2025/2531

17.12.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2531 DELLA COMMISSIONE

del 16 dicembre 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme di riferimento e le specifiche applicabili ai registri 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 45 *terdecies*, paragrafo 3,

considerando quanto segue:

(1) Con il regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([2]) è stato introdotto nel regolamento (UE) n. 910/2014 un elenco di nuovi servizi fiduciari e servizi fiduciari qualificati, tra cui la registrazione di dati elettronici in un registro elettronico qualificato. La Commissione deve redigere un elenco di norme di riferimento e, se necessario, stabilire specifiche per tali servizi.

(2) Un registro elettronico è una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni di dati e l'accuratezza dell'ordine cronologico di tali registrazioni. Per garantire che la registrazione dei dati in un registro elettronico qualificato sia ordinata cronologicamente, coerente e affidabile, è necessario stabilire un insieme comune di specifiche per la registrazione dei dati elettronici in un registro elettronico qualificato.

(3) La presunzione di conformità di cui all'articolo 45 *terdecies*, paragrafo 2, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi fiduciari qualificati per la registrazione di dati elettronici in un registro elettronico qualificato 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.

(4) 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.

(5) La Commissione valuta periodicamente le nuove tecnologie, pratiche, norme o specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183, la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, pratiche, norme o specifiche tecniche e per seguire le migliori pratiche nel 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 alle attività di trattamento di dati personali a norma del presente regolamento, tenendo anche conto degli orientamenti 02/2025 del comitato europeo per la protezione dei dati sul trattamento di dati personali attraverso le tecnologie blockchain ([5]).

(7) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 21 ottobre 2025 ([7]).

(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

Le norme di riferimento e le specifiche di cui all'articolo 45 *terdecies*, paragrafo 3, del regolamento (UE) n. 910/2014 figurano, per i registri elettronici qualificati, 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 16 dicembre 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) «EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers».

ALLEGATO

Elenco delle specifiche tecniche e delle norme di riferimento applicabili ai registri elettronici distribuiti qualificati

1. Ai fini del presente regolamento si applicano le definizioni seguenti:

   a) «carattere definitivo»: lo stato di una registrazione di dati di un registro elettronico in cui è diventata irreversibile e non può essere modificata o rimossa;

   b) «registro elettronico distribuito»: un registro elettronico condiviso tra una serie di nodi di registro elettronico distribuito e sincronizzato tra i nodi di registro elettronico distribuito utilizzando un meccanismo di consenso;

   c) «nodo di registro elettronico distribuito»: un dispositivo o un processo che fa parte di una rete di registro elettronico distribuito e conserva una copia completa o parziale delle registrazioni di dati di un registro elettronico;

   d) «rete di registro elettronico distribuito»: una rete di nodi di registro elettronico distribuito che costituisce un sistema di registro elettronico distribuito;

   e) «sistema di registro elettronico distribuito»: un sistema che implementa un registro elettronico distribuito;

   f) «consenso»: un accordo tra nodi di registro elettronico distribuito sulla validità delle transazioni e sul mantenimento di un insieme coerente e ordinato di transazioni convalidate in tutto il sistema di registro elettronico distribuito;

   g) «meccanismo di consenso»: l'insieme di norme e procedure mediante le quali è raggiunto il consenso;

   h) «norme di disciplina»: l'insieme di protocolli, politiche e meccanismi che stabilisce le modalità di funzionamento del sistema di registro elettronico distribuito, di convalida dei dati e di aggiunta degli stessi a un registro elettronico nonché di interazione dei partecipanti;

   i) «transazione»: l'unità più piccola di un processo di lavoro all'interno di un registro elettronico;

   j) «processo di lavoro»: una o più sequenze di azioni necessarie per produrre un risultato conforme alle norme di disciplina di un registro elettronico;

   k) «transazione convalidata»: una transazione per cui l'integrità, l'autenticità e le condizioni specifiche per il protocollo richieste sono state verificate secondo le norme di disciplina del sistema di registro elettronico distribuito;

   l) «collegamento crittografico»: un riferimento a dati stabilito utilizzando tecniche crittografiche idonee a garantire l'integrità, l'autenticità o la tracciabilità dei dati referenziati e la corretta sequenza delle registrazioni di dati;

   m) «relazione sul registro»: una presentazione strutturata di informazioni verificabili estratte dalle registrazioni di dati di un registro elettronico, che fornisce anche indicazioni su specifiche attività, stati o conformità a norme predefinite;

   n) «fornitore di registri elettronici qualificati»: un prestatore di servizi fiduciari qualificato che presta un servizio fiduciario qualificato consistente nella registrazione di dati in un registro elettronico qualificato;

   o) «registro elettronico distribuito qualificato»: un registro elettronico distribuito che soddisfa i requisiti di un registro elettronico qualificato.

2. Qualora il prestatore di servizi fiduciari qualificato debba elaborare una relazione sul registro, questa è prodotta in modo automatizzato.

3. I fornitori di registri elettronici qualificati creano, aggiornano e mantengono un registro elettronico qualificato e vi registrano dati elettronici conformemente alle specifiche stabilite in:

   a) per tutti i fornitori di registri elettronici qualificati, ETSI EN 319 401 v3.1.1 (2024-06) con i seguenti adattamenti:

      — 2.1 riferimenti normativi

        [1] gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati), pubblicati dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

[2] IETF RFC 7515 (maggio 2015): «JSON Web Signature (JWS)».

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

[4] Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, 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).

[5] Regolamento di esecuzione (UE) 2024/3144 della Commissione, del 18 dicembre 2024, che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione.

[6] ISO/IEC 15408:2022 (parti da 1 a 5): «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security»;

— 6.1 dichiarazione sulla pratica del servizio fiduciario:

  — REQ-6.1-12 La dichiarazione sulla pratica del registro elettronico comprende almeno le seguenti informazioni:

    — le capacità funzionali e tecniche della piattaforma del registro elettronico e il suo utilizzo durante l'intera prestazione della registrazione di dati in un registro elettronico qualificato come servizio fiduciario qualificato;

    — i meccanismi specifici di autenticazione dell'origine dei dati utilizzati durante la prestazione del servizio;

    — i meccanismi specifici di ordinamento cronologico sequenziale dei dati utilizzati durante la prestazione del servizio;

    — se del caso, il collegamento crittografico utilizzato per garantire la sequenza delle registrazioni di dati;

    — se del caso, il meccanismo di consenso che garantisce il carattere definitivo e l'integrità delle registrazioni di dati e delle transazioni conservate nel registro, compreso qualsiasi margine temporale supplementare fino al raggiungimento del carattere definitivo e dell'integrità;

    — i meccanismi specifici di integrità dei dati utilizzati per prestare il servizio;

  — 6.2 termini e condizioni:

    — REQ-6.2-03 Prima di avviare una relazione contrattuale gli abbonati e le parti facenti affidamento sul servizio fiduciario sono informati in modo chiaro, completo e facilmente accessibile, in uno spazio accessibile al pubblico e individualmente, di termini e condizioni precisi, compresi gli elementi sopraelencati;

  — 6.3 politica di sicurezza delle informazioni:

    — REQ-6.3-04X Il prestatore di servizi fiduciari stabilisce procedure per notificare all'organismo di vigilanza eventuali modifiche nella prestazione del servizio fiduciario, conformemente ai requisiti commerciali e alle disposizioni legislative e regolamentari pertinenti. Il prestatore di servizi fiduciari effettua la notifica all'organismo di vigilanza almeno:

      — un mese prima dell'attuazione di qualsiasi modifica;

      — tre mesi prima della cessazione prevista di una prestazione di servizi fiduciari;

  — 7.2 risorse umane:

    — REQ-7.2-04X Il personale del prestatore di servizi fiduciari 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-7.2-05X Sono compresi aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza;

— 7.5 controlli crittografici:

— REQ-7.5-01X Sono predisposti adeguati controlli di sicurezza per la gestione di qualsiasi chiave crittografica, algoritmo crittografico e dispositivo crittografico durante tutto il loro ciclo di vita, seguendo, se del caso, un approccio di agilità crittografica.

— REQ-7.5-02 Per prestare i suoi servizi fiduciari, il prestatore di servizi fiduciari seleziona e utilizza tecniche crittografiche adeguate conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1].

In particolare:

— REQ-7.5-03 I fornitori di registri elettronici qualificati stabiliscono l'origine delle registrazioni di dati nel registro elettronico. A tal fine utilizzano firme elettroniche avanzate basate su certificati qualificati o sigilli elettronici avanzati basati su certificati qualificati creati dagli utenti del servizio conformemente alle norme e specifiche seguenti:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). «Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures».

b) ETSI EN 319 132-1 V1.3.1 (2024-07). «Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures».

c) ETSI TS 119 182-1 V1.2.1 (2024-07). «Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures», con il seguente adattamento:

— 5.1.8 parametro di intestazione x5c (catena di certificati X.509)

— Il parametro di intestazione x5c definito al punto 4.1.6 dell'IETF RFC 7515 [2] deve essere presente nella firma JAdES come parametro di intestazione firmato o non firmato.

— Il parametro di intestazione x5c deve avere la semantica specificata al punto 4.1.6 dell'IETF RFC 7515 [2].

— Il parametro di intestazione x5c deve avere la sintassi specificata al punto 4.1.6 dell'IETF RFC 7515 [2].

— REQ-7.5-04 I fornitori di registri elettronici qualificati garantiscono l'ordine cronologico sequenziale univoco delle registrazioni di dati nel registro elettronico. A tal fine utilizzano collegamenti crittografici, basati su elenchi di hash o alberi di hash, utilizzando funzioni crittografiche di hash, conformemente alle specifiche e alle norme seguenti:

a) dimensione dell'output di SHA-256 o superiore, conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1].

b) dimensione dell'output di SHA3-256 o superiore, conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1].

In alternativa, quando utilizzano la registrazione temporale per garantire l'ordine cronologico sequenziale univoco delle registrazioni di dati nel registro elettronico, i fornitori di registri elettronici qualificati utilizzano marcature temporali qualificate.

— REQ-7.5-05 I fornitori di registri elettronici qualificati garantiscono l'integrità delle registrazioni di dati nel registro elettronico qualificato. A tal fine utilizzano firme elettroniche avanzate basate su certificati qualificati o sigilli elettronici avanzati basati su certificati qualificati, conformemente alle norme e specifiche seguenti:

a) qualsiasi formato di firma o sigillo conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1];

b) dimensione dell'output di SHA-256 o superiore, conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1];

c) dimensione dell'output di SHA3-256 o superiore, conformemente ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [1].

d) I fornitori di registri elettronici qualificati garantiscono l'identificazione immediata di ogni successiva modifica dei dati registrati in un registro elettronico qualificato.

— REQ-7.5-06 Qualora siano utilizzati meccanismi di firma digitale, le chiavi di firma private del fornitore di registri elettronici qualificati sono detenute e utilizzate 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 ([1]) [6] 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 certificati a livello EAL 4 o superiore; oppure

b) sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) ([2]) ([3]) [4][5], e certificato a livello EAL 4 o superiore; oppure

c) fino al 31.12.2030, FIPS PUB 140-3 ([4]) [3] 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 [4][5], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

([1]) ISO/IEC 15408:2022 (parti da 1 a 5): «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».
([2]) Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, 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) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).
([3]) Regolamento di esecuzione (UE) 2024/3144 della Commissione, del 18 dicembre 2024, che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione (GU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).
([4]) FIPS PUB 140-3 (2019): «Security Requirements for Cryptographic Modules».

— 7.8 sicurezza della rete:

— REQ-7.8-14X La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 è eseguita almeno una volta a trimestre.

— REQ-7.8-18X Il test di penetrazione richiesto dal requisito REQ-7.8-17X è eseguito almeno una volta all'anno.

— REQ-7.8-21X Anche i firewall devono essere configurati in modo da bloccare tutti i protocolli e gli accessi non necessari per il funzionamento del prestatore di servizi fiduciari;

— 7.9.1 monitoraggio e tenuta di registro:

— REQ-7.9.1-02X Le attività di monitoraggio tengono conto della sensibilità delle informazioni raccolte o analizzate;

— 7.12 cessazione e piani di cessazione del prestatore di servizi fiduciari:

— REQ-7.12-02 A Il piano di cessazione del prestatore di servizi fiduciari 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].

b) Inoltre, per tutti i fornitori di registri elettronici qualificati che utilizzano tecnologie di registro elettronico distribuito:

(1) ISO 23257:2022 «Blockchain and distributed ledger technologies – Reference architecture», punto 9, che fornisce una descrizione completa del sistema basato sulla tecnologia di registro elettronico distribuito, della corrispondente rete basata su tecnologia di registro elettronico distribuito e dei nodi basati su tecnologia di registro elettronico distribuito;

(2) ISO/TS 23635:2022. «Blockchain and distributed ledger technologies – Guidelines for governance», per quanto riguarda le politiche e le pratiche scritte e accessibili al pubblico relative alla struttura di governance per il servizio di registro elettronico prestato.