2025/1944

30.9.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1944 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 le norme di riferimento applicabili ai processi di invio e ricezione dei dati nei servizi elettronici di recapito certificato qualificati e l'interoperabilità di tali servizi

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 44, paragrafi 2 e 2 ter,

considerando quanto segue:

(1) I servizi elettronici di recapito certificato qualificati forniscono un canale sicuro per la trasmissione di documenti, comprese prove dell'avvenuto invio e dell'avvenuta ricezione dei dati. Essi sono intesi a fornire certezza nell'identificazione del destinatario e a garantire un elevato livello di sicurezza nell'identificazione del mittente.

(2) La presunzione di conformità di cui all'articolo 44, paragrafo 1 bis, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi fiduciari qualificati per la fornitura di servizi elettronici di recapito certificato 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.

(3) Se un prestatore di servizi fiduciari rispetta i requisiti di cui all'allegato I 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) A norma dell'articolo 44, paragrafo 2 bis, del regolamento (UE) n. 910/2014, qualora concordino l'interoperabilità dei loro servizi, è importante che i prestatori di servizi fiduciari qualificati rispettino norme e specifiche appropriate di cui all'allegato II del presente regolamento di esecuzione al fine di trasferire facilmente i dati elettronici certificati tra due o più prestatori di servizi fiduciari qualificati e di promuovere pratiche eque nel mercato interno.

(5) 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).

(6) 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 a tutte le attività di trattamento di dati personali a norma del presente regolamento.

(7) 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.

(8) 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 per i servizi elettronici di recapito certificato qualificati

Le norme di riferimento e le specifiche di cui all'articolo 44, paragrafo 2, del regolamento (UE) n. 910/2014 figurano nell'allegato I del presente regolamento.

Articolo 2

Norme di riferimento e specifiche per l'interoperabilità dei servizi elettronici di recapito certificato qualificati

Le norme di riferimento e le specifiche di cui all'articolo 44, paragrafo 2 ter, del regolamento (UE) n. 910/2014 figurano nell'allegato II del presente regolamento.

Articolo 3

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 I

Elenco delle norme di riferimento e delle specifiche di cui all'articolo 1

La norma ETSI EN 319 521 V1.1.1 (2019-02) («ETSI EN 319 521») si applica con gli adeguamenti seguenti.

1. Per ETSI EN 319 521

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 EN 319 411-1 V1.5.1 (2025-04) «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements».

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) «Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture».

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) «Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content».

— [5] 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) ([1]).

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

— [7] Regolamento di esecuzione (UE) 2024/482 ([2]) della Commissione, 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) ([3]).

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

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

2) 3.1 Termini

— sigillo elettronico avanzato: quale definito nel regolamento (UE) n. 910/2014 [i.1];

— firma elettronica avanzata: quale definita nel regolamento (UE) n. 910/2014 [i.1];

— sigillo elettronico qualificato: quale definito nel regolamento (UE) n. 910/2014 [i.1];

— firma elettronica qualificata: quale definita nel regolamento (UE) n. 910/2014 [i.1].

— 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.

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

3) 5.1.1 Disposizioni comuni

— REQ-ERDS-5.1.1-01 L'ERDS assicura che la disponibilità, l'integrità e la riservatezza dei contenuti degli utenti siano adeguatamente garantite mentre sono gestite dall'ERDS, selezionando tecniche crittografiche adeguate per l'integrità e la riservatezza conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dell'ENISA [5].

4) 5.2.1.1 Aspetti generali

— REQ-QERDS-5.2.1.1-01 Il QERDSP verifica con un livello di sicurezza molto elevato l'identità del destinatario, direttamente o facendo affidamento su una terza parte e utilizzando uno dei mezzi seguenti o di una combinazione degli stessi, ove necessario:

(a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale;

(b) a distanza, mediante un mezzo di identificazione elettronica che rispetta i requisiti di cui all'articolo 8 del regolamento (UE) n. 910/2014 [i.1] per quanto riguarda il livello di garanzia «elevato», o mediante il portafoglio europeo di identità digitale;

(c) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato;

(d) utilizzando altri metodi di identificazione che garantiscano che la persona fisica o il rappresentante autorizzato della persona giuridica possano essere identificati con un livello di sicurezza molto elevato. La garanzia che tale identificazione sia effettuata con un livello di sicurezza molto elevato è confermata da un organismo di valutazione della conformità.

— REQ-QERDS-5.2.1.1-01A Il QERDSP verifica l'identità del mittente con mezzi adeguati, direttamente o facendo affidamento su una terza parte, sulla base di uno dei metodi seguenti o di una combinazione degli stessi, ove necessario:

(a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale;

(b) a distanza, mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 del regolamento (UE) n. 910/2014 [i.1] per quanto riguarda il livello di garanzia «significativo», a condizione che sia stato rilasciato sulla base della precedente presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica;

(c) mediante un certificato di firma elettronica avanzata o di sigillo elettronico avanzato, a condizione che il certificato sia stato rilasciato alla persona fisica o a un rappresentante autorizzato della persona giuridica in base alla «Normalised Certificate Policy» (NCP) quale definita nella norma ETSI EN 319 411-1 [2]; o

(d) utilizzando altri metodi di identificazione che garantiscano che la persona fisica o il rappresentante autorizzato della persona giuridica possano essere identificati con un livello di sicurezza molto elevato. La garanzia che tale identificazione sia effettuata con un livello di sicurezza elevato è confermata da un organismo di valutazione della conformità.

— NOTA La terza parte che verifica l'identità del mittente e del destinatario può essere un altro QERDSP se il mittente e il destinatario sono abbonati a QERDSP diversi.

5) 5.2.1.2 Identificazione del destinatario e trasferimento dei contenuti dell'utente

— REQ-QERDS-5.2.1.2-03 Se l'identificazione del destinatario si basa su un processo interno QERDS, il QERDSP conduce l'intero processo in un ambiente sicuro e controllato.

6) 5.2.2 Disposizioni per l'autenticazione UE del QERDS

— REQ-QERDS-5.2.2-03 [CONDIZIONALE] Il QERDSP vincola all'identità di un mittente verificata conformemente al punto 5.2.1 uno dei mezzi di autenticazione seguenti:

(a) meccanismi di autenticazione a due fattori;

(b) portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 del regolamento (UE) n. 910/2014 [i.1] per quanto riguarda il livello di garanzia «elevato» o «significativo»;

(c) un'autenticazione TLS reciproca, che comprende il certificato rilasciato al mittente in base alla NCP quale definita nella norma ETSI EN 319 411-1 [2];

(d) una firma digitale supportata da un certificato rilasciato in base alla NCP quale definita nella norma ETSI EN 319 411-1 [2];

(e) altri mezzi che garantiscono l'autenticazione del mittente identificato. La conformità del vincolo è confermata da un organismo di valutazione della conformità. Esempio: può essere compreso l'utilizzo di uno dei mezzi di cui alle lettere a), b) e d) di cui sopra, per registrare un certificato client Transport Layer Security (TLS) per l'invio automatizzato tramite TLS reciproco o per registrare un certificato di sigillo digitale utilizzato per sigillare le asserzioni di autenticazione con l'ERDS. Possono essere applicati anche altri meccanismi in cui i mittenti identificati si avvalgono di servizi di terzi delegati.

— REQ-QERDS-5.2.2-03A [CONDIZIONALE] Il QERDSP vincola all'identità di un destinatario verificata conformemente al punto 5.2.1 uno dei mezzi di autenticazione seguenti, a condizione che i mezzi, o qualsiasi combinazione degli stessi, garantiscano un livello di sicurezza molto elevato riguardo all'identità del destinatario autenticato:

(a) un meccanismo di autenticazione a più fattori;

(b) il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 del regolamento (UE) n. 910/2014 [i.1] riguardo al livello di garanzia «elevato» o «significativo»;

(c) un certificato di firma elettronica qualificata o di sigillo elettronico qualificato;

(d) altri mezzi che garantiscono l'autenticazione del destinatario identificato. La conformità del vincolo è confermata da un organismo di valutazione della conformità. Esempio: può essere compreso l'utilizzo di uno dei mezzi di cui alle lettere da a) a c) di cui sopra, per registrare un certificato client Transport Layer Security (TLS) per l'invio automatizzato tramite TLS reciproco o per registrare un certificato di sigillo digitale utilizzato per sigillare le asserzioni di autenticazione con l'ERDS. Possono essere applicati anche altri meccanismi in cui i mittenti identificati si avvalgono di servizi di terzi delegati.

— REQ-QERDS-5.2.2-04 [CONDIZIONALE] Se il mittente si collega al QERDS su una connessione sicura che richiede un'autenticazione reciproca da macchina a macchina tra la macchina del mittente e il server del QERDS sulla base di certificati rilasciati conformemente alla NCP definita nella norma ETSI EN 319 411-1 [2], una volta stabilita tale connessione sicura, per una seconda fase di autenticazione del mittente possono essere adottati meccanismi di autenticazione a fattore unico se le procedure organizzative e le misure di sicurezza in essere garantiscono la sicurezza nell'autenticazione del mittente.

7) 5.4.1 Disposizioni comuni

— REQ-ERDS-5.4.1-06 L'ERDS genera e mette a disposizione delle legittime parti interessate prove ERDS relative a eventi ERD quali definiti al punto 6 della norma ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 L'ERDSP archivia le prove e/o sintesi delle prove per ciascuna prova rilasciata.

— REQ-ERDS-5.4.1-08 Le prove ERDS generate dall'ERDS sono conformi alla semantica delle prove definita al punto 8 della norma ETSI EN 319 522-2 [4].

8) 7.2.1 Disposizioni comuni

— REQ-ERDS-7.2.1-02 Il personale dell'ERDSP in ruoli di fiducia è 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.

— REQ-ERDS-7.2.1-03 La conformità al requisito REQ-ERDS-7.2.1-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza.

9) 7.3.2 Gestione dei media

— REQ-ERDS-7.3.1-02 Si applicano tutti i requisiti della norma ETSI EN 319 401 [1], punto 7.3.3.

10) 7.5 Controlli crittografici

— REQ-ERDS-7.5-01A L'ERDS seleziona e utilizza tecniche crittografiche idonee, conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dell'ENISA [5].

— REQ-ERDSP-7.5-03 La chiave privata di firma dell'ERDS 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 [6] o in «Common Criteria for Information Technology Security Evaluation», versione CC:2002, 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) sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) [7][8], e certificato a livello EAL 4 o superiore; o

(c) fino al 31.12.2030, FIPS PUB 140-3 [9] 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][8], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

11) 7.8 Sicurezza della rete

— REQ-ERDSP-7.8-04 L'ERDSP utilizza protocolli e algoritmi all'avanguardia per la cifratura al livello Transport Layer conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dell'ENISA [5].

— REQ-ERDSP-7.8-06 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.

— REQ-ERDSP-7.8-07 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.

— REQ-ERDSP-7.8-08 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento del TSP.

12) 7.12 Piani di cessazione dell'ERDSP e dell'ERDS

— REQ-ERDS-7.12-03 Il piano di cessazione dell'ERDSP 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].

13) 7.14 Catena di approvvigionamento

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

ALLEGATO II

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

Si applicano le norme 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») ed ETSI EN 319 522-4-3 V1.1.1 (2018-09) («ETSI EN 319 522-4-3»).