2025/2531

17.12.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/2531 AL COMISIEI

din 16 decembrie 2025

de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește standardele de referință și specificațiile privind registrele 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 45l alineatul (3),

întrucât:

(1) Prin Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului ([2]), a fost introdusă în Regulamentul (UE) nr. 910/2014 o listă de noi servicii de încredere și de servicii de încredere calificate, inclusiv înregistrarea datelor electronice într-un registru electronic calificat. Comisia trebuie să stabilească o listă de standarde de referință și, dacă este necesar, să stabilească specificații privind aceste servicii.

(2) Un registru electronic este o secvență de înregistrări electronice de date destinată să asigure integritatea înregistrărilor respective și acuratețea ordinii cronologice a înregistrărilor respective. Pentru a se asigura faptul că înregistrarea datelor într-un registru electronic calificat este ordonată cronologic, coerentă și fiabilă, este necesar să se stabilească un set comun de specificații pentru înregistrarea datelor electronice într-un registru electronic calificat.

(3) Prezumția de respectare a cerințelor prevăzută la articolul 45l alineatul (2) din Regulamentul (UE) nr. 910/2014 ar trebui să se aplice numai în cazul în care serviciile de încredere calificate pentru înregistrarea datelor electronice într-un registru electronic calificat respectă standardele prevăzute în prezentul regulament. Aceste standarde ar trebui să reflecte practicile consacrate și să fie recunoscute pe scară largă în sectoarele relevante. Standardele ar trebui adaptate pentru a include controale suplimentare care să asigure securitatea și credibilitatea serviciului de încredere calificat.

(4) 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 prezume conformitatea cu cerințele relevante ale Regulamentului (UE) nr. 910/2014 și să ia în considerare în mod corespunzător o astfel de prezumție pentru acordarea sau confirmarea statutului de serviciu de încredere 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-și demonstra conformitatea cu cerințele Regulamentului (UE) nr. 910/2014.

(5) Comisia evaluează periodic tehnologiile, practicile, standardele sau specificațiile tehnice nou-apărute. În conformitate cu considerentul 75 din Regulamentul (UE) 2024/1183, Comisia ar trebui să revizuiască și, dacă este necesar, să actualizeze prezentul regulament pentru a-l menține aliniat la evoluțiile mondiale, la tehnologiile, practicile, standardele sau specificațiile tehnice nou-apărute 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).

(6) 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, ținând seama, de asemenea, de Orientările 02/2025 ale Comitetului european pentru protecția datelor privind prelucrarea datelor cu caracter personal prin intermediul tehnologiilor blockchain ([5]).

(7) 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 ([6]) și a emis un aviz la 21 octombrie 2025 ([7]).

(8) 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 45l alineatul (3) din Regulamentul (UE) nr. 910/2014, referitoare la registrele electronice calificate, sunt prevăzute în anexa la prezentul regulament.

Articolul 2

Intrarea 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, 16 decembrie 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]) edpb_guidelines_202502_blockchain_en.

([6]) 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).

([7]) Observațiile formale ale AEPD cu privire la proiectul de regulament de punere în aplicare de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 în ceea ce privește standardele de referință și specificațiile privind registrele electronice calificate.

ANEXĂ

Lista specificațiilor tehnice și a standardelor de referință privind registrele electronice distribuite calificate

1. În sensul prezentului regulament, se aplică următoarele definiții:

   (a) „caracter definitiv” înseamnă starea unei înregistrări de date dintr-un registru electronic care corespunde faptului că aceasta a devenit ireversibilă și nu poate fi modificată sau eliminată;

   (b) „registru electronic distribuit” înseamnă un registru electronic care este partajat între un set de noduri de registre electronice distribuite și care este sincronizat între nodurile de registre electronice distribuite cu ajutorul unui mecanism de consens;

   (c) „nod de registru electronic distribuit” înseamnă un dispozitiv sau un proces care face parte dintr-o rețea de registre electronice distribuite și care stochează o copie completă sau parțială a înregistrărilor de date dintr-un registru electronic;

   (d) „rețea de registre electronice distribuite” înseamnă o rețea de noduri de registre electronice distribuite care alcătuiesc un sistem de registre electronice distribuite;

   (e) „sistem de registre electronice distribuite” înseamnă un sistem care implementează un registru electronic distribuit;

   (f) „consens” înseamnă un acord între nodurile de registre electronice distribuite cu privire la validitatea tranzacțiilor și menținerea unui set coerent și ordonat de tranzacții validate în cadrul sistemului de registre electronice distribuite;

   (g) „mecanism de consens” înseamnă setul de norme și proceduri prin care se ajunge la un consens;

   (h) „norme de reglementare” înseamnă setul de protocoale, politici și mecanisme care dictează modul în care funcționează sistemul de registre electronice distribuite, modul în care datele sunt validate și adăugate într-un registru electronic și modul în care interacționează participanții;

   (i) „tranzacție” înseamnă cea mai mică unitate a unui proces de lucru din cadrul unui registru electronic;

   (j) „proces de lucru” înseamnă una sau mai multe secvențe de acțiuni necesare pentru a produce un rezultat care este conform cu normele de reglementare ale unui registru electronic;

   (k) „tranzacție validată” înseamnă o tranzacție pentru care integritatea, autenticitatea și condițiile specifice protocolului necesare au fost verificate în conformitate cu normele de reglementare ale sistemului de registre electronice distribuite;

   (l) „legătură criptografică” înseamnă o trimitere la date care este stabilită utilizând tehnici criptografice adecvate pentru a asigura integritatea, autenticitatea sau trasabilitatea datelor de referință și secvența corectă a înregistrărilor de date;

   (m) „raport privind registrul” înseamnă o prezentare structurată a informațiilor verificabile extrase din înregistrările de date ale unui registru electronic și care oferă informații cu privire la anumite activități ori stări sau cu privire la conformitatea cu normele predefinite;

   (n) „furnizor de registru electronic calificat” înseamnă un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat ce constă în înregistrarea datelor într-un registru electronic calificat;

   (o) „registru electronic distribuit calificat” înseamnă un registru electronic distribuit care îndeplinește cerințele aplicabile unui registru electronic calificat.

2. În cazul în care prestatorul de servicii de încredere calificat trebuie să elaboreze un raport privind registrul, raportul respectiv trebuie întocmit într-o manieră automată.

3. Furnizorii de registre electronice calificate creează un registru electronic calificat, înregistrează date electronice într-un astfel de registru, actualizează și mențin registrul respectiv în conformitate cu specificațiile stabilite în:

   (a) Pentru toți furnizorii de registre electronice calificate, ETSI EN 319 401 v3.1.1 (2024-06), cu următoarele adaptări:

      — 2.1 Referințe normative:

         [1] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanisme criptografice convenite”, publicat de Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor („ENISA”).

[2] IETF RFC 7515 (mai 2015): „Semnătura web JSON (JWS)".

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

[4] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC).

[5] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei din 18 decembrie 2024 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.

[6] ISO/IEC 15408:2022 (părțile 1-5): „Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare a securității IT".

— 6.1 Declarația privind practicile referitoare la serviciile de încredere:

  — REQ-6.1-12 Declarația privind practicile referitoare la registrele electronice include cel puțin următoarele informații:

    — capabilitățile funcționale și tehnice ale platformei registrului electronic și utilizarea acesteia pe toată durata prestării serviciului de înregistrare a datelor într-un registru electronic calificat ca serviciu de încredere calificat;

    — mecanismele specifice de autentificare a originii datelor utilizate în momentul prestării serviciului;

    — mecanismele specifice de ordonare cronologică secvențială utilizate în momentul prestării serviciului;

    — dacă este cazul, legătura criptografică utilizată pentru a garanta secvența de înregistrări de date;

    — dacă este cazul, mecanismul de consens care asigură caracterul definitiv și integritatea înregistrărilor de date și a tranzacțiilor stocate în registru, inclusiv orice perioadă de precauție până la obținerea caracterului definitiv și a integrității;

    — mecanismele specifice de asigurare a integrității datelor utilizate în momentul prestării serviciului.

  — 6.2 Termene și condiții:

    — REQ-6.2-03 Înainte de a intra într-o relație contractuală, abonații și părțile care se bazează pe serviciul de încredere sunt informați într-un mod clar, cuprinzător și ușor accesibil, într-un spațiu accesibil publicului și în mod individual, cu privire la termenele și condițiile precise, inclusiv cu privire la elementele enumerate mai sus.

  — 6.3 Politica în domeniul securității informațiilor:

    — REQ-6.3-04X Prestatorul de servicii de încredere stabilește proceduri pentru notificarea organismului de supraveghere cu privire la orice modificare survenită în prestarea serviciului de încredere, în conformitate cu cerințele comerciale și cu actele cu putere de lege și normele administrative relevante. Prestatorul de servicii de încredere transmite notificări organismului de supraveghere cel puțin:

      — cu o lună înainte de punerea în aplicare a oricărei modificări;

      — cu trei luni înainte de încetarea planificată a prestării unui serviciu de încredere.

  — 7.2 Resurse umane:

    — REQ-7.2-04X Personalul prestatorului de servicii de încredere cu roluri de încredere trebuie să fie în măsură să îndeplinească cerința privind „cunoștințele de specialitate, experiența și calificările" prin formare și acreditări oficiale, prin experiență efectivă sau printr-o combinație a celor două.

— REQ-7.2-05X Acest lucru include actualizări periodice (cel puțin o dată la 12 luni) cu privire la noile amenințări și la practicile actuale în materie de securitate.

— 7.5 Controale criptografice:

— REQ-7.5-01X Trebuie instituite controale de securitate adecvate pentru gestionarea oricăror chei criptografice, algoritmi criptografici și dispozitive criptografice pe parcursul întregului lor ciclu de viață, urmând, după caz, o abordare bazată pe agilitatea criptografică.

— REQ-7.5-02 În vederea prestării serviciilor de încredere, prestatorul de servicii de încredere selectează și utilizează tehnici criptografice adecvate, conforme cu documentul „Mecanisme criptografice convenite" aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1].

În mod concret:

— REQ-7.5-03 Furnizorii de registre electronice calificate stabilesc originea înregistrărilor de date din registrul electronic. În acest sens, aceștia utilizează semnături electronice avansate bazate pe certificate calificate sau sigilii electronice avansate bazate pe certificate calificate create de utilizatorii serviciului în conformitate cu următoarele standarde și specificații:

(a) ETSI EN 319 122-1 V1.3.1 (2023-06). Semnături electronice și infrastructuri (ESI); Semnături digitale în format CAdES; Partea 1: Elemente de construcție și semnături de bază CAdES.

(b) ETSI EN 319 132-1 V1.3.1 (2024-07). Semnături electronice și infrastructuri de încredere (ESI); Semnături digitale în format XAdES; Partea 1: Elemente de construcție și semnături de bază XAdES.

(c) ETSI TS 119 182-1 V1.2.1 (2024-07). Semnături electronice și infrastructuri de încredere (ESI); Semnături digitale în format JAdES; Partea 1: Elemente de construcție și semnături de bază JAdES, cu următoarea adaptare:

— 5.1.8 Parametrul de antet x5c (X.509 Lanțul de certificate)

— Parametrul de antet x5c, astfel cum este definit în clauza 4.1.6 din IETF RFC 7515 [2], trebuie să fie prezent în semnătura în format JAdES fie ca parametru de antet semnat, fie ca parametru de antet nesemnat.

— Parametrul de antet x5c trebuie să aibă semantica specificată în IETF RFC 7515 [2], clauza 4.1.6.

— Parametrul de antet x5c trebuie să aibă semantica specificată în IETF RFC 7515 [2], clauza 4.1.6.

— REQ-7.5-04: Furnizorii de registre electronice calificate garantează ordinea cronologică secvențială unică a înregistrărilor de date din registrul electronic. În acest scop, ei utilizează legături criptografice bazate pe liste hash sau arbori hash, utilizând funcții hash criptografice, în conformitate cu următoarele specificații și standarde:

(a) SHA-256 sau dimensiuni ale rezultatului funcției hash mai mari, în conformitate cu documentul „Mecanisme criptografice convenite" aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1].

(b) SHA3-256 sau dimensiuni ale rezultatului funcției hash mai mari, în conformitate cu documentul „Mecanisme criptografice convenite" aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1].

Ca alternativă, atunci când recurg la înregistrarea timpului pentru a garanta ordinea cronologică secvențială unică a înregistrărilor de date din registrul electronic, furnizorii de registre electronice calificate trebuie să utilizeze mărci temporale calificate.

— REQ-7.5-05 Furnizorii de registre electronice calificate asigură integritatea înregistrărilor de date dintr-un registru electronic calificat. În acest scop, ei utilizează semnături electronice avansate bazate pe certificate calificate sau sigilii electronice avansate bazate pe certificate calificate, în conformitate cu următoarele standarde și specificații:

  (a) orice format de semnătură sau sigiliu conform cu documentul „Mecanisme criptografice convenite” aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1];

  (b) SHA-256 sau dimensiuni ale rezultatului funcției hash mai mari, în conformitate cu documentul „Mecanisme criptografice convenite” aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1];

  (c) SHA3-256 sau dimensiuni ale rezultatului funcției hash mai mari, în conformitate cu documentul „Mecanisme criptografice convenite” aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [1].

  (d) Furnizorii de registre electronice calificate asigură detectibilitatea imediată a oricărei modificări ulterioare a datelor înregistrate într-un registru electronic calificat.

— REQ-7.5-06 În cazul în care se utilizează mecanisme de semnătură digitală, cheile private de semnătură ale furnizorilor de registre electronice calificate sunt păstrate și utilizate într-un dispozitiv criptografic securizat care este un sistem credibil, certificat în conformitate cu:

  (a) criteriile comune de evaluare a securității IT, astfel cum sunt stabilite în ISO/IEC 15408 ([1]) [6] 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, și certificat la nivelul EAL 4 sau la un nivel de securitate mai ridicat sau

  (b) sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC) ([2]) ([3])[4] [5] și certificat la nivelul EAL 4 sau la un nivel de securitate mai ridicat sau

  (c) până la 31.12.2030, FIPS PUB 140-3 ([4]) [3] nivelul 3.

Această certificare se referă la un obiectiv de securitate sau un profil de protecție ori la 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 [4][5], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

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

([2]) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([3]) Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei din 18 decembrie 2024 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 (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

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

— 7.8 Securitatea rețelelor

— REQ-7.8-14X Scanarea pentru a detecta vulnerabilităților prevăzută de REQ-7.8-13 se efectuează cel puțin o dată pe trimestru.

— REQ-7.8-18X Testul de penetrare prevăzut de REQ-7.8-17X se efectuează cel puțin o dată pe an.

— REQ-7.8-21X: Firewall-urile trebuie configurate astfel încât să se împiedice toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității prestatorului de servicii de încredere.

— 7.9.1 Monitorizare și jurnalizare

— REQ-7.9.1-02X Activitățile de monitorizare țin seama de sensibilitatea oricăror informații colectate sau analizate.

— 7.12 Încetarea activității prestatorului de servicii de încredere și planul în caz de încetare a serviciilor

— REQ-7.12-02A Planul prestatorului de servicii de încredere în caz de încetare a serviciilor respectă cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014 [i.1].

(b) În plus, pentru toți furnizorii de registre electronice calificate care utilizează tehnologiile registrelor electronice distribuite:

1. ISO 23257:2022 Tehnologia blockchain și tehnologia registrelor distribuite – Arhitectura de referință, clauza 9, care oferă o descriere completă a sistemului tehnologic al registrelor electronice distribuite, a rețelei tehnologice a registrelor electronice distribuite corespunzătoare și a nodurilor tehnologice ale registrelor electronice distribuite;
2. ISO/TS 23635:2022. Tehnologia blockchain și tehnologia registrelor distribuite – Orientări privind guvernanța, în ceea ce privește politicile și practicile scrise și accesibile publicului legate de structura de guvernanță a serviciului de registre electronice furnizat.