2025/1567

30.7.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1567 DELLA COMMISSIONE

del 29 luglio 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e dispositivi qualificati per la creazione di un sigillo elettronico a distanza come servizi fiduciari 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 29 bis, paragrafo 2, e l'articolo 39 bis,

considerando quanto segue:

(1) I servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza svolgono un ruolo cruciale nell'ambiente imprenditoriale digitale, promuovendo la transizione dai processi tradizionali su supporto cartaceo agli equivalenti elettronici. Tali servizi fiduciari qualificati contribuiscono a una gestione sicura e affidabile di tali dispositivi a distanza per conto dei firmatari e dei creatori dei sigilli, in maniera tale da garantire che siano soddisfatte le condizioni per le firme elettroniche qualificate e i sigilli elettronici qualificati.

(2) Al fine di migliorare la certezza del diritto e l'affidabilità dei servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e dei servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza, i prestatori di servizi fiduciari qualificati che forniscono tali servizi qualificati dovrebbero rispettare le norme di cui al presente regolamento.

(3) Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. È opportuno che siano adattate per includere controlli che garantiscano la sicurezza e l'affidabilità dei servizi fiduciari qualificati, oltre a garantire che, rispettivamente, i firmatari abbiano il controllo esclusivo, con un elevato livello di sicurezza, sull'uso dei loro dati per la creazione di una firma elettronica e i creatori del sigillo abbiano il controllo sull'uso dei loro dati per la creazione di un sigillo elettronico.

(4) Al fine di garantire un periodo di tempo adeguato per la verifica dei prestatori di servizi fiduciari per quanto riguarda la conformità ai nuovi requisiti, il presente regolamento dovrebbe applicarsi a decorrere da 24 mesi dalla sua entrata in vigore.

(5) La Commissione valuta periodicamente tecnologie, pratiche, norme o specifiche tecniche nuove. 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, le nuove tecnologie, 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]) dovrebbero applicarsi 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

Le norme di riferimento e le specifiche per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e di dispositivi qualificati per la creazione di un sigillo elettronico a distanza come servizi fiduciari qualificati di cui all'articolo 29 bis, paragrafo 2, e all'articolo 39 bis del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

Articolo 2

Entrata in vigore e applicabilità

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

Il presente regolamento si applica a decorrere dal 19 agosto 2027.

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

Fatto a Bruxelles, il 29 luglio 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 la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e dispositivi qualificati per la creazione di un sigillo elettronico a distanza

La norma ETSI TS 119 431-1 V1.3.1 (2024-12) ("ETSI TS 119 431-1") si applica allo scopo di valutare la conformità al servizio applicativo *EU Server Signing Application Service v2 Policy* (SSASP) conformemente all'allegato A di tale norma, con i seguenti adeguamenti:

1) 2.1 Riferimenti normativi

   — [1] ETSI EN 319 401 V3.1.1 (2024-06): "Firme elettroniche e infrastrutture fiduciarie (ESI); Requisiti di politica generale per i prestatori di servizi fiduciari";

   — [7] 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]).

2) 6.1 Responsabilità delle pubblicazioni e dell'archivio

   — OVR-6.1-04: Le informazioni individuate in OVR-6.1-01 sono disponibili al pubblico e a livello internazionale.

3) 6.4.4 Controlli del personale

   — OVR-6.4.4-02: Il servizio SSASP impiega personale in ruoli di fiducia e, se del caso, subappaltatori in ruoli di fiducia, che possiedono le conoscenze specialistiche, l'esperienza e le qualifiche necessarie sulla base di formazione e credenziali formali o dell'esperienza, o di una loro combinazione.

   — OVR-6.4.4-03: La conformità a OVR-6.4.4-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle pratiche di sicurezza vigenti.

4) 6.4.9 Cessazione del servizio SSASP

   — OVR-6.4.9-02: Il piano di cessazione del servizio SSASP è conforme agli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.1].

5) 6.5.5 Controlli di sicurezza della rete

   — OVR-6.5.5-02: La scansione delle vulnerabilità richiesta da REQ-7.8-13 di ETSI EN 319 401 [1] deve essere eseguita almeno una volta al trimestre.

   — OVR-6.5.5-03: I firewall devono essere configurati in modo da impedire tutti i protocolli e gli accessi non necessari per il funzionamento del TSP.

6) 6.8.5 Controlli crittografici

   — OVR-6.8.5-01: Devono essere posti in essere adeguati controlli di sicurezza per la gestione di tutte le tecniche crittografiche del servizio SSASP durante tutto il loro ciclo di vita.

   — OVR-6.8.5-02: Per quanto riguarda OVR-6.8.5-01, il servizio SSASP seleziona e utilizza tecniche crittografiche adeguate conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza dell'ENISA [7].

7) Allegato A, sezione A.3 Requisiti generali

   — OVR-A.3-02 [EUSPv2]: La dichiarazione sulla prassi del TSP include il riferimento alla certificazione del QSCD impiegato conformemente ai requisiti del regolamento (UE) n. 910/2014 [i.1], allegato II.

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