REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1929 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 stabilirea legăturii între dată și oră și date și stabilirea exactității surselor orei indicate pentru furnizarea mărcilor temporale 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 42 alineatul (2),

întrucât:

(1) Mărcile temporale electronice calificate joacă un rol esențial în mediul digital prin promovarea tranziției de la procesele tradiționale pe suport de hârtie la echivalentele electronice. Prin stabilirea unei legături între informațiile privind data și ora și datele electronice, mărcile temporale electronice calificate contribuie la asigurarea exactității datei și orei pe care acestea o indică și a integrității documentelor digitale la care se raportează data și ora indicate.

(2) Prezumția de conformitate prevăzută la articolul 42 alineatul (1a) din Regulamentul (UE) nr. 910/2014 ar trebui să se aplice numai în cazul în care serviciile de încredere calificate pentru emiterea de mărci temporale calificate respectă standardele stabilite în prezentul regulament. Aceste standarde ar trebui să reflecte practicile consacrate și să fie recunoscute pe scară largă în sectoarele relevante. Aceste standarde ar trebui adaptate pentru a include controale suplimentare care să asigure securitatea și fiabilitatea serviciului de încredere calificat, precum și a stabilirii legăturii între dată și oră și date și a exactității surselor orei.

(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 de punere în aplicare, 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 cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (Directiva privind viața privată și comunicațiile electronice) (JO L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

(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

Standardele de referință și specificațiile menționate la articolul 42 alineatul (2) din Regulamentul (UE) nr. 910/2014 sunt stabilite în anexa la prezentul regulament.

Articolul 2

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).

ANEXĂ

Lista standardelor de referință și a specificațiilor pentru serviciile de marcă temporală calificată

Standardele ETSI EN 319 421 V1.3.1 ([1]) („ETSI EN 319 421") și ETSI EN 319 422 V1.1.1 ([2]) („ETSI EN 319 422") se aplică cu următoarele adaptări:

1. În cazul ETSI EN 319 421:

    1. 2.1 Referințe normative:

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

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

        — [5] ETSI EN 319 422 V1.1.1 (2016-03) „Semnături electronice și infrastructuri (ESI); Profiluri pentru protocolul de marcare temporală și pentru tokenul de marcă temporală".

        — [6] necompletat.

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

        — [10] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([4]) 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).

        — [11] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei ([5]) 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.

    2. 3.1 Termeni

        — perioada de valabilitate a certificatelor: intervalul de timp cuprins între notBefore și notAfter inclusiv, în care autoritatea de certificare („AC") garantează că va păstra informații cu privire la statutul certificatului.

    3. 3.3 Abrevieri

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

    4. 6.2 Declarația privind practicile referitoare la serviciile de încredere

        — OVR-6.2-03 TSA include declarații cu privire la disponibilitatea serviciului său de marcare temporală în declarația sa de informare privind TSA.

    5. 7.3 Securitatea personalului

        — OVR-7.3-02 Personalul TSA 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-7.3-03 Conformitatea cu OVR-7.3-02 include actualizări periodice (cel puțin o dată la 12 luni) privind noile amenințări și practicile actuale în materie de securitate.

([1]) EN 319 421 - Semnături electronice și infrastructuri (ESI) – Cerințe de politică și de securitate pentru prestatorii de servicii de încredere care emit mărci temporale, V1.3.1.

([2]) EN 319 422 – Semnături electronice și infrastructuri (ESI) – Profiluri pentru protocolul de marcare temporală și pentru tokenul de marcă temporală, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.

([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([4]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([5]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6. 7.6.2 Generarea cheilor TSU

— TIS-7.6.2-03 Generarea cheii (cheilor) TSU se efectuează în cadrul unui 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 [3] 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 [10] [11] și certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

(c) până la 31 decembrie 2030, FIPS PUB 140-3 [7] 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 [10] [11], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— TIS-7.6.2-04 – necompletat.

— NOTA 3 – necompletată.

— TIS-7.6.2-05A Algoritmul de generare a cheilor TSU, lungimea cheii de semnare rezultate și algoritmul de semnătură utilizat pentru semnarea mărcilor temporale și, respectiv, pentru semnarea certificatelor de cheie publică ale TSU sunt conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice [9] și publicate de ENISA.

— NOTA 4 – necompletată.

— TIS-7.6.2-06A Cheia de semnătură a TSU este exportată și importată într-un alt dispozitiv criptografic securizat numai în cazul în care acest export și import sunt efectuate în condiții de siguranță și în conformitate cu certificarea dispozitivelor respective.

7. 7.6.3 Protecția cheii private a TSU

— TIS-7.6.3-02 Cheia privată a TSU 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 [3] 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) [10] [11], certificat în conformitate cu EAL 4 sau cu un nivel de securitate mai ridicat; sau

(c) până la 31 decembrie 2030, FIPS PUB 140-3 [7] 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 [10] [11], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

— TIS-7.6.3-03 – necompletat.

— NOTA 2 – necompletată.

8. 7.6.7 Sfârșitul ciclului de viață al cheii TSU

— TIS-7.6.7-03A Data de expirare a cheilor private ale TSU trebuie să respecte mecanismele criptografice convenite [9].

— Nota 1 – necompletată.

9. 7.10 Securitatea rețelelor

— OVR-7.10-05 Scanarea vulnerabilității solicitată de REQ-7.8-13 din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe trimestru.

— OVR-7.10-06 Testul de penetrare prevăzut de REQ-7.8-17X din ETSI EN 319 401 [1] se efectuează cel puțin o dată pe an.

— OVR-7.10-07 Firewall-urile trebuie configurate astfel încât să se prevină toate protocoalele și accesările care nu sunt necesare pentru desfășurarea activității TSA.

10. 7.14 Încetarea prestării serviciului TSA și planurile în caz de încetare a serviciului

— OVR-7.14-01A Planul privind încetarea activității TSP respectă cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014 [i.4].

2. În cazul ETSI EN 319 422:

1. 2.1 Referințe normative

— [5] necompletat.

— [6] necompletat.

— [8] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: „Mecanismele criptografice convenite”.

— [9] RFC 9110 HTTP Semantics.

2. 4.1.3 Algoritmi de dispersie care trebuie utilizați

— Se aplică următoarea clauză:

Algoritmii de dispersie utilizați pentru dispersia informațiilor care trebuie marcate cu marca temporală, durata preconizată a mărcii temporale și funcțiile hash selectate în funcție de timp trebuie să fie conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

3. 4.2.3 Algoritmi care trebuie să beneficieze de sprijin

— Se aplică următoarea clauză:

Algoritmii de semnătură cu token de marcă temporală care trebuie să beneficieze de sprijin trebuie să fie conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

4. 4.2.4 Lungimi ale cheilor care trebuie să beneficieze de sprijin

— Se aplică următoarea clauză:

Lungimile cheilor algoritmului de semnătură pentru algoritmul de semnătură selectat sunt conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA.

— NOTA – necompletată.

5. 5.1.3 Algoritmi care trebuie să beneficieze de sprijin

— Se aplică următoarea clauză:

Algoritmii de dispersie pentru datele de marcă temporală care trebuie să beneficieze de sprijin, durata preconizată a mărcii temporale și funcțiile hash selectate în funcție de timp trebuie să fie conforme cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

6. 5.2.3 Algoritmi care trebuie să fie utilizați

— Se aplică următoarea clauză:

Algoritmii de dispersie utilizați pentru dispersia informațiilor care trebuie marcate cu marca temporală și algoritmii de semnătură cu token de marcă temporală trebuie să fie conformi cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

7. 6.3 Cerințe privind lungimile cheilor

— Se aplică următoarea clauză:

Lungimea cheii pentru algoritmul de semnătură selectat al certificatului TSU este conformă cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

8. 6.5 Cerințe privind algoritmii

— Se aplică următoarea clauză:

Cheia publică a TSU și semnătura certificatului TSU utilizează algoritmi care sunt conformi cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

— NOTA – necompletată.

9. 7 Profiluri pentru protocoalele de transport care trebuie să beneficieze de sprijin

— Clientul de marcă temporală și serverul de marcă temporală trebuie să fie compatibile cu protocolul de marcă temporală prin intermediul HTTPS [9], astfel cum este definit în clauza 3.4 din IETF RFC 3161 [1].

10. 8 Identificatorii de obiect ai algoritmilor criptografici

— Se aplică următoarea clauză:

Cheia publică a TSU și semnătura certificatului TSU utilizează algoritmi care sunt conformi cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de ENISA [8].

11. 9.1 Declarația de conformitate cu regulamentul

— În cazul în care un token de marcă temporală este declarat de TSA ca fiind o marcă temporală electronică calificată în conformitate cu Regulamentul (UE) nr. 910/2014 [i.2], acesta trebuie să conțină o singură instanță a extensiei qcStatements în câmpul extensiei tokenului de marcă temporală, cu utilizarea sintaxei definite în IETF RFC 3739 [i.3], clauza 3.2.6.

— Extensia qcStatements trebuie să conțină o singură instanță a mențiunii „esi4-qtstStatement-1”, astfel cum este definită în anexa B.

— Extensia qcStatements nu este marcată ca fiind critică.