2025/1942

30.9.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1942 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 validare a semnăturilor electronice calificate și serviciile calificate de validare 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]) și, în special, articolul 33 alineatul (2) și articolul 40,

întrucât:

(1) Serviciile calificate de validare a semnăturilor electronice calificate și a sigiliilor electronice calificate asigură integritatea, autenticitatea și corectitudinea procesului și a rezultatelor validării semnăturilor electronice calificate și, respectiv, a sigiliilor electronice calificate. Aceste servicii de încredere calificate joacă un rol esențial în mediul de afaceri digital prin promovarea tranziției de la procesele tradiționale pe suport de hârtie la cele electronice echivalente.

(2) Prezumția de conformitate prevăzută la articolul 33 alineatul (2) și articolul 40 din Regulamentul (UE) nr. 910/2014 ar trebui să se aplice numai în cazul în care serviciile calificate de validare a semnăturilor electronice calificate și a sigiliilor electronice calificate respectă standardele tehnice prevăzute în prezentul regulament. Standardele respective 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 serviciilor de încredere calificate, precum și capacitatea de a verifica statutul de calificat și valabilitatea tehnică a semnăturilor electronice calificate și a sigiliilor electronice calificate.

(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 și 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 33 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 personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor 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 pentru serviciile calificate de validare a semnăturilor electronice calificate și pentru serviciile calificate de validare a sigiliilor electronice calificate

Standardele ETSI TS 119 441 V1.2.1 (2023-10) ([1]) („ETSI TS 119 441") și ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) („ETSI TS 119 172-4") se aplică cu următoarele adaptări:

1. În cazul ETSI TS 119.441:

1. 2.1 Referințe normative

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

— [3] ETSI EN 319.102-1 V1.4.1 (2024-06) „Semnături electronice și infrastructuri (ESI); Proceduri pentru crearea și validarea semnăturilor digitale AdES; Partea 1: Creare și validare".

— [4] ISO/IEC 15408-1:2022 – Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare pentru securitatea IT.

— [5] necompletat.

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

— [7] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([3]) 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).

— [8] 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".

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Semnături electronice și infrastructuri (ESI); Proceduri pentru crearea și validarea semnăturilor digitale AdES; Partea 2: Raport de validare a semnăturii".

— [10] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanismele criptografice convenite" publicate de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA") ([4]);

— [11] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei ([5]) de modificare a Regulamentului de punere în aplicare (UE) 2024/4822 în ceea ce privește standardele internaționale aplicabile și de rectificare a regulamentului de punere în aplicare respectiv.

— [12] ETSI EN 319 411-1 „Semnături electronice și infrastructuri (ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care emit certificate; Partea 1: Cerințe generale".

([1]) ETSI TS 119 441 – Semnături și infrastructuri electronice (ESI); Cerințe de politică pentru TSP care furnizează servicii de validare a semnăturilor, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – Semnături și infrastructuri electronice (ESI); Politici în materie de semnătură; Partea 4: Norme privind aplicabilitatea semnăturii (politica de validare) pentru semnături/sigilii electronice calificate europene care utilizează liste sigure, V1.1.1 (2021-05).
([3]) JO 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]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2. 2.2 Referințe informative

— [i.11] necompletat.

3. 3.3 Abrevieri

— Sistemul european de certificare a securității cibernetice bazat pe criterii comune EUCC.

4. 4.3.3 Proces

— NOTA 10: A se vedea ETSI EN 319 102-1 [3] pentru orientări și ETSI TS 119 172-4 [8] pentru orientări suplimentare privind semnătura sau sigiliul calificat UE.

5. 6.1 Declarația privind practicile referitoare la serviciul de validare a semnăturilor

— OVR-6.1-02 Declarația privind practicile referitoare la serviciul de validare a semnăturilor (SVS) trebuie structurată în conformitate cu anexa A.

— OVR-6.1-03 Declarația privind practicile referitoare la SVS trebuie să enumere sau să facă trimitere la politicile SVS compatibile (de exemplu, prin intermediul OID) și să le descrie pe scurt.

6. 6.3 Politica în domeniul securității informațiilor

— OVR-6.3-02 Politica de securitate trebuie să documenteze controalele de securitate și confidențialitate puse în aplicare pentru a proteja datele cu caracter personal.

7. 7.2 Resurse umane

— OVR-7.2-02 Personalul prestatorului serviciului de validare a semnăturilor (SVSP) 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.

8. 7.5 Comenzi criptografice

— OVR-7.5-02 [CONDIȚIONAT] La semnarea rapoartelor de validare, certificatul de semnătură publică al SVSP corespunzător cheii private de semnătură a SVSP se eliberează de către o AC de încredere, în conformitate cu politica de certificare a NCP + certificat, astfel cum se specifică în ETSI EN 319 411-1 [12]. Acesta ar trebui să fie eliberat în conformitate cu o politică de certificare corespunzătoare specificată în ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDIȚIONAT] La semnarea rapoartelor de validare, cheia de semnătură privată a SVSP 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 [4] 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 [7] [11] 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 [6] 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 [7] [11], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— OVR-7.5-04 – necompletat.

— OVR-7.5-06A 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.

9. 7.7 Securitatea operațională

— OVR-7.7-02 Pentru a se asigura că sistemele utilizate pentru dezvoltarea aplicației aplică măsuri de securitate adecvate și se adaptează la medii de aplicare specifice, SVA utilizează un mediu de aplicare care este menținut cu soluții de securitate actualizate.

— OVR-7.7-03 Următoarele cerințe specificate în ETSI TS 119 101 [1] clauza 5.2 se aplică SVA: GSM 1.3.

10. 7.8 Securitatea rețelelor

— OVR-7.8-02 Dacă accesul de la distanță la sistemele de stocare sau prelucrare a datelor confidențiale este permis, se adoptă și se descrie o politică oficială ca parte a elementelor impuse de OVR-6.3-02.

— OVR-7.8-04 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— OVR-7.8-05 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— OVR-7.8-06: Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității SVSP.

11. 7.12 Încetarea prestării serviciului de validare a semnăturii și planurile în cazul încetării acestui serviciu

— OVR-7.12-02 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.1].

12. 7.14 Lanțul de aprovizionare

— OVR-7.14-01 Se aplică cerințele specificate în ETSI EN 319 401 [2] clauza 7.14.

13. 8.1 Procesul de validare a semnăturilor

— VPR-8.1-07 Cererea de validare (SVA) trebuie să respecte cerințele din ETSI TS 119 101 [1], clauza 7.4 SIA 1-SIA 4.

— VPR-8.1-11 [CONDIȚIONAT] Atunci când SVS vizează validarea semnăturilor electronice calificate sau a sigiliilor electronice calificate în conformitate cu articolul 32 alineatul (1) (sau, respectiv, articolul 40) din Regulamentul (UE) nr. 910/2014 [i.1], procesul de validare trebuie să respecte cerințele ETSI TS 119 172-4 [8].

14. 8.2 Protocolul de validare a semnăturii

— SVP-8.2-03 Răspunsul de validare a semnăturii trebuie să conțină OID al politicii SVS.

15. 8.4 Raportul de validare a semnăturii

— SVR-8.4-02 Raportul de validare este conform cu ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDIȚIONAT] Atunci când o politică de validare a semnăturii nu este complet prelucrată de SVS, raportul trebuie, pe lângă raportarea privind constrângerile validate, să raporteze cu privire la constrângerile care au fost ignorate sau depășite.

— SVR-8.4-15 Raportul de validare trebuie să indice în mod clar originea fiecărei tehnologii PoE (din interiorul semnăturii, de la client, de la server).

— SVR-8.4-16 Raportul de validare conține o semnătură a raportului de validare, care este semnătura digitală a SVSP.

— SVR-8.4-17 [CONDIȚIONAT] La semnarea rapoartelor de validare, formatul și obiectivul semnăturii trebuie să fie conforme cu ETSI TS 119 102-2 [9].

16. 9 Cadru pentru definirea politicilor privind serviciile de validare, bazat pe o politică privind serviciile de încredere, definită în prezentul document:

— OVR-9-05 [CONDIȚIONAT] Atunci când se elaborează o politică SVS pe baza unei politici privind serviciile de încredere definite în prezentul document, se efectuează o evaluare a riscurilor pentru a evalua cerințele operaționale și a determina cerințele de securitate care trebuie incluse în politica pentru comunitatea și domeniul de aplicabilitate menționate.

— OVR-9-06 [CONDIȚIONAT] Atunci când se elaborează o politică SVS privind o politică de servicii de încredere definită în prezentul document, politica este aprobată și modificată în conformitate cu un proces de revizuire definit, care include responsabilitățile pentru menținerea politicii.

— OVR-9-07 [CONDIȚIONAT] Atunci când se elaborează o politică SVS referitoare la o politică privind serviciile de încredere definită în prezentul document, trebuie să existe un proces de revizuire definit pentru a se asigura că politica este susținută de declarațiile privind practicile.

— OVR-9-08 [CONDIȚIONAT] Atunci când elaborează o politică SVS referitoare la o politică privind serviciile de încredere definită în prezentul document, prestatorul de servicii de încredere pune politicile sprijinite de TSP la dispoziția comunității sale de utilizatori.

— OVR-9-09 [CONDIȚIONAT] Atunci când se elaborează o politică SVS referitoare la o politică privind serviciile de încredere definită în prezentul document, revizuirile politicilor sprijinite de TSP sunt puse la dispoziția abonaților.

17. Anexa B (normativ) Serviciul calificat de validare pentru QES, astfel cum este definit la articolul 33 din Regulamentul (UE) nr. 910/2014:

— VPR-B-02 [CONDIȚIONAT] În cazul în care SVSP este un prestator al serviciului de validare a semnăturilor calificat (QSVSP), punerea în aplicare trebuie să fie conformă cu ETSI TS 119 172-4 [8].

— Nota 2 – necompletată.

— OVR-B-04 [CONDIȚIONAT] În cazul în care SVSP este un QSVSP, testele din OVR-B-03 trebuie să verifice diferite cazuri de utilizare, pozitive și negative.

— VPR-B-11 [CONDIȚIONAT] În cazul în care SVSP este un QSVSP, SVSP controlează calculul hash (fie efectuează calculul în ceea ce privește serverul, fie controlează clientul dacă acest lucru este permis în ceea ce privește clientul).

— Nota 5 – necompletată.

— Nota 6 – necompletată.

— VPR-B-15 [CONDIȚIONAT] În cazul în care SVSP este un QSVSP, pentru a satisface cerințele de la VPR-B-13 la VPR-B-14, raportul de validare trebuie să fie conform cu ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDIȚIONAT] În cazul în care SVSP este un QSVSP, punerea în aplicare respectă mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [10] pentru utilizarea unor tehnici criptografice adecvate atunci când furnizează servicii calificate de validare pentru QES.

18. Anexa C (informativă) Cartografierea cerințelor Regulamentului (UE) nr. 910/2014, secțiunea „Furnizarea validării în conformitate cu articolul 32 alineatul (1)”, al doilea paragraf:

— pentru a se asigura că sunt verificate toate condițiile impuse de articolul 32 alineatul (1) și articolul 40 din Regulamentul (UE) nr. 910/2014 [i.1], este necesar un algoritm de validare corect. Acesta oferă același rezultat determinist pentru o semnătură sau un sigiliu supus validării. Politica de validare a semnăturilor este esențială în acest scop. ETSI TS 119 172-4 [8] a fost emis din această perspectivă, pe baza algoritmului de validare specificat în ETSI EN 319 102-1 [3].

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 (2024-11) „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 24 de ore pentru certificatul de semnare. Nu se stabilește nicio valoare pentru RevocationFreshnessConstraints pentru alte certificate decât certificatul de semnare, inclusiv pentru certificatele compatibile cu marcaje temporale.

3. 4.4 Procesul de verificare a aplicabilității tehnice (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:

(a) procesul se oprește;

(b) 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;

(c) rezultatul de mai sus și rezultatele tuturor proceselor intermediare trebuie să fie reflectate în raportul de verificare a normelor privind aplicabilitatea semnăturii.