2025/1946

30.9.2025

# REGOLAMENTO DI ESECUZIONE (UE) 2025/1946 DELLA COMMISSIONE

**del 29 settembre 2025**

**recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda i servizi di conservazione qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE ([1]), in particolare l'articolo 34, paragrafo 2, e l'articolo 40,

considerando quanto segue:

(1) I servizi di conservazione qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati garantiscono l'integrità, l'autenticità, la prova dell'esistenza e l'accessibilità a lungo termine delle prove di conservazione di tali firme elettroniche e sigilli elettronici. Ciò consente di dimostrare la loro validità giuridica nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici. Tali servizi sono prestati in modo indipendente o nell'ambito di un altro servizio fiduciario qualificato, come i servizi di archiviazione elettronica qualificati.

(2) La presunzione di conformità di cui all'articolo 34, paragrafo 1 bis, e all'articolo 40, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi di conservazione qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati sono conformi alle norme stabilite nel presente regolamento. Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Esse dovrebbero essere adattate in modo da includere controlli supplementari che garantiscano la sicurezza e l'affidabilità dei servizi fiduciari qualificati, nonché la capacità di verificare nel tempo la qualifica e la validità tecnica delle firme e dei sigilli.

(3) Se un prestatore di servizi fiduciari rispetta i requisiti di cui all'allegato del presente regolamento, gli organismi di vigilanza dovrebbero presumere la conformità ai pertinenti requisiti del regolamento (UE) n. 910/2014 e tenere debitamente conto di tale presunzione per la concessione o la conferma della qualifica del servizio fiduciario. Un prestatore di servizi fiduciari qualificato può comunque fare affidamento su altre pratiche per dimostrare la conformità ai requisiti del regolamento (UE) n. 910/2014.

(4) La Commissione valuta periodicamente le nuove tecnologie, pratiche, norme o specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([2]), la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, norme o specifiche tecniche e per seguire le migliori pratiche sul mercato interno.

([1]) GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([4]) si applicano alle attività di trattamento di dati personali a norma del presente regolamento.

(6) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([5]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 6 giugno 2025.

(7) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

*Articolo 1*

**Norme di riferimento e specifiche**

Le norme di riferimento e le specifiche di cui all'articolo 34, paragrafo 2, e all'articolo 40 del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

*Articolo 2*

**Entrata in vigore**

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 29 settembre 2025

*Per la Commissione*
*La presidente*
Ursula VON DER LEYEN

([3]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

*ALLEGATO*

**Elenco delle norme di riferimento e delle specifiche di cui all'articolo 2**

Le norme ETSI TS 119 511 V1.1.1 (2019-06) ("ETSI TS 119 511") e ETSI TS 119 172-4 V1.1.1 (2021-05) ("ETSI TS 119 172-4") si applicano con gli adeguamenti seguenti.

1. Per ETSI TS 119 511

1) 2.1 Riferimenti normativi

— [1] ETSI EN 319 401 V3.1.1 (2024-06) "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

— [2] ETSI TS 119 612 (V2.3.1) "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

— [5] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules".

— [6] Regolamento di esecuzione (UE) 2024/482 della Commissione ([1]) recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

— [7] Regolamento di esecuzione (UE) 2024/3144 della Commissione ([2]) che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione.

— [8] Gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: "Agreed Cryptographic Mechanisms" (meccanismi crittografici concordati) pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

— [10] ISO/IEC 15408:2022 (parti da 1 a 5) "Information security, cybersecurity and privacy protection – Evaluation criteria for IT security".

2) 3.1 Termini

— dispositivo crittografico sicuro: dispositivo che detiene la chiave privata dell'utente, protegge tale chiave da compromissione ed esegue funzioni di firma o decrittazione per conto dell'utente.

3) 6.4 Profili di conservazione

— OVR-6.4-08A [WTS][WOS] La durata prevista delle prove è conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA 3 vuota.

4) 6.5 Politica in materia di prove di conservazione

— OVR-6.5-04A Gli algoritmi crittografici utilizzati sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA 1 vuota.

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

5) 7.2 Risorse umane

— OVR-7.2-02 Il personale del PSP in ruoli di fiducia e, se del caso, i subcontraenti del PSP in ruoli di fiducia sono in grado di soddisfare il requisito in materia di "competenze, esperienza e qualifiche" mediante formazione e credenziali formali, o effettiva esperienza, o una combinazione di entrambe.

— OVR-7.2-03 La conformità al requisito OVR-7.2-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza.

6) 7.5 Controlli crittografici

— OVR-7.5-05 [CONDIZIONALE] Quando il PSP firma (in parte) una prova di conservazione, la chiave di firma privata del PSP è detenuta e utilizzata all'interno di un dispositivo crittografico sicuro che è un sistema affidabile certificato conformemente a quanto segue:

a) criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 [10] o in "Common Criteria for Information Technology Security Evaluation", versione CC:2022, parti da 1 a 5, pubblicato dai partecipanti all'accordo "Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security", e certificato a livello EAL 4 o superiore; o

b) EUCC [6][7], e certificato a livello EAL 4 o superiore; o

c) fino al 31.12.2030, FIPS PUB 140-3 [5] livello 3.

Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC [6][7], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— OVR-7.5-06 [CONDIZIONALE] vuoto.

— OVR-7.5-07 [CONDIZIONALE] Quando il PSP firma (in parte) una prova di conservazione, eventuali copie di backup delle chiavi di firma private del PSP sono protette dal dispositivo crittografico sicuro per garantirne l'integrità e la riservatezza prima di essere memorizzate al di fuori di tale dispositivo.

— OVR-7.5-08 La chiave di firma privata di un PSP è esportata e importata in un altro dispositivo crittografico sicuro solo se l'esportazione e l'importazione sono effettuate in modo sicuro e conformemente alla certificazione di tali dispositivi.

7) 7.8 Sicurezza della rete

— OVR-7.8-03 La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 della norma ETSI EN 319 401 [1] è eseguita almeno una volta a trimestre.

— OVR-7.8-04 Il test di penetrazione richiesto dal requisito REQ-7.8-17X della norma ETSI EN 319 401 [1] è eseguito almeno una volta all'anno.

— OVR-7.8-05 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento del PSP.

8) 7.14 Monitoraggio crittografico

— OVR-7.14-03A La valutazione degli algoritmi crittografici nei requisiti OVR-7.14.01 e OVR-7.14.02 è conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

9) 7.12 Cessazione del TSP e piani di cessazione

— OVR-7.12-01A Il piano di cessazione del TSP è conforme ai requisiti stabiliti negli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.2].

10) 7.17 Catena di approvvigionamento

— OVR-7.17-01 Si applicano i requisiti specificati nella norma ETSI EN 319 401 [1], punto 7.14.

11) Allegato A (normativo): Servizio di conservazione qualificato delle firme elettroniche qualificate quale definito all'articolo 34 del regolamento (UE) n. 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) Il servizio di conservazione conserva tutte le informazioni necessarie per verificare la qualifica della firma elettronica o del sigillo elettronico che non sarebbero pubblicamente disponibili fino alla fine del periodo di conservazione;

b) il servizio di conservazione garantisce che, in qualsiasi momento durante il periodo di conservazione, le informazioni conservate siano tali da consentire, se fornite come input nel processo di cui al punto 4.4 della norma ETSI TS 119 172-4 [9], che l'esito di tale processo determini chiaramente se, al momento della conservazione, la firma o il sigillo digitale fosse tecnicamente idoneo per l'implementazione di una firma elettronica qualificata dell'UE o di un sigillo elettronico qualificato dell'UE.

— OVR-A-03 [PDS][PDS+PGD] Le validazioni temporali utilizzate nelle prove di conservazione sono validazioni temporali qualificate a norma del regolamento (UE) n. 910/2014 [i.2].

2. Per ETSI TS 119 172-4

1) 2.1 Riferimenti normativi

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

— Tutti i riferimenti a "ETSI TS 119 102-1 [1]" si intendono fatti a "ETSI EN 319 102-1 [1]".

— [2] ETSI TS 119 612 (V2.3.1) "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

— [13] ETSI TS 119 101 V1.1.1 (2016-03) "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

2) 4.2 Vincoli di convalida e procedure di convalida, requisito REQ-4.2-03, sezione "X.509 vincoli di convalida", lettera c):

— i) se un certificato dell'entità finale rappresenta un'ancora di fiducia, non sono utilizzati i RevocationCheckingConstraints;

— ii) se un certificato dell'entità finale non rappresenta un'ancora di fiducia, i RevocationCheckingConstraints sono impostati su "eitherCheck" come definito nella norma ETSI TS 119 172-1 [3], punto A.4.2.1, tabella A.2, righe m)2.1;

— iii) se un certificato dell'entità finale rappresenta un'ancora di fiducia, non sono utilizzati i RevocationFreshnessConstraints definiti nella norma ETSI TS 119 172-1 [3], punto A.4.2.1, tabella A.2, righe m)2.2;

— iv) se un certificato dell'entità finale non rappresenta un'ancora di fiducia, i RevocationFreshnessConstraints definiti nella norma ETSI TS 119 172-1 [3], punto A.4.2.1, tabella A.2, righe m)2.2, sono utilizzati con un valore massimo di 0 per il certificato di firma, garantendo che le informazioni sulla revoca siano accettate solo se sono state rilasciate dopo il *best signature time*. Per i certificati diversi dal certificato di firma, compresi i certificati attestanti validazioni temporali, non sono fissati valori per i RevocationFreshnessConstraints.

3) 4.3 Requisiti in materia di convalida della firma e pratiche di verifica delle norme di applicabilità

— REQ-4.3-02 Le applicazioni di convalida della firma sono conformi alla norma ETSI TS 119 101 [13].

4) 4.4 Processo di verifica dell'applicabilità tecnica (norme)

— REQ-4.4.2-03 Se uno dei controlli specificati nel requisito REQ-4.4.2-01 non dà esito positivo, allora:

— il processo si interrompe;

— la firma è definita tecnicamente come indeterminata, ossia né come una firma elettronica qualificata dell'UE né come un sigillo elettronico qualificato dell'UE;

— l'esito di cui sopra e gli esiti di tutti i processi intermedi sono riportati nella relazione di verifica delle norme di applicabilità della firma.