REGOLAMENTO DI ESECUZIONE (UE) 2026/1735 DELLA COMMISSIONE

del 15 luglio 2026

che modifica il regolamento di esecuzione (UE) 2025/1569 per quanto riguarda le norme e le specifiche applicabili

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 *quinquies*, paragrafo 5, l'articolo 45 *sexies*, paragrafo 2, e l'articolo 45 *septies*, paragrafi 6 e 7,

considerando quanto segue:

(1) Al fine di garantire il massimo livello di armonizzazione tra gli Stati membri per lo sviluppo dei portafogli europei di identità digitale, le specifiche tecniche per i portafogli sono fondate sul lavoro svolto sulla base della raccomandazione (UE) 2021/946 della Commissione ([2]) e, in particolare, sull'architettura e sul quadro di riferimento. Poiché l'architettura e il quadro di riferimento si sono evoluti in modo significativo dall'adozione del regolamento di esecuzione (UE) 2025/1569 della Commissione ([3]), è ora opportuno modificare detto regolamento di esecuzione per allinearlo alle nuove norme e specifiche.

(2) Conformemente agli obiettivi del regolamento (UE) n. 910/2014, sono state selezionate diverse norme per soddisfare i requisiti applicabili al rilascio, alla gestione e alla verifica degli attestati elettronici di attributi. Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Ove necessario, tali norme dovrebbero essere adattate o integrate al fine di garantire un elevato livello di sicurezza e integrità degli attestati elettronici di attributi, agevolando nel contempo l'interoperabilità transfrontaliera e l'efficace funzionamento del mercato interno. In linea con tale obiettivo, il presente regolamento aggiorna i requisiti applicabili al rilascio e alla revoca degli attestati elettronici qualificati di attributi e degli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica, o per suo conto, e introduce i requisiti per l'apposizione di firma e sigillo sui risultati della verifica rispetto a fonti autentiche.

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

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

([2]) Raccomandazione (UE) 2021/946 della Commissione, del 3 giugno 2021, relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale (GU L 210 del 14.6.2021, pag. 51, ELI: http://data.europa.eu/eli/reg/2021/946/oj).

([3]) Regolamento di esecuzione (UE) 2025/1569 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 gli attestati elettronici qualificati di attributi e gli attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto (GU L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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: https//data.europa.eu/eli/reg/2016/679/oj).

([5]) 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).

(4) 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 17 aprile 2026 ([7]).

(5) 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

Modifiche del regolamento di esecuzione (UE) 2025/1569

Il regolamento di esecuzione (UE) 2025/1569 è così modificato:

1) all'articolo 3, il paragrafo 2 è sostituito dal seguente:

«2. Nel caso di rilascio di attestati elettronici di attributi inclusi in regimi registrati nel catalogo di regimi per gli attestati di attributi, i fornitori di attestati elettronici qualificati di attributi e i fornitori di attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto devono conformarsi ai requisiti del regime per gli attestati di attributi corrispondente. Le politiche e le procedure stabilite dagli emittenti di attestati al fine di rispettare i requisiti dei regimi per gli attestati di attributi rientrano nella valutazione della conformità di cui al regolamento (UE) n. 910/2014.»;

2) l'articolo 4 è così modificato:

a) il paragrafo 1 è soppresso;

b) il paragrafo 3 è sostituito dal seguente:

«3. I fornitori di attestati elettronici qualificati di attributi e i fornitori di attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto, qualora tali attestati siano rilasciati con un periodo di validità superiore alle 24 ore, li revocano almeno nelle circostanze seguenti:

a) su richiesta della persona cui è stato rilasciato l'attestato elettronico di attributi o, se del caso, del soggetto cui si riferisce l'attestato;

b) se il fornitore viene a conoscenza del fatto che la sicurezza o l'affidabilità degli attestati elettronici qualificati di attributi o degli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto è stata compromessa;

c) in altre situazioni, come previsto dal diritto dell'Unione o nazionale.»;

c) il paragrafo 4 è sostituito dal seguente:

«4. I fornitori di attestati elettronici qualificati di attributi e i fornitori di attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto istituiscono tecniche di revoca e metodi di gestione che tutelino la vita privata e ostacolino la correlabilità e la tracciabilità. Le tecniche di revoca devono essere conformi ai requisiti di cui all'allegato II.»;

([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: https//data.europa.eu/eli/reg/2018/1725/oj).

([7]) «EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties» | Garante europeo della protezione dei dati.

3) l'articolo 9 è così modificato:

   a) dopo il paragrafo 2 è inserito il seguente paragrafo 2 *bis*:

   «2 *bis*.Il meccanismo di verifica deve essere conforme alle specifiche di cui all'allegato IV.»;

   b) il paragrafo 4 è sostituito dal seguente:

   «4. Il risultato della verifica indica se l'attributo è stato verificato o no e specifica l'organismo del settore pubblico responsabile della fonte autentica o, se del caso, l'organismo del settore pubblico designato per agire per conto della fonte autentica rispetto alla quale è stato verificato l'attributo.

   Il risultato della verifica è firmato o sigillato dall'organismo del settore pubblico responsabile di una fonte autentica, o dall'intermediario designato riconosciuto a livello nazionale, utilizzando almeno una firma elettronica avanzata basata rispettivamente su un certificato qualificato di firme elettroniche o su un sigillo elettronico avanzato basato su un certificato qualificato di sigilli elettronici.».

4) L'allegato I è sostituito dal testo che figura nell'allegato I del presente regolamento.

5) L'allegato II è sostituito dal testo che figura nell'allegato II del presente regolamento.

6) Il testo che figura nell'allegato III del presente regolamento è aggiunto come allegato IV.

Articolo 2

Entrata in vigore

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

L'articolo 1, paragrafo 3, si applica a decorrere dal 1º gennaio 2027.

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

Fatto a Bruxelles, il 15 luglio 2026

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

«*ALLEGATO I*

Elenco delle norme di riferimento e delle specifiche di cui all'articolo 3

La norma ETSI TS 119 471 V1.1.1 (2025-05) si applica con i seguenti adattamenti:

1) 2.1 Riferimenti normativi

[1] ETSI EN 319 401 V3.2.1 (2026-01): "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers";

[2] 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] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules";

[4] Regolamento di esecuzione (UE) 2024/482 della Commissione ([1])

[5] Regolamento di esecuzione (UE) 2024/3144 della Commissione ([2])

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

2) 3.1 Termini

È aggiunto il termine seguente:

— 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) 4. Servizi fiduciari EAA

— Non si applica il punto 4.2.2.2 "Verification of attributes against authentic sources".

— REQ-EAASP-4.2.2.3-02: l'EAASP si autentica nei confronti dell'istanza EUDIW implementando meccanismi di autenticazione reciproca che utilizzano un certificato di accesso valido.

— REQ-EAASP-4.2.2.3-03: l'EAASP convalida l'unità EUDIW e *l'eventuale revoca dell'istanza EUDIW*.

— *Non si applica* il punto *4.3.2* "*EUDIW Specific*".

4) 6.1 Dichiarazione sulla prassi dell'EAAS

— REQ-EAASP-6.1-02: l'EAASP illustra il meccanismo di revoca nella dichiarazione sulla prassi dell'EAAS

5) 6.3 Politica di sicurezza delle informazioni

— REQ-EAASP-6.3-02: l'EAASP stabilisce procedure per notificare all'organismo di vigilanza eventuali modifiche nella prestazione del servizio fiduciario di attestati elettronici di attributi e l'intenzione di cessare tali attività, conformemente ai requisiti commerciali e alle disposizioni legislative e regolamentari pertinenti, anche conformemente ai requisiti degli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014. L'EAASP 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.

([1]) 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/oj).

([2]) 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).

6) 7.5 Controlli crittografici

— REQ-EAASP-7.5.2-05: nullo

— REQ-EAASP-7.5.2-06: nullo

— REQ-EAASP-7.5.3-01A: 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-EAASP-7.5.3-01B: per prestare i suoi servizi fiduciari, l'EAASP seleziona e utilizza tecniche crittografiche adeguate conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [2].

— REQ-EAASP-7.5.3-02: l'EAASP provvede affinché il dispositivo crittografico sicuro che utilizza per la firma o il sigillo digitale dell'EAA sia un dispositivo qualificato per la creazione di una firma o di un sigillo e che tutte le altre firme digitali o tutti gli altri sigilli digitali utilizzati per fornire il corrispondente servizio fiduciario di attestati elettronici di attributi, o parte di esso, siano creati mediante 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 nei criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, versione 3.1 (CC3.1) fino al 31.8.2027 o nella versione CC:2022, parti da 1 a 5, pubblicati dai partecipanti all'accordo "Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security", oppure quali definiti nella norma ISO/IEC 15408 [6], e certificati a livello EAL 4 o superiore, oppure

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

  c) FIPS-140-2level 3 da utilizzare fino al 31.8.2027 per i sistemi certificati esistenti oppure FIPS PUB 140-3 [3] level 3 fino al 31.12.2030.

  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.

— REQ-EAASP-7.5.5-01: nullo

— REQ-EAASP-7.5.5-02: nullo

— REQ-EAASP-7.5.5-04: nullo

7) 7.9 Gestione delle vulnerabilità e degli incidenti

— REQ-EAASP-7.9-02: le attività di monitoraggio tengono conto della sensibilità delle informazioni raccolte o analizzate.

8) 7.12 Piani di cessazione e cessazione dell'EAASP e dell'EAAS

— REQ-EAASP-7.12-04: il piano di cessazione dell'EAASP 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].».

ALLEGATO II

«ALLEGATO II

Specifiche tecniche di cui agli articoli 3 e 4

I fornitori di attestati elettronici qualificati di attributi e i fornitori di attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto rilasciano i rispettivi attestati nel rispetto di almeno una delle norme di cui all'allegato II del regolamento di esecuzione (UE) 2024/2979 della Commissione ([1]) e applicano le tecniche di revoca pertinenti di cui all'allegato II del regolamento di esecuzione (UE) 2024/2979 della Commissione.».

([1]) Regolamento di esecuzione (UE) 2024/2979 della Commissione, del 28 novembre 2024, recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda l'integrità e le funzionalità di base dei portafogli europei di identità digitale (GU L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ALLEGATO III

«ALLEGATO IV

Elenco delle norme e delle specifiche tecniche di cui all'articolo 9

I meccanismi di verifica di cui all'articolo 9 sono conformi a uno degli elementi seguenti o a entrambi, con i seguenti adattamenti:

a) le specifiche tecniche di cui al punto 6.1.1 della norma ETSI TS 119 478 V1.1.1 (2026-01) — Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources;

   — REQ-ASIP-6.1.1.2-04-01 [CONDIZIONALE]: se l'attributeVerificationResult è http://uri.etsi.org/19478/VerificationResult/Match o http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, l'attributeVerificationResult può contenere un elemento attributeValue;

   — REQ-ASIP-6.1.1.2-04-02 [CONDIZIONALE]: se l'attributeVerificationResult ricevuto è http://uri.etsi.org/19478/VerificationResult/Match e l'attributeVerificationResult contiene un elemento attributeValue, allora l'elemento attributeValue contiene lo stesso valore presente nella richiesta;

   — REQ-ASIP-6.1.1.2-04-03 [CONDIZIONALE]: se l'attributeVerificationResult ricevuto è http://uri.etsi.org/19478/VerificationResult/MatchWithVariation e l'attributeVerificationResult contiene un elemento attributeValue, allora l'elemento attributeValue contiene lo stesso valore dell'attributo conservato nella fonte autentica;

   — REQ-ASIP-6.1.1.2-06-04-01 [CONDIZIONALE]: se il fragmentVerificationResult è http://uri.etsi.org/19478/VerificationResult/Match o http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, l'attributeVerificationResult può contenere un elemento fragmentValue;

   — REQ-ASIP-6.1.1.2-06-04-02 [CONDIZIONALE]: se il fragmentVerificationResult ricevuto è http://uri.etsi.org/19478/VerificationResult/Match e l'attributeVerificationResult contiene un elemento fragmentValue, allora l'elemento fragmentValue contiene lo stesso valore presente nella richiesta;

   — REQ-ASIP-6.1.1.2-06-04-03 [CONDIZIONALE]: se il fragmentVerificationResult ricevuto è http://uri.etsi.org/19478/VerificationResult/MatchWithVariation e l'attributeVerificationResult contiene un elemento fragmentValue, allora l'elemento fragmentValue contiene lo stesso valore del frammento dell'attributo conservato nella fonte autentica;

b) le specifiche tecniche di cui al punto 6.2.3 della norma ETSI TS 119 478 V1.1.1 (2026-01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources.

   — REQ-ASIP-6.2.3.2.1-08-04: l'elemento AttributeVerificationResponse può includere esattamente un elemento figlio TextValue, XMLValue o AttributeProperties.».