSI TS 119 172-1 [3], clauza A.4.2.1, tabelul A.2 rândul (m)2.1;

— (iii) în cazul în care un certificat al entității finale reprezintă o ancoră de încredere, nu se utilizează RevocationFreshnessConstraints definit în ETSI TS 119 172-1 [3], clauza A.4.2.1, tabelul A.2 rândul (m)2.2;

— (iv) în cazul în care un certificat al entității finale nu reprezintă o ancoră de încredere, RevocationFreshnessConstraints definit în ETSI TS 119 172-1 [3], clauza A.4.2.1, tabelul A.2 rândul (m)2.2 trebuie utilizat cu o valoare maximă de 0 pentru certificatul de semnare, asigurându-se că informațiile privind revocarea sunt acceptate numai dacă au fost eliberate după cea mai bună dată de semnare. Nu se stabilește nicio valoare pentru RevocationFreshnessConstraints pentru alte certificate decât certificatul de semnare, inclusiv pentru certificatele care însoțesc marcaje temporale.

3. 4.3 Cerințe privind validarea semnăturii și practicile de verificare a normelor privind aplicabilitatea

— REQ-4.3-02 Cererile de validare a semnăturilor trebuie să fie conforme cu ETSI TS 119 101 [13].

4. 4.4 Procesul de verificare a aplicabilității tehnice (sau a normelor privind aplicabilitatea tehnică)

— REQ-4.4.2-03 În cazul în care oricare dintre verificările specificate în REQ-4.4.2-01 eșuează, atunci:

— procesul se oprește;

— semnătura se stabilește din punct de vedere tehnic ca fiind nedeterminată, și anume nu este nici o semnătură electronică calificată a UE, nici un sigiliu electronic calificat al UE;

— rezultatul de mai sus și rezultatele tuturor proceselor intermediare trebuie să fie reflectate în raportul de verificare referitor la normele privind aplicabilitatea semnăturii.