2025/1944

30.9.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1944 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 standardele de referință pentru procesele de trimitere și primire a datelor în cadrul serviciilor calificate de distribuție electronică înregistrată și în ceea ce privește interoperabilitatea serviciilor respective

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 44 alineatul (2) și articolul 44 alineatul (2b),

întrucât:

(1) Serviciile calificate de distribuție electronică înregistrată oferă un canal securizat pentru transmiterea documentelor, inclusiv dovada trimiterii și primirii datelor. Scopul lor este de a asigura certitudinea identificării destinatarului și de a garanta un nivel ridicat de încredere în identificarea expeditorului.

(2) Prezumția că sunt respectate cerințele, prevăzută la articolul 44 alineatul (1a) din Regulamentul (UE) nr. 910/2014, ar trebui să se aplice numai în cazul în care serviciile de încredere calificate pentru furnizarea de servicii calificate de distribuție electronică înregistrată 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 adaptate pentru a include controale suplimentare care să asigure securitatea și credibilitatea serviciului de încredere calificat.

(3) În cazul în care un prestator de servicii de încredere aderă la cerințele prevăzute în anexa I 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) În temeiul articolului 44 alineatul (2a) din Regulamentul (UE) nr. 910/2014, în cazul în care prestatorii de servicii de încredere calificați convin asupra interoperabilității dintre serviciile pe care le prestează, este important ca aceștia să adere la standardele și specificațiile adecvate, prevăzute în anexa II la prezentul regulament de punere în aplicare, pentru a transfera cu ușurință date electronice înregistrate între doi sau mai mulți prestatori de servicii de încredere calificați și pentru a promova practici echitabile pe piața internă.

(5) 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).

(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 tuturor activităților de prelucrare a datelor cu caracter personal efectuate în temeiul prezentului regulament.

(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 ([5]) și a emis un aviz la 6 iunie 2025.

(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 pentru serviciile calificate de distribuție electronică înregistrată

Standardele de referință și specificațiile menționate la articolul 44 alineatul (2) din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa I la prezentul regulament.

Articolul 2

Standarde de referință și specificații pentru interoperabilitatea dintre serviciile calificate de distribuție electronică înregistrată

Standardele de referință și specificațiile menționate la articolul 44 alineatul (2b) din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa II la prezentul regulament.

Articolul 3

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).

ANEXA I

Lista standardelor de referință și a specificațiilor menționate la articolul 1

Standardul ETSI EN 319 521 V1.1.1 (2019-02) („ETSI EN 319 521”) se aplică cu următoarele adaptări:

1. În cazul ETSI EN 319.521:

(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 EN 319 411-1 V1.5.1 (2025-04) „Semnături electronice și infrastructuri (ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care emit certificate; Partea 1: Cerințe generale”.

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Semnături electronice și infrastructuri (ESI); Servicii de distribuție electronică înregistrată; Partea 1: Cadru și arhitectură”.

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Semnături electronice și infrastructuri (ESI); Servicii de distribuție electronică înregistrată; Partea 2: Conținuturi semantice”.

— [5] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanismele criptografice convenite” publicate de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”) ([1]);

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

— [7] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([2]) 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] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei ([3]) 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.

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

(2) 3.1 Termeni

— sigiliul electronic avansat: astfel cum este definit în Regulamentul (UE) nr. 910/2014 [i.1].

— semnătură electronică avansată: astfel cum este definită în Regulamentul (UE) nr. 910/2014 [i.1].

— sigiliu electronic calificat: astfel cum este definit în Regulamentul (UE) nr. 910/2014 [i.1].

— semnătură electronică calificată: astfel cum este definită în Regulamentul (UE) nr. 910/2014 [i.1].

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

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

(3) 5.1.1 Dispoziții comune

— REQ-ERDS-5.1.1-01 Serviciul de distribuție electronică înregistrată (ERDS) se asigură că disponibilitatea, integritatea și confidențialitatea conținutului utilizatorului sunt garantate în mod adecvat atât timp cât este gestionat de ERDS, selectând tehnici criptografice adecvate de integritate și confidențialitate conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [5].

(4) 5.2.1.1 General

— REQ-QERDS-5.2.1.1-01 Prestatorul de servicii de distribuție electronică înregistrată calificat (QERDSP) verifică, cu un nivel foarte ridicat de încredere, identitatea destinatarului fie direct, fie bazându-se pe un terț și utilizând unul dintre următoarele mijloace sau o combinație a acestora, după caz:

(a) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern;

(b) de la distanță, utilizând un mijloc de identificare electronică care îndeplinește cerințele prevăzute la articolul 8 din Regulamentul (UE) nr. 910/2014 [i.1] în ceea ce privește nivelul de asigurare „ridicat” sau prin intermediul portofelului european pentru identitatea digitală;

(c) prin intermediul unui certificat al unei semnături electronice calificate sau al unui sigiliu electronic calificat;

(d) prin utilizarea altor metode de identificare, care asigură faptul că persoana fizică sau reprezentantul autorizat al persoanei juridice poate fi identificat cu un nivel foarte ridicat de încredere. Asigurarea că această identificare este efectuată cu un nivel foarte ridicat de încredere este confirmată de un organism de evaluare a conformității.

— REQ-QERDS-5.2.1.1-01A QERDSP verifică identitatea expeditorului prin mijloace adecvate, fie direct, fie recurgând la un terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora:

(a) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern;

(b) de la distanță, prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele prevăzute la articolul 8 din Regulamentul (UE) nr. 910/2014 [i.1] în ceea ce privește nivelul de asigurare „substanțial”, cu condiția ca acesta să fi fost emis pe baza prezenței fizice anterioare a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice;

(c) prin intermediul unui certificat al unei semnături electronice avansate sau al unui sigiliu electronic avansat, cu condiția ca certificatul să fi fost eliberat persoanei fizice sau unui reprezentant autorizat al persoanei juridice în conformitate cu politica normalizată de certificare (NCP), astfel cum este definită în ETSI EN 319 411-1 [2]; sau

(d) prin utilizarea altor metode de identificare, care asigură faptul că persoana fizică sau reprezentantul autorizat al persoanei juridice poate fi identificat cu un nivel foarte ridicat de încredere. Asigurarea că această identificare este efectuată cu un nivel ridicat de încredere este confirmată de un organism de evaluare a conformității.

— NOTĂ Partea terță care verifică identitatea expeditorului și a destinatarului poate fi un alt QERDSP dacă expeditorul și destinatarul sunt abonați la alți QERDSP.

(5) 5.2.1.2 Identificarea destinatarului și predarea conținutului utilizatorului

— REQ-QERDS-5.2.1.2-03 Dacă identificarea destinatarului se bazează pe un proces intern al QERDSP, prestatorul de servicii de distribuție electronică înregistrată calificat trebuie să desfășoare întregul proces într-un mediu securizat și controlat.

(6) 5.2.2 Dispoziții privind autentificarea EU QERDS

— REQ-QERDS-5.2.2-03 [CONDIȚIONAT] Atunci când QERDSP leagă mijloacele de autentificare de o identitate a expeditorului, verificată în conformitate cu clauza 5.2.1, aceasta trebuie să fie una dintre următoarele:

(a) mecanisme de autentificare cu doi factori;

(b) portofel european pentru identitatea digitală sau un mijloc de identificare electronică notificat care îndeplinește cerințele prevăzute la articolul 8 din Regulamentul (UE) nr. 910/2014 [i.1] în ceea ce privește nivelul de asigurare „ridicat” sau „substanțial”;

(c) o autentificare TLS reciprocă, care include certificatul eliberat expeditorului în conformitate cu NCP, astfel cum este definită în ETSI EN 319 411-1 [2];

(d) o semnătură digitală susținută de un certificat eliberat în temeiul NCP, astfel cum este definită în ETSI EN 319 411-1 [2];

(e) alte mijloace care asigură autentificarea expeditorului identificat. Conformitatea stabilirii legăturii este certificată de un organism de evaluare a conformității. Exemplu: Aceasta poate include utilizarea unuia dintre mijloacele de mai sus de la literele (a), (b) și (d) pentru înregistrarea unui certificat de client *Transport Layer Security* (TLS) pentru trimiterea automată prin intermediul TLS reciproc sau pentru înregistrarea unui certificat de sigiliu digital utilizat pentru aplicarea unui sigiliu pe afirmațiile în vederea autentificării cu ERDS. Se pot aplica, de asemenea, alte mecanisme în care expeditorii identificați utilizează servicii delegate furnizate de terți.

— REQ-QERDS-5.2.2-03A [CONDIȚIONAT] Atunci când QERDSP leagă mijloacele de autentificare de o identitate a destinatarului verificată în conformitate cu clauza 5.2.1, aceasta este una dintre următoarele, cu condiția ca mijloacele sau orice combinație de mijloace să asigure un nivel foarte ridicat de încredere în ceea ce privește identitatea destinatarului autentificat:

(a) un mecanism de autentificare multifactor;

(b) portofel european pentru identitatea digitală sau un mijloc de identificare electronică notificat care îndeplinește cerințele prevăzute la articolul 8 din Regulamentul (UE) nr. 910/2014 [i.1] în ceea ce privește nivelul de asigurare „ridicat” sau „substanțial”;

(c) un certificat al unei semnături electronice calificate sau al unui sigiliu electronic calificat;

(d) alte mijloace care asigură autentificarea destinatarului identificat. Conformitatea stabilirii legăturii este certificată de un organism de evaluare a conformității. Exemplu: Acest lucru poate include utilizarea unuia dintre mijloacele de mai sus de la literele (a)-(c) pentru înregistrarea unui certificat de client *Transport Layer Security* (TLS) pentru trimiterea automată prin intermediul TLS reciproc sau pentru înregistrarea unui certificat de sigiliu digital utilizat pentru aplicarea unui sigiliu pe afirmațiile în vederea autentificării cu ERDS. Se pot aplica, de asemenea, alte mecanisme în care expeditorii identificați utilizează servicii delegate furnizate de terți.

— REQ-QERDS-5.2.2-04 [CONDIȚIONAT] Dacă expeditorul se conectează la QERDSP printr-o conexiune securizată care necesită autentificarea reciprocă mașină-mașină între mașina expeditorului și serverul QERDSP pe baza certificatelor eliberate în conformitate cu NCP, astfel cum este definită în ETSI EN 319 411-1 [2], atunci, după stabilirea acestei conexiuni securizate, pot fi adoptate mecanisme de autentificare cu un singur factor pentru o a doua etapă a autentificării expeditorului dacă procedurile organizatorice și măsurile de securitate instituite asigură încrederea în autentificarea expeditorului.

(7) 5.4.1 Dispoziții comune

— REQ-ERDS-5.4.1-06 ERDS generează și pune la dispoziția părților interesate legitime dovezi privind evenimentele ERD, astfel cum sunt definite în clauza 6 din ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 ERDSP arhivează dovezile și/sau elementele de probă pentru fiecare dovadă pe care a eliberat-o.

— REQ-ERDS-5.4.1-08 Dovezile ERDS, generate de serviciul de distribuție electronică înregistrată, trebuie să fie conforme cu dovezile semantice definite în clauza 8 din ETSI EN 319 522-2 [4].

(8) 7.2.1 Dispoziții comune

— REQ-ERDS-7.2.1-02 Personalul ERDSP, care îndeplinește 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.

— REQ-ERDS-7.2,1-03 Conformitatea cu REQ-ERDS-7.2,1-02 include actualizări periodice (cel puțin o dată la 12 luni) privind noile amenințări și practicile actuale în materie de securitate.

(9) 7.3.2 Gestionarea mijloacelor de comunicare în masă

— REQ-ERDS-7.3.1-02 Se aplică toate cerințele specificate în ETSI EN 319 401 [1], clauza 7.3.3.

(10) 7.5 Comenzi criptografice

— REQ-ERDS-7.5-01A ERDS selectează și utilizează tehnici criptografice adecvate în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [5].

— REQ-ERDSP-7.5-03 Cheia privată de semnătură a ERDS este stocată și utilizată într-un dispozitiv criptografic securizat care este un sistem fiabil certificat în conformitate cu:

(a) criteriile comune de evaluare a securității IT, astfel cum sunt stabilite în ISO/IEC 15408 [6] sau în criteriile comune de evaluare a securității IT, versiunea CC: 2002, 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) sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC) [7] [8], 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 [9] 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] [8], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

(11) 7.8 Securitatea rețelelor

— REQ-ERDSP-7.8-04 ERDSP utilizează protocoale și algoritmi de ultimă generație pentru criptarea la nivelul stratului de transport, în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [5].

— REQ-ERDSP-7.8-06 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— REQ-ERDSP-7.8-07 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— REQ-ERDSP-7.8-08 Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității prestatorului de servicii de încredere.

(12) 7.12 Încetarea activității ERDSP și planurile privind încetarea activității ERDS

— REQ-ERDS-7.12-03 Planul privind încetarea activității ERDSP respectă cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014 [i.1].

(13) 7.14 Lanțul de aprovizionare

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

ANEXA II

Lista standardelor de referință și a specificațiilor menționate la articolul 2

Se aplică standardele ETSI EN 319 522-1 V1.2.1 (2024-01) („ETSI EN 319 522-1”), ETSI EN 319 522-2 V1.2.1 (2024-01) („ETSI EN 319 522-2”), ETSI EN 319 522-3 V1.2.1 (2024-01) („ETSI EN 319 522-3”), ETSI EN 319 522-4-1 V1.2.1 (2019-01) („ETSI EN 319 522-4-1”), ETSI EN 319 522-4-2 V1.1.1 (2018-09) („ETSI EN 319 522-4-2”) și ETSI EN 319 522-4-3 V1.1.1 (2018-09) („ETSI EN 319 522-4-3”).