2025/1943

30.9.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1943 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 privind certificatele calificate pentru semnături electronice și certificatele calificate pentru sigiliile electronice

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 28 alineatul (6) și articolul 38 alineatul (6),

întrucât:

(1) Certificatele calificate pentru semnăturile electronice și certificatele calificate pentru sigiliile electronice joacă un rol esențial în mediul de afaceri digital, promovând tranziția de la procesele tradiționale pe suport de hârtie la cele electronice echivalente. Prin corelarea datelor de validare a semnăturilor electronice sau a sigiliilor electronice cu o persoană fizică sau, respectiv, juridică și prin confirmarea numelui persoanei respective, certificatele calificate sporesc certitudinea în ceea ce privește identitatea semnatarului și a creatorului sigiliului.

(2) Prezumția de conformitate prevăzută la articolul 28 alineatul (6) și la articolul 38 alineatul (6) din Regulamentul (UE) nr. 910/2014 ar trebui să se aplice numai în cazul în care serviciile de încredere calificate pentru emiterea de certificate calificate pentru semnăturile electronice și serviciile de încredere calificate pentru eliberarea de certificate calificate pentru sigiliile electronice 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 serviciilor de încredere calificate și a conținutului certificatelor 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, la noile tehnologii, standarde sau specificații tehnice, precum și pentru a respecta bunele practici de pe piața internă.

(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.

([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).

([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).

(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 privind certificatele calificate pentru semnăturile electronice și sigiliile electronice

(1) Standardele de referință și specificațiile menționate la articolul 28 alineatul (6) din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa I la prezentul regulament.

(2) Standardele de referință și specificațiile menționate la articolul 38 alineatul (6) din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa II 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

([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 privind certificatele calificate pentru semnăturile electronice

Standardele ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2”), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1”), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2”) și ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5”) se aplică cu următoarele adaptări:

1. În cazul ETSI EN 319 411-2:

1. 2.1 Referințe normative

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Semnături electronice și infrastructuri de încredere (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 de încredere (ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care emit certificate; Partea 1: Cerințe generale”, cu următoarele adaptări:

Clauza 2.1 Referințe normative ale ETSI EN 319 411-1 V1.5.1 se modifică după cum urmează:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 2: Profilul de certificat pentru certificatele eliberate persoanelor fizice”.

— [14] ETSI EN 319 412-1 V1.6.1 „Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 1: Prezentare generală și structuri comune de date”.

— [3] ETSI EN 319 412-5 V2.5.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 5: Declarații privind controlul calității”.

— [5] ETSI EN 319 412-1 V1.6.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 1: Prezentare generală și structuri comune de date”.

— [6] CEN/TS 419261:2015 „Cerințe de securitate pentru sisteme fiabile de gestionare a certificatelor și a marcajelor temporale”.

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

— [8] 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).

— [9] Regulamentul de punere în aplicare (UE) 2024/3144 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).

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

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

([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.

2. 5.2 Cerințe referitoare la declarația privind practicile de certificare (*Certification Practice Statement* – CPS)

— OVR-5.2-02 Politica (politicile) de certificare (*Certificate Policy* – CP) identificate în documentația prestatorului de servicii de încredere (TSP) trebuie să specifice cerințele privind profilurile de certificat care trebuie utilizate.

3. 5.3 Denumirea și identificarea politicii de certificare

— OVR-5.3-01 În cazul în care se aduc modificări unei PC, astfel cum se descrie în clauza 4.2.2, care afectează aplicabilitatea, atunci identificatorul politicii trebuie modificat.

4. 6.1 Responsabilități legate de publicare și de registru

— OVR-6.1-02 Informațiile identificate în DIS-6.1-04 din ETSI EN 319 411-1 [2] sunt puse la dispoziția publicului la nivel internațional.

5. 6.2.2 Validarea inițială a identității

— REG-6.2.2-01A Colectarea atributelor și a dovezilor privind identitatea subiectului, precum și validarea acestora sunt cele specificate în conformitate cu actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (1c) din Regulamentul (UE) nr. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] și [QCP-n-qscd] Identitatea persoanei fizice și, dacă este cazul, orice atribute specifice ale persoanei se verifică în conformitate cu actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (1c) din Regulamentul (UE) nr. 910/2014 [i.1].

— Nota 1 – necompletată.

6. 6.3.3 Eliberarea certificatelor

— GEN-6.3.3-01 Se aplică cerințele GEN-6.3.3-01 – GEN-6.3.3-10 identificate în ETSI EN 319 411-1 [2], clauza 6.3.3.

— GEN-6.3.3-02 [CONDIȚIONAT] În cazul în care se eliberează un certificat unei persoane fizice identificate în asociere cu persoana juridică, atributele subiectului care identifică organizația în certificat reprezintă persoana juridică sau entitatea subordonată persoanei juridice respective, iar identificatorul subiectului din certificat este persoana fizică.

— GEN-6.3.3-03 Identificatorul PC este [OPȚIUNE]:

(a) [QCP-n]

— astfel cum se specifică în clauza 5.3 litera (a); și/sau

— un identificator digital al obiectului (OID), alocat de TSP, de alte părți interesate relevante sau de o standardizare ulterioară pentru o politică de certificare care îmbunătățește cerințele corespunzătoare de politică aplicabile definite în prezentul document.

(b) [QCP-n-qscd]

— astfel cum se specifică în clauza 5.3 litera (c); și/sau

— un OID, alocat de TSP, de alte părți interesate relevante sau de o standardizare ulterioară pentru o politică de certificare care îmbunătățește cerințele corespunzătoare de politică aplicabile definite în prezentul document.

7. 6.3.5 Utilizarea perechii de chei și a certificatelor

— SDP-6.3.5-02A [CONDIȚIONAT] În cazul în care TSP gestionează QSCD pentru subiect, TSP este un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a semnăturii electronice la distanță, în conformitate cu Regulamentul (UE) nr. 910/2014 [i.1]

— SDP-6.3.5-11A Obligațiile abonatului (a se vedea clauza 6.3.4) includ, în cazul în care abonatul sau subiectul generează cheile subiectului:

(a) obligația de a genera cheile subiectului utilizând un algoritm conform cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice [7] și publicate de ENISA, pentru utilizările cheii certificate, astfel cum au fost identificate în PC;

(b) obligația de a utiliza lungimea și algoritmul cheii conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice [7] și publicate de ENISA, pentru utilizările cheii certificate, astfel cum au fost identificate în PC, în perioada de valabilitate a certificatului.

8. 6.3.10 Servicii privind statutul certificatelor

— CSS-6.3.10-08 [CONDIȚIONAT] Dacă sunt furnizate liste ale certificatelor revocate (CRL), TSP păstrează integritatea și disponibilitatea celei mai recente CRL cel puțin pentru perioada specificată în CPS, astfel cum se solicită în CSS-6.3.10-12.

9. 6.4.4 Controale ale personalului

— OVR-6.4.4-02 Personalul TSP 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-6.4.4-03 Conformitatea cu OVR-6.4.4-02 include actualizări periodice (cel puțin o dată la 12 luni) privind noile amenințări și practicile actuale în materie de securitate.

— OVR-6.4.4-04 Pe lângă rolurile de încredere identificate în ETSI EN 319 401 [1] (clauza 7.2-15), trebuie sprijinite rolurile de încredere ale responsabililor cu înregistrarea și revocarea cu responsabilități, astfel cum sunt definite în TS 419261 [6]. În cazurile în care prestatorul de servicii de încredere calificat (QTSP) este gestionat direct de către un stat membru sau un organism din sectorul public sau este exploatat în numele unui stat membru sau al unui organism din sectorul public, aceste roluri suplimentare de încredere pot fi îndeplinite de unul sau mai mulți reprezentanți oficiali care acționează pentru sau în numele responsabililor cu înregistrarea și revocarea care exercită funcții în administrațiile locale sau regionale.

10. 6.4.9 Încetarea activității autorității de certificare (CA) sau a autorității de înregistrare (RA)

— OVR-6.4.9-02 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].

11. 6.5.1 Generarea și instalarea perechilor de chei

— OVR-6.5.1-01A Generarea perechilor de chei CA se efectuează utilizând un algoritm conform cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopul semnării de către CA.

— OVR-6.5.1-01B Lungimea și algoritmul cheii selectate pentru cheia de semnătură a CA sunt conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopul semnării de către CA.

— OVR-6.5.1-01C [CONDIȚIONAT] În cazul în care CA generează cheile subiectului, cheile subiectului generate de CA respectă mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopurile menționate în PC în perioada de valabilitate a certificatului.

12. 6.5.2 Protecția cheilor private și controale tehnice ale modulelor criptografice

— GEN-6.5.2-01 Se aplică toate cerințele identificate în ETSI EN 319 411-1 [2] clauza 6.5.2, cu excepția cerințelor OVR-6.5.2-01, OVR-6.5.2-03 și OVR-6.5.2-04.

— GEN-6.5.2-02 Generarea perechilor de chei ale TSP, inclusiv cheile utilizate de serviciile de revocare și înregistrare, se efectuează în cadrul unui dispozitiv criptografic securizat care este un sistem de încredere certificat, în conformitate cu:

— 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: 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

— sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC) [8] [9], certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

— până la 31.12.2030, FIPS PUB 140-3 [11] 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 [8] [9], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— GEN-6.5.2-03 Cheia de semnătură privată a CA este ținută și utilizată în cadrul unui dispozitiv criptografic securizat care îndeplinește cerințele GEN-6.5.2-01 și GEN-6.5.2-02.

13. 6.5.7 Controale de securitate a rețelei

— OVR-6.5.7-02 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— OVR-6.5.7-03 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— OVR-6.5.7-04 Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității TSP.

14. 6.6.1 Profilul de certificat

— GEN-6.6.1-05 Certificatul include unul dintre identificatorii de politică identificați în GEN-6.3.3-03 [OPȚIUNE]. Certificatul poate include și alte OID alocate de TSP.

2. În cazul ETSI EN 319 412-2:

1. 2.1 Referințe normative

— [2] ETSI EN 319 412-5 V2.5.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 5: Declarații privind controlul calității”.

— [9] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia „Mecanisme criptografice convenite”, publicat de ENISA.

2. 4.2.2 Semnătură

— GEN-4.2.2-2 Algoritmul de semnătură este selectat în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [9].

— NOTA – necompletată.

3. 4.2.3.1 Emitenți persoane juridice

— GEN-4.2.3.1-3 În cazul în care se știe că există un număr de înregistrare adecvat, identitatea emitentului conține identificatorul organizationIdentifier cu valoarea respectivului număr de înregistrare, astfel cum se menționează în registrul oficial corespunzător care stabilește numărul de înregistrare respectiv.

4. 4.2.5 Informații cu privire la cheia publică a subiectului

— GEN-4.2.5-2 Cheia publică a subiectului este selectată în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [9].

— NOTA – necompletată.

5. 4.2.6 Numărul de serie

— GEN-4.2.6-01 Numărul de serie al certificatului (astfel cum se specifică în IETF RFC 5280 [1] clauza 4.1.2.2) este unic pentru fiecare certificat eliberat de TSP.

ANEXA II

Lista standardelor de referință și a specificațiilor pentru certificatele calificate pentru sigiliile electronice

Standardele ETSI EN 319 411-2 V2.6.1 („ETSI EN 319 411-2”), ETSI EN 319 412-1 V1.6.1 („ETSI EN 319 412-1”), ETSI EN 319 412-3 V1.3.1 („ETSI EN 319 412-3”), ETSI EN 319 412-2 V2.4.1 („ETSI EN 319 412-2”) și ETSI EN 319 412-5 V2.5.1 („ETSI EN 319 412-5”) se aplică cu următoarele adaptări:

1. În cazul ETSI EN 319 411-2:

1. 2.1 Referințe normative

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Semnături electronice și infrastructuri de încredere (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 de încredere (ESI); Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care emit certificate; Partea 1: Cerințe generale”, cu următoarele adaptări:

Clauza 2.1 Referințe normative ale ETSI EN 319 411-1 V1.5.1 se modifică după cum urmează:

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

— [10] ETSI EN 319 412-2 V2.4.1 „Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 2: Profilul de certificat pentru certificatele eliberate persoanelor fizice”.

— [14] ETSI EN 319 412-1 V1.6.1 „Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 1: Prezentare generală și structuri comune de date”.

— [3] ETSI EN 319 412-5 V2.5.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 5: Declarații privind controlul calității”.

— [5] ETSI EN 319 412-1 V1.6.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 1: Prezentare generală și structuri comune de date”.

— [6] CEN/TS 419261:2015 „Cerințe de securitate pentru sisteme fiabile de gestionare a certificatelor și a marcajelor temporale” (elaborate de CEN).

— [7] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanisme criptografice convenite” publicate de ENISA.

— [8] Regulamentul de punere în aplicare (UE) 2024/482 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).

— [9] Regulamentul de punere în aplicare (UE) 2024/3144 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.

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

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

2. 5.2 Cerințe referitoare la declarația privind practicile de certificare (*Certification Practice Statement* - CPS)

— OVR-5.2-02 Politica (politicile) de certificare (*Certificate Policy* – CP) identificate în documentația TSP trebuie să specifice cerințele privind profilurile de certificat care trebuie utilizate.

3. 5.3 Denumirea și identificarea politicii de certificare

— OVR-5.3-01 În cazul în care se aduc modificări unei PC, astfel cum se descrie în clauza 4.2.2, care afectează aplicabilitatea, atunci identificatorul politicii trebuie modificat.

4. 6.1 Responsabilități legate de publicare și de registru

— OVR-6.1-02 Informațiile identificate în DIS-6.1-04 din ETSI EN 319 411-1 [2] sunt puse la dispoziția publicului la nivel internațional.

5. 6.2.2 Validarea inițială a identității

— REG-6.2.2-01A Colectarea atributelor și a dovezilor privind identitatea subiectului, precum și validarea acestora sunt cele specificate în conformitate cu actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (1c) din Regulamentul (UE) nr. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] și [QCP-l-qscd] Identitatea persoanei juridice și, dacă este cazul, orice atribute specifice ale persoanei se verifică în conformitate cu actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (1c) din Regulamentul (UE) nr. 910/2014 [i.1].

— NOTA 3 A se vedea nota 2.

6. 6.3.3 Eliberarea certificatelor

— GEN-6.3.3-01 Se aplică cerințele GEN-6.3.3-01 - GEN-6.3.3-10 identificate în ETSI EN 319 411-1 [2], clauza 6.3.3.

— GEN-6.3.3-02 Identificatorul PC este [OPȚIUNE]:

(a) [QCP-l]

— astfel cum se specifică în clauza 5.3 litera (b); și/sau

— un OID, alocat de TSP, de alte părți interesate relevante sau de o standardizare ulterioară pentru o politică de certificare care îmbunătățește cerințele corespunzătoare de politică aplicabile definite în prezentul document.

(b) [QCP-l-qscd]

— astfel cum se specifică în clauza 5.3 litera (d); și/sau

— un OID, alocat de TSP, de alte părți interesate relevante sau de o standardizare ulterioară pentru o politică de certificare care îmbunătățește cerințele de politică aplicabile definite în prezentul document.

7. 6.3.5 Utilizarea perechii de chei și a certificatelor

— SDP-6.3.5-02A [CONDIȚIONAT] În cazul în care TSP gestionează QSCD pentru subiect, TSP este un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a sigiliului electronic la distanță, în conformitate cu Regulamentul (UE) nr. 910/2014 [i.1]

— SDP-6.3.5-11A Obligațiile abonatului (a se vedea clauza 6.3.4) includ, în cazul în care abonatul sau subiectul generează cheile subiectului:

(a) obligația de a genera cheile subiectului utilizând un algoritm conform cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7], pentru utilizările cheii certificate, astfel cum au fost identificate în PC; și

(b) obligația de a utiliza lungimea și algoritmul cheii conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7], pentru utilizările cheii certificate, astfel cum au fost identificate în PC, în perioada de valabilitate a certificatului.

8. 6.3.10 Servicii privind statutul certificatelor

— CSS-6.3.10-08 [CONDIȚIONAT] Dacă sunt furnizate liste ale certificatelor revocate (CRL), TSP păstrează integritatea și disponibilitatea celei mai recente CRL cel puțin pentru perioada specificată în CPS, astfel cum se solicită în CSS-6.3.10-12.

9. 6.4.4 Controale ale personalului

— OVR-6.4.4-02 Personalul TSP 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-6.4.4-03 Conformitatea cu OVR-6.4.4-02 include actualizări periodice (cel puțin o dată la 12 luni) privind noile amenințări și practicile actuale în materie de securitate.

— OVR-6.4.4-04 Pe lângă rolurile de încredere identificate în ETSI EN 319 401 [1] (clauza 7.2-15), trebuie sprijinite rolurile de încredere ale responsabililor cu înregistrarea și revocarea cu responsabilități, astfel cum sunt definite în TS 419261 [6]. În cazurile în care QTSP este gestionat direct de către un stat membru sau un organism din sectorul public sau este exploatat în numele unui stat membru sau al unui organism din sectorul public, aceste roluri suplimentare de încredere pot fi îndeplinite de unul sau mai mulți reprezentanți oficiali care acționează pentru sau în numele responsabililor cu înregistrarea și revocarea care exercită funcții în administrațiile locale sau regionale.

10. 6.4.9 Rezilierea de către autoritatea de certificare (CA) sau autoritatea de înregistrare (RA)

— OVR-6.4.9-02 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]].

11. 6.5.1 Generarea și instalarea perechilor de chei

— OVR-6.5.1-01A Generarea perechilor de chei CA se efectuează utilizând un algoritm conform cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopul semnării de către CA.

— OVR-6.5.1-01B Lungimea și algoritmul cheii selectate pentru cheia de semnătură a CA sunt conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopul semnării de către CA.

— OVR-6.5.1-01C [CONDIȚIONAT] În cazul în care CA generează cheile subiectului, cheile subiectului generate de CA respectă mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [7] în scopurile menționate în PC în perioada de valabilitate a certificatului.

12. 6.5.2 Protecția cheilor private și controale tehnice ale modulelor criptografice

— GEN-6.5.2-01 Se aplică toate cerințele identificate în ETSI EN 319 411-1 [2] clauza 6.5.2, cu excepția cerințelor OVR-6.5.2-01, OVR-6.5.2-03 și OVR-6.5.2-04.

— GEN-6.5.2-02 Generarea perechilor de chei ale TSP, inclusiv cheile utilizate de serviciile de revocare și înregistrare, se efectuează în cadrul unui dispozitiv criptografic securizat care este un sistem de încredere certificat, în conformitate cu:

  — 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: 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

  — sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC) [8] [9], certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

  — până la 31.12.2030, FIPS PUB 140-3 [11] 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 [8] [9], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— GEN-6.5.2-03 Cheia de semnătură privată a CA este ținută și utilizată în cadrul unui dispozitiv criptografic securizat care îndeplinește cerințele GEN-6.5.2-01 și GEN-6.5.2-02.

13. 6.5.7 Controale de securitate a rețelei

— OVR-6.5.7-02 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— OVR-6.5.7-03 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— OVR-6.5.7-04 Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității TSP.

14. 6.6.1 Profilul de certificat

— GEN-6.6.1-05 Certificatul include unul dintre identificatorii de politică identificați în GEN-6.3.3-02 [OPȚIUNE].

2. În cazul ETSI EN 319 412-3:

1. 2.1 Referințe normative

— [2] ETSI EN 319 412-2 V2.4.1 „Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 2: Profilul de certificat pentru certificatele eliberate persoanelor fizice”.

2. 4.2.1 Subiect

— LEG-4.2.1-6 Atributul organizationIdentifier conține o identificare a organizației în cauză, diferită de denumirea organizației. În cazul în care se cunoaște existența unui număr de înregistrare corespunzător, atributul organizationIdentifier conține o valoare a respectivului număr de înregistrare, astfel cum se menționează în registrul oficial corespunzător care stabilește numărul de înregistrare respectiv.

3. În cazul ETSI EN 319 412-2:

1. 2.1 Referințe normative

— [2] ETSI EN 319 412-5 V2.5.1 „Semnături electronice și infrastructuri de încredere (ESI); Profiluri de certificat; Partea 5: Declarații privind controlul calității”.

— [9] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanisme criptografice convenite” publicate de ENISA.

2. 2.2 Referințe informative

— [i.7] necompletat.

3. 4.2.2 Semnătură

— GEN-4.2.2-2 Algoritmul de semnătură este selectat în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [9].

— NOTA – necompletată.

4. 4.2.3.1 Emitenți persoane juridice

   — GEN-4.2.3.1-3 În cazul în care se știe că există un număr de înregistrare adecvat, identitatea emitentului conține identificatorul organizationIdentifier cu valoarea respectivului număr de înregistrare, astfel cum se menționează în registrul oficial corespunzător care stabilește numărul de înregistrare respectiv.

5. 4.2.5 Informații cu privire la cheia publică a subiectului

   — GEN-4.2.5-2 Cheia publică a subiectului este selectată în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [9].

   — NOTA – necompletată.

6. 4.2.6 Numărul de serie

   — GEN-4.2.6-01 Numărul de serie al certificatului (astfel cum se specifică în IETF RFC 5280 [1] clauza 4.1.2.2) este unic pentru fiecare certificat eliberat de TSP.