2025/1942

30.9.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1942 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 convalida qualificati delle firme elettroniche qualificate e i servizi di convalida qualificati 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 33, paragrafo 2, e l'articolo 40,

considerando quanto segue:

(1) I servizi di convalida qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati garantiscono l'integrità, l'autenticità e la correttezza del processo e dei risultati della convalida rispettivamente di firme elettroniche qualificate e di sigilli elettronici qualificati. Tali servizi fiduciari qualificati svolgono un ruolo cruciale nell'ambiente imprenditoriale digitale, promuovendo la transizione dai processi cartacei tradizionali ai loro equivalenti elettronici.

(2) La presunzione di conformità di cui all'articolo 33, paragrafo 2, e all'articolo 40 del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi di convalida qualificati delle firme elettroniche qualificate e dei sigilli elettronici qualificati sono conformi alle norme tecniche 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 la qualifica e la validità tecnica delle firme elettroniche qualificate e dei sigilli elettronici qualificati.

(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 33, 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 per i servizi di convalida qualificati delle firme elettroniche qualificate e i servizi di convalida qualificati dei sigilli elettronici qualificati

Le norme ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») ed ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4») si applicano con gli adeguamenti seguenti.

1. Per ETSI TS 119 441

1) 2.1 Riferimenti normativi

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

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

— [4] ISO/IEC 15408-1:2022 – «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».

— [5] vuoto.

— [6] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules».

— [7] Regolamento di esecuzione (UE) 2024/482 della Commissione ([3]), 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).

— [8] 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».

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) «Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report».

— [10] 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) ([4]).

— [11] Regolamento di esecuzione (UE) 2024/3144 della Commissione, che modifica il regolamento di esecuzione (UE) 2024/4822 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione ([5]).

— [12] ETSI EN 319 411-1 «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements»

([1]) ETSI TS 119 441 - «Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services», V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 - «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists», V1.1.1 (2021-05).
([3]) GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) GU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Riferimenti informativi

— [i.11] vuoto.

3) 3.3 Abbreviazioni

— EUCC Sistema europeo di certificazione della cibersicurezza basato sui criteri comuni

4) 4.3.3 Processo

— NOTA 10 Cfr. ETSI EN 319 102-1 [3] per orientamenti ed ETSI TS 119 172-4 [8] per ulteriori orientamenti per la firma o il sigillo qualificati dell'UE.

5) 6.1 Dichiarazione sulla pratica del servizio di convalida della firma

— OVR-6.1-02 La dichiarazione sulla pratica dell'SVS è strutturata come nell'allegato A.

— OVR-6.1-03 La dichiarazione sulla pratica dell'SVS elenca le politiche di SVS supportate (ad esempio attraverso OID) o vi fa riferimento, descrivendole brevemente.

6) 6.3 Politica di sicurezza delle informazioni

— OVR-6.3-02 La politica di sicurezza documenta i controlli di sicurezza e di tutela della vita privata effettuati per proteggere i dati personali.

7) 7.2 Risorse umane

— OVR-7.2-02 Il personale dell'SVSP in ruoli di fiducia e, se del caso, i subcontraenti dell'SVSP 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.

8) 7.5 Controlli crittografici

— OVR-7.5-02 [CONDIZIONALE] Quando le relazioni di convalida sono firmate, il certificato di firma pubblica dell'SVSP corrispondente alla chiave di firma privata dell'SVSP è rilasciato da una CA affidabile, conformemente alla politica di certificazione NCP+ come specificato nella norma ETSI EN 319 411-1 [12]. Il certificato dovrebbe essere rilasciato conformemente a una politica di certificazione appropriata specificata nella norma ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDIZIONALE] Quando le relazioni di convalida sono firmate, la chiave di firma privata dell'SVSP 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 [4] 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 [7][11], e certificato a livello EAL 4 o superiore; o

(c) fino al 31.12.2030, FIPS PUB 140-3 [6] 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 [7][11], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— OVR-7.5-04 vuoto.

— OVR-7.5-06 La chiave di firma privata di un SVSP 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.

9) 7.7 Sicurezza operativa

— OVR-7.7-02 Per garantire che i sistemi su cui è sviluppata l'applicazione applichino misure di sicurezza adeguate e si adattino a specifici ambienti di applicazione, la SVA utilizza un ambiente di applicazione mantenuto con correzioni di sicurezza aggiornate.

— OVR-7.7-03 I requisiti seguenti specificati nella norma ETSI TS 119 101 [1], punto 5.2, si applicano alla SVA: GSM 1.3.

10) 7.8 Sicurezza della rete

— OVR-7.8-02 Se è consentito l'accesso remoto a sistemi di archiviazione o trattamento di dati riservati, è adottata e descritta una politica formale come parte degli elementi richiesti da OVR-6.3-02.

— OVR-7.8-04 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-7.8-05 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-7.8-06 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento dell'SVSP.

11) 7.12 Cessazione del servizio di convalida della firma e piani di cessazione

— OVR-7.12-02 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.1].

12) 7.14 Catena di approvvigionamento

— OVR-7.14-01 Si applicano i requisiti specificati nella norma ETSI EN 319 401 [2], punto 7.14.

13) 8.1 Processo di convalida della firma

— VPR-8.1-07 La domanda di convalida (SVA) è conforme ai requisiti indicati nella norma ETSI TS 119 101 [1], punto 7.4, da SIA 1 a SIA 4.

— VPR-8.1-11 [CONDIZIONALE] Quando l'SVS intende convalidare firme elettroniche qualificate o sigilli elettronici qualificati conformemente all'articolo 32, paragrafo 1 (o rispettivamente all'articolo 40) del regolamento (UE) n. 910/2014 [i.1], il processo di convalida segue i requisiti della norma ETSI TS 119 172-4 [8].

14) 8.2 Protocollo di convalida della firma

— SVP-8.2-03 La risposta di convalida della firma reca l'OID della politica di SVS.

15) 8.4 Relazione di convalida della firma

— SVR-8.4-02 La relazione di convalida è conforme alla norma ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDIZIONALE] Quando una politica di convalida della firma non è elaborata completamente dall'SVS, la relazione, oltre a riferire sui vincoli convalidati, riporta i vincoli che sono stati ignorati o annullati.

— SVR-8.4-15 La relazione di convalida indica chiaramente l'origine di ciascun PoE (dalla firma, dal client, dal server).

— SVR-8.4-16 La relazione di convalida reca una firma della relazione di convalida, corrispondente alla firma digitale dell'SVSP.

— SVR-8.4-17 [CONDIZIONALE] Quando le relazioni di convalida sono firmate, il formato e l'obiettivo della firma sono conformi alla norma ETSI TS 119 102-2 [9].

16) 9 Quadro per la definizione di politiche dei servizi di convalida basate su una politica in materia di servizi fiduciari definita nel presente documento:

— OVR-9-05 [CONDIZIONALE] Quando una politica di SVS è basata su una politica in materia di servizi fiduciari definita nel presente documento, è effettuata una valutazione dei rischi per valutare i requisiti commerciali e determinare i requisiti di sicurezza da includere nella politica per la comunità e l'applicabilità dichiarate.

— OVR-9-06 [CONDIZIONALE] Quando una politica SVS è basata su una politica in materia di servizi fiduciari definita nel presente documento, tale politica è approvata e modificata conformemente a un processo di revisione definito, che comprende le responsabilità per il mantenimento della politica.

— OVR-9-07 [CONDIZIONALE] Quando una politica di SVS è basata su una politica in materia di servizi fiduciari definita nel presente documento, esiste un processo di revisione definito per garantire che la politica sia supportata dalle dichiarazioni sulle pratiche.

— OVR-9-08 [CONDIZIONALE] Quando una politica di SVS è basata su una politica in materia di servizi fiduciari definita nel presente documento, il TSP mette a disposizione della propria comunità di utenti le politiche supportate.

— OVR-9-09 [CONDIZIONALE] Quando una politica di SVS è basata su una politica in materia di servizi fiduciari definita nel presente documento, le revisioni delle politiche supportate dal TSP sono messe a disposizione degli abbonati.

17) Allegato B (normativo) Servizio di convalida qualificato delle firme elettroniche qualificate quale definito all'articolo 33 del regolamento (UE) n. 910/2014

— VPR-B-02 [CONDIZIONALE] Se l'SVSP è un QSVSP l'attuazione è conforme alla norma ETSI TS 119 172-4 [8].

— NOTA 2 vuota.

— OVR-B-04 [CONDIZIONALE] Se l'SVSP è un QSVSP, le prove nel requisito OVR-B-03 verificano diversi casi d'uso, positivi e negativi.

— VPR-B-11 [CONDIZIONALE] Se l'SVSP è un QSVSP, l'SVSP controlla il calcolo hash (eseguendo il calcolo sul lato server o controllando il client se è consentito dal lato client).

— NOTA 5 vuota.

— NOTA 6 vuota.

— VPR-B-15 [CONDIZIONALE] Se l'SVSP è un QSVSP, al fine di soddisfare i requisiti da VPR-B-13 a VPR-B-14 la relazione di convalida è conforme alla norma ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDIZIONALE] Se l'SVSP è un QSVSP, l'attuazione è conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dell'ENISA [10] per l'uso di tecniche crittografiche adeguate nella fornitura di servizi di convalida qualificati di firme elettroniche qualificate.

18) Allegato C (informativo) Mappatura dei requisiti del regolamento (UE) n. 910/2014, «Convalida conformemente all'articolo 32, paragrafo 1», secondo comma:

— per garantire la verifica di tutte le condizioni prescritte all'articolo 32, paragrafo 1, e all'articolo 40 del regolamento (UE) n. 910/2014 [i.1], è necessario un algoritmo di convalida corretto. Esso fornisce lo stesso risultato deterministico per una firma o un sigillo sottoposti a convalida. La politica di convalida delle firme è fondamentale a tale scopo. La norma ETSI TS 119 172-4 [8], basata sull'algoritmo di convalida specificato nella norma ETSI EN 319 102-1 [3], è stata pubblicata in tale prospettiva.

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 (2024-11) «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 24 ore per il certificato di firma. Per i certificati diversi dal certificato di firma, compresi i certificati attestanti validazioni temporali, non sono fissati valori per i RevocationFreshnessConstraints.

3) 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:

(a) il processo si interrompe;

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

(c) 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.