2026/1731

22.7.2026

REGOLAMENTO DI ESECUZIONE (UE) 2026/1731 DELLA COMMISSIONE

del 15 luglio 2026

che modifica i regolamenti di esecuzione (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 e (UE) 2024/2982 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 5 *bis*, paragrafo 23,

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 si fondano sul lavoro svolto sulla base della raccomandazione (UE) 2021/946 della Commissione ([2]), in particolare sull'architettura e sul quadro di riferimento. Dato che l'architettura e il quadro di riferimento si sono evoluti in modo significativo rispetto all'epoca dei regolamenti di esecuzione (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) e (UE) 2024/2982 ([6]), sarebbe ora opportuno modificare tali regolamenti al fine di allinearli alle nuove norme, specifiche e procedure.

Conformemente agli obiettivi del regolamento (UE) n. 910/2014, sono state selezionate diverse norme per soddisfare tali requisiti specifici. Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Ad esempio, dato che il formato VCDM W3C è utilizzato come formato di riferimento per gli attestati, in particolare nel settore dell'istruzione, anche i portafogli europei di identità digitale dovrebbero supportare tale formato quando sono disponibili i nuovi profili nel formato VCDM W3C. Ove necessario, tali norme dovrebbero essere adattate o integrate al fine di garantire la sicurezza e l'affidabilità dei portafogli europei di identità digitale, agevolando nel contempo l'interoperabilità transfrontaliera e il funzionamento efficace del mercato interno.

(2) Per qualsiasi uso del portafoglio che richieda la presentazione dell'immagine del volto dell'utente del portafoglio, le soluzioni di portafoglio devono supportare la funzionalità di divulgazione selettiva e la divulgazione deve essere soggetta al pieno controllo da parte dell'utente. Per proteggere la capacità di decidere in merito alla divulgazione e tutelare l'immagine del volto nei confronti di richieste di divulgazione non intenzionali o non autorizzate, la progettazione a livello di architettura dei portafogli europei di identità digitale dovrebbe prevedere meccanismi di avvertimento e registrare tutte le transazioni relative all'uso dell'immagine del volto. Per garantire che l'utente del portafoglio sia a conoscenza della condivisione di dati biometrici, gli avvertimenti dovrebbero indicare che la

([1]) GU L 257 del 28.8.2014, pag. 73, ELI: http://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/reco/2021/946/oj).

([3]) Regolamento di esecuzione (UE) 2024/2977 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 i dati di identificazione personale e gli attestati elettronici di attributi rilasciati ai portafogli europei di identità digitale (GU L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) 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).

([5]) Regolamento di esecuzione (UE) 2024/2980 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 le notifiche alla Commissione in relazione all'ecosistema dei portafogli europei di identità digitale (GU L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Regolamento di esecuzione (UE) 2024/2982 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 i protocolli e le interfacce che devono essere supportati dal quadro europeo di identità digitale (GU L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

richiesta comporta la condivisione di dati biometrici e imporre all'utente in modo esplicito di confermare la divulgazione. Se una parte facente affidamento sulla certificazione tratta l'immagine del volto al fine di identificare in modo univoco una persona fisica o di confermarne l'identità dichiarata, si applicano gli articoli 6 e 9 e del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([7]) nonché tutti gli altri requisiti di tale regolamento, compreso quello relativo al trattamento dell'immagine del volto da parte delle parti facenti affidamento sulla certificazione, che dovrebbe essere limitato a quanto necessario per l'uso previsto. L'uso previsto dovrebbe essere comunicato all'utente del portafoglio, unitamente alla richiesta di divulgazione, in un linguaggio chiaro e comprensibile. Affinché si tenga debitamente conto della sensibilità dei dati biometrici, l'utente del portafoglio dovrebbe confermare esplicitamente e specificamente la divulgazione dell'immagine del volto. Il silenzio o il ricorso a caselle preselezionate non dovrebbero essere considerati una conferma da parte dell'utente del portafoglio. La conferma esplicita dell'utente del portafoglio dovrebbe essere una salvaguardia tecnica e non costituire di per sé una base giuridica per il trattamento. Come stabilito all'articolo 9, paragrafo 4, del regolamento (UE) 2016/679, gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

(3) Al fine di concedere agli Stati membri tempo sufficiente per adeguare le loro procedure nazionali, l'immagine del volto dell'utente del portafoglio può far parte dei dati obbligatori di identificazione personale per le persone fisiche soltanto a decorrere dall'11 agosto 2028. Qualora tali immagini provengano da documenti di identità esistenti, quali carte d'identità o passaporti, si applicano i requisiti pertinenti di cui rispettivamente ai regolamenti (UE) 2025/1208 ([8]) o (CE) n. 2252/2004 del Consiglio ([9]).

(4) Il regolamento (UE) n. 910/2014 impone che i portafogli siano in grado di visualizzare un marchio di fiducia UE per i portafogli di identità digitale quale indicazione verificabile, semplice e riconoscibile del fatto che un portafoglio è stato fornito conformemente al regolamento. L'uso di tale marchio di fiducia sosterrà il funzionamento efficace del mercato interno, garantirà una concorrenza leale e tutelerà gli interessi dei consumatori. Al fine di consentire l'uso di tale marchio di fiducia, è opportuno stabilirne le caratteristiche visive e tecniche.

(5) Come stabilito all'articolo 12 *ter* del regolamento (UE) n. 910/2014, i gatekeeper devono consentire ai fornitori di portafogli europei di identità digitale e agli emittenti di mezzi di identificazione elettronica notificati un'interoperabilità efficace con lo stesso sistema operativo e le stesse componenti hardware o software e, ai fini dell'interoperabilità, un accesso efficace agli stessi. Tale interoperabilità e tale accesso efficaci devono essere forniti a titolo gratuito e indipendentemente dal fatto che tali componenti hardware o software costituiscano parte del sistema operativo, siano disponibili per il gatekeeper in questione o da esso utilizzati nella fornitura dei servizi interessati. Dato che tutte le soluzioni di portafoglio dovrebbero supportare un insieme comune di protocolli e interfacce al fine di garantire l'utilizzabilità, la sicurezza e l'interoperabilità in tutti gli Stati membri, i gatekeeper dovrebbero rendere disponibili il sistema operativo e le componenti hardware o software necessari per attuare i protocolli e le interfacce di cui all'allegato XII del presente regolamento. In tale contesto, nei flussi online tra dispositivi, sia per il controllo di prossimità fisica che per il trasferimento di dati tra i due dispositivi, i gatekeeper dovrebbero preferire un canale di comunicazione locale, come consentito dalla versione 2.3 delle specifiche del Client To Authenticator Protocol (CTAP) ([10]), rispetto all'utilizzo dei servizi di tunnel ibrido CTAP.

(6) Al fine di concedere agli Stati membri, ai fornitori di certificati di registrazione della parte facente affidamento sul portafoglio e ai fornitori di portafogli il tempo sufficiente per consentire alle unità di portafoglio di autenticare e convalidare i certificati di registrazione della parte facente affidamento sul portafoglio, tale requisito dovrebbe applicarsi solo a decorrere dall'11 agosto 2028.

(7) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([11]) si applicano a tutte le attività di trattamento di dati personali ai sensi del presente regolamento.

([7]) 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).

([8]) Regolamento (UE) 2025/1208 del Parlamento europeo e del Consiglio, del 12 giugno 2025, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione (GU L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (GU L 385 del 29.12.2004, pag. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma proposta da Fido Alliance, «*Client to Authenticator Protocol (CTAP)*», 26 febbraio 2026.

([11]) 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).

(8) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([12]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 17 aprile 2026 ([13]).

(9) 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) 2024/2977

Il regolamento di esecuzione (UE) 2024/2977 è così modificato:

1) è inserito il seguente articolo 3 *bis*:

«*Articolo 3* bis

Protezione dell'immagine del volto

1. Oltre al rispetto dei requisiti relativi alle informazioni di cui al regolamento (UE) 2016/679, i fornitori di portafogli garantiscono che le soluzioni di portafoglio da essi fornite emettano avvertimenti agli utenti dei portafogli qualora le parti facenti affidamento sul portafoglio richiedano la divulgazione dell'immagine del volto, indicando che la richiesta comporta la condivisione di dati biometrici e richiede l'approvazione della divulgazione selettiva dell'immagine del volto.

2. Per l'attuazione della divulgazione selettiva dell'immagine del volto a una parte facente affidamento sul portafoglio, i fornitori di portafogli garantiscono che le soluzioni di portafoglio impongano all'utente del portafoglio di confermare esplicitamente e specificamente la presentazione dell'immagine del volto.

3. L'immagine del volto non è conservata dalle parti facenti affidamento sul portafoglio, fatto salvo il caso in cui il suo trattamento sia necessario a fini di identificazione o autenticazione conformemente al diritto dell'Unione in materia di protezione dei dati o qualora ciò sia previsto dal diritto dell'Unione o nazionale, nel rispetto del diritto dell'Unione in materia di protezione dei dati. L'immagine del volto non è trasferita a paesi terzi od organizzazioni internazionali, fatto salvo il caso in cui ciò sia consentito dal diritto dell'Unione in materia di protezione dei dati.»;

2) all'articolo 4, il paragrafo 1 è sostituito dal seguente:

«1. Gli attestati elettronici di attributi rilasciati a unità di portafoglio sono conformi ad almeno una delle norme di cui all'allegato II del regolamento di esecuzione (UE) 2024/2979 della Commissione.»;

3) all'articolo 5, paragrafo 4, la lettera b) è sostituita dalla seguente:

«b) qualora l'attestato di unità di portafoglio dell'unità di portafoglio a cui sono stati rilasciati i dati di identificazione personale sia stato revocato;»;

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

([12]) 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).

([13]) Osservazioni formali del GEPD sul progetto di regolamento di esecuzione per quanto riguarda le norme e le specifiche applicabili e la rettifica del regolamento di esecuzione (UE) 2024/2980 |Garante europeo della protezione dei dati.

Articolo 2

Modifiche del regolamento di esecuzione (UE) 2024/2979

Il regolamento di esecuzione (UE) 2024/2979 è così modificato:

1) all'articolo 3, il paragrafo 2 è soppresso.

2) All'articolo 5, paragrafo 1, la lettera a) è sostituita dalla seguente:

«a) effettuino operazioni crittografiche del portafoglio che coinvolgono risorse critiche conservate in un dispositivo crittografico sicuro per il portafoglio e non necessarie per l'autenticazione dell'utente del portafoglio soltanto nei casi in cui tali applicazioni abbiano autenticato con successo gli utenti del portafoglio;»;

3) è inserito l'articolo 5 *bis* seguente:

«*Articolo 5* bis

Meccanismi crittografici

Ai fini dell'articolo 4, paragrafo 2, i fornitori di portafogli utilizzano solo i meccanismi crittografici di cui all'allegato I *bis*.»;

4) l'articolo 6 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. I fornitori di portafogli rilasciano attestati di unità di portafoglio per ciascuna unità di portafoglio. I fornitori di portafogli firmano o sigillano gli attestati di unità di portafoglio in modo tale che le firme o i sigilli possano essere convalidati mediante un certificato che figura nell'elenco conformemente all'allegato II, sezione 2, punto 1, lettera h), del regolamento di esecuzione (UE) 2024/2980.»;

b) il paragrafo 2 è sostituito dal seguente:

«2. I fornitori di portafogli garantiscono che gli attestati di unità di portafoglio di cui al paragrafo 1 siano conformi alle specifiche tecniche di cui all'allegato I ter.»;

c) al paragrafo 3, la lettera b) è sostituita dalla seguente:

«b) forniscono meccanismi sicuri di identificazione e autenticazione per gli utenti del portafoglio, che *sono indipendenti dalle unità di portafoglio;*»;

5) all'articolo 9, paragrafo 2, la lettera b) è sostituita dalla seguente:

«b) il nome, i dati di contatto e l'identificatore univoco della corrispondente parte facente affidamento sul portafoglio e dello Stato membro in cui tale parte è stabilita;»;

6) all'articolo 10, il paragrafo 1 è sostituito dal seguente:

«1. I fornitori di portafogli garantiscono che gli attestati elettronici di attributi rilasciati conformemente alle specifiche tecniche applicabili per politiche di divulgazione incorporate comuni di cui all'allegato III possano essere trattati dalle unità di portafoglio che forniscono.»;

7) l'articolo 12 è così modificato:

a) al paragrafo 2, la lettera c) è sostituita dalla seguente:

«c) creazione di firme o sigilli come minimo nel formato obbligatorio per firme o sigilli di cui all'allegato IV;»;

b) il paragrafo 3 è sostituito dal seguente:

«3. Le applicazioni per la creazione di firme possono essere integrate in istanze di portafoglio o essere esterne a queste ultime.»;

c) è inserito il paragrafo seguente:

«4. Le applicazioni per la creazione di firme utilizzate dalle unità di portafoglio supportano come minimo l'interfaccia di programmazione di un'applicazione di cui all'allegato IV.»;

8) all'articolo 14, il paragrafo 1 è soppresso;

9) è inserito il seguente articolo 14 *bis*:

«*Articolo 14* bis

Marchio di fiducia UE per i portafogli di identità digitale

1. I fornitori di portafogli garantiscono che le unità di portafoglio espongano il marchio di fiducia UE per i portafogli di identità digitale. Il marchio di fiducia UE per i portafogli di identità digitale è conforme al formato di cui agli allegati VI e VII.

2. I fornitori di portafogli garantiscono che le unità di portafoglio consentano agli utenti del portafoglio di accedere alle informazioni che consentono loro di verificare lo stato di certificazione della soluzione di portafoglio. A tal fine i fornitori di portafogli garantiscono che, a seguito della registrazione di una soluzione di portafoglio, le corrispondenti unità di portafoglio includano gli URL forniti dalla Commissione europea per tale verifica. I fornitori di portafogli garantiscono che le loro unità di portafoglio abbiano accesso ai dati del marchio di fiducia UE per i portafogli di identità digitale conformi alle specifiche tecniche di cui all'allegato VIII.

3. I colori di riferimento per il marchio di fiducia UE per i portafogli di identità digitale sono Pantone n. 661 e 116, oppure blu (100 % ciano + 67 % magenta + 0 % giallo + 40 % nero) e giallo (0 % ciano + 20 % magenta + 100 % giallo + 0 % nero), quando si ricorre alla quadricromia; se si usano colori RGB, i colori di riferimento sono blu (0 rosso + 51 verde + 153 blu) e giallo (255 rosso + 204 verde + 0 blu).

4. Soltanto qualora l'uso del colore non sia praticabile, il marchio di fiducia UE per i portafogli di identità digitale può essere utilizzato in bianco e nero come stabilito nell'allegato VII.

5. Se utilizzato su uno sfondo scuro, il marchio di fiducia UE per i portafogli di identità digitale può essere utilizzato in formato negativo utilizzando lo stesso colore di fondo. Se il marchio di fiducia UE per i portafogli di identità digitale è utilizzato a colori su uno sfondo colorato che ne rende difficile la visualizzazione, è possibile utilizzare una linea esterna di delimitazione intorno al marchio di fiducia UE per i portafogli di identità digitale al fine di migliorare il contrasto rispetto ai colori dello sfondo.

6. Il marchio di fiducia UE per i portafogli di identità digitale presenta una dimensione minima di 64 × 85 pixel con una risoluzione di 150 dpi.

7. I fornitori di portafogli garantiscono che il marchio di fiducia UE per i portafogli di identità digitale sia utilizzato in modo da consentire un'indicazione chiara dell'unità di portafoglio cui detto marchio fa riferimento. Il marchio di fiducia UE per i portafogli di identità digitale può essere associato a elementi grafici o testuali che indichino in maniera chiara l'unità di portafoglio per la quale è utilizzato, a condizione che non ne modifichino la riconoscibilità come marchio di fiducia UE per i portafogli di identità digitale, né alterino l'associazione con l'elenco dei portafogli europei di identità digitale certificati di cui all'articolo 5 quinquies del regolamento (UE) n. 910/2014.

8. Qualora abbiano revocato un attestato di unità di portafoglio, i fornitori di portafogli garantiscono che il marchio di fiducia UE per i portafogli di identità digitale non sia più visualizzato dalla corrispondente unità di portafoglio.»;

10) sono aggiunti gli allegati I *bis* e I *ter* che figurano negli allegati II e III del presente regolamento;

11) L'allegato II è sostituito dall'allegato IV del presente regolamento.

12) L'allegato III è sostituito dall'allegato V del presente regolamento.

13) L'allegato IV è modificato conformemente all'allegato VI del presente regolamento.

14) L'allegato V è soppresso.

15) Il testo che figura nell'allegato VII del presente regolamento è inserito come allegato VI.

16) Il testo che figura nell'allegato VIII del presente regolamento è inserito come allegato VII.

17) Il testo che figura nell'allegato IX del presente regolamento è inserito come allegato VIII.

Articolo 3

Modifiche del regolamento di esecuzione (UE) 2024/2980

Il regolamento di esecuzione (UE) 2024/2980 è così modificato:

1) all'articolo 5, il paragrafo 2 è sostituito dal seguente:

«2. Se del caso, la Commissione redige, tiene aggiornato e pubblica un elenco contenente le informazioni notificate dagli Stati membri sui fornitori di portafogli, sui fornitori di dati di identificazione personale, sui fornitori di certificati di accesso delle parti facenti affidamento sul portafoglio e sui fornitori di certificati di registrazione delle parti facenti affidamento sul portafoglio di cui all'allegato II, sezioni 2, 3, 4 e 5.»;

2) L'allegato II del regolamento di esecuzione (UE) 2024/2980 è modificato conformemente all'allegato X del presente regolamento.

Articolo 4

Modifiche del regolamento di esecuzione (UE) 2024/2982

Il regolamento di esecuzione (UE) 2024/2982 è così modificato:

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

«2) la presentazione degli attributi dei dati di identificazione personale e degli attestati elettronici di attributi alle parti facenti affidamento sul portafoglio;»;

2) l'articolo 3 è così modificato:

a) il punto 1 è sostituito dal seguente:

«1) autentichino e convalidino i certificati di accesso della parte facente affidamento sul portafoglio quando interagiscono con parti facenti affidamento sul portafoglio senza delegare l'esecuzione di tali processi a un browser del sistema operativo o a un'altra applicazione intermedia;»;

b) il punto 2 è soppresso.

c) il punto 3 è sostituito dal seguente:

«3) autentichino e convalidino le richieste presentate utilizzando certificati di accesso della parte facente affidamento sul portafoglio;»;

d) il punto 4 è sostituito dal seguente:

«4) autentichino e convalidino il certificato di registrazione della parte facente affidamento sul portafoglio;»;

e) il punto 5 è sostituito dal seguente:

«5) consentano agli utenti del portafoglio di visualizzare le informazioni contenute nei certificati di accesso della parte facente affidamento sul portafoglio;»;

f) il punto 8 è soppresso.

g) il punto 9 è sostituito dal seguente:

«9) non presentino gli attributi richiesti alle parti facenti affidamento sul portafoglio fino a quando non sono completati i passaggi seguenti:

a) verifica del fatto che le politiche di divulgazione incorporate siano state elaborate all'interno dell'unità di portafoglio conformemente all'articolo 10 del regolamento di esecuzione (UE) 2024/2979;

b) verifica del fatto che gli utenti del portafoglio abbiano approvato parzialmente o integralmente la presentazione.»;

3) all'articolo 4, il paragrafo 1 è sostituito dal seguente:

«1. I fornitori di portafogli garantiscono che le soluzioni di portafoglio supportino i protocolli e le interfacce di cui all'allegato I per il rilascio di dati di identificazione personale e attestati elettronici di attributi a unità di portafoglio.»;

4) l'articolo 5 è così modificato:

   a) i paragrafi 1 e 2 sono sostituiti dai seguenti:

      «1. I fornitori di portafogli garantiscono che le soluzioni di portafoglio supportino protocolli e interfacce per la presentazione di attributi a parti facenti affidamento sul portafoglio, a distanza, e se opportuno in prossimità, conformemente alle specifiche tecniche di cui all'allegato II.

      2. I fornitori di portafogli garantiscono che, su richiesta degli utenti, le unità di portafoglio rispondano alle richieste autenticate e convalidate con successo delle parti facenti affidamento sul portafoglio di cui all'articolo 3, conformemente alle specifiche tecniche di cui all'allegato II.»;

   b) il paragrafo 5 è soppresso.

5) L'articolo 8 è sostituito dal seguente:

   «*Articolo 8*

   Entrata in vigore

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

   L'articolo 3, paragrafo 4, si applica a decorrere dall'11 agosto 2028.

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

6) L'allegato è soppresso.

7) Il testo che figura nell'allegato XI del presente regolamento è aggiunto come allegato I.

8) Il testo che figura nell'allegato XII del presente regolamento è aggiunto come allegato II.

Articolo 5

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 15 luglio 2026

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

«ALLEGATO

Specifiche tecniche per i dati di identificazione personale di cui all'articolo 3, paragrafo 3

1) Sezione 1: Insieme di dati di identificazione delle persone fisiche

Tabella 1

Dati di identificazione personale obbligatori per le persone fisiche per la divulgazione selettiva

Identificatore dei dati	Definizione
`family_name`	Cognome/i attuale/i dell'utente a cui i dati di identificazione personale fanno riferimento.
`given_name`	Nome/i attuale/i, compresi secondi nomi se del caso, dell'utente a cui i dati di identificazione personale fanno riferimento.
`birth_date`	Giorno, mese e anno in cui è nato l'utente a cui i dati di identificazione personale fanno riferimento.
`birth_place`	Paese, sotto forma di codice paese alpha-2, come specificato nella norma ISO 3166-1, oppure Stato, provincia, distretto o area locale o comune, città o località in cui è nato l'utente a cui i dati di identificazione personale fanno riferimento.
`nationality`	Uno o più codici paese alpha-2, come specificati nella norma ISO 3166-1, che rappresentano la cittadinanza dell'utente a cui i dati di identificazione personale fanno riferimento.
`portrait`	Salvo rifiuto esplicito dell'utente, se del caso, l'immagine del volto dell'utente a cui i dati di identificazione personale fanno riferimento, conforme ai requisiti di qualità per un tipo di immagine frontale di cui alla norma ISO/IEC 39794-5 o, per la retrocompatibilità, di cui alla norma ISO/IEC 19794-5, punti 8.2, 8.3 e 8.4, fornita sotto forma di dati di immagine codificati senza intestazioni o blocchi di cui al punto 5 della norma ISO/IEC 19794-5, fatta eccezione per i dati dell'immagine stessi (un file JPEG), si applica a decorrere dall'11 agosto 2028.

— Gli stati membri possono prevedere che l'utente abbia la possibilità di rifiutare l'inserimento dell'immagine del volto nei dati di identificazione personale.

— Gli Stati membri provvedono affinché la divulgazione selettiva si applichi a ciascun identificatore dei dati, compresa l'immagine del volto;

— se la data di nascita della persona fisica non è nota, gli Stati membri devono scegliere valori adeguati conformi alle specifiche di cui alle sezioni 4.1 o 4.2 (a seconda dei casi) del presente allegato;

— se la cittadinanza della persona fisica non è nota, gli Stati membri devono utilizzare il valore "QU";

— se la persona fisica non dispone di alcuna cittadinanza, gli Stati membri devono utilizzare il valore "QS";

— se l'utente rifiuta l'inclusione dell'immagine del volto, gli Stati membri impostano il valore su "vuoto".

Tabella 2

Dati di identificazione personale facoltativi per le persone fisiche per la divulgazione selettiva

Identificatore dei dati	Definizione
resident_address	L'indirizzo completo del luogo presso il quale risiede o può essere contattato attualmente l'utente a cui i dati di identificazione personale fanno riferimento (via, numero civico, città ecc.).
resident_country	Il paese in cui risiede attualmente l'utente a cui i dati di identificazione personale fanno riferimento, sotto forma di codice paese alpha-2, come specificato nella norma ISO 3166-1.
resident_state	Lo Stato, la provincia, il distretto o l'area locale in cui risiede attualmente l'utente a cui i dati di identificazione personale fanno riferimento.
resident_city	Il comune, la città, la località o il paese in cui risiede attualmente l'utente a cui i dati di identificazione personale fanno riferimento.
resident_postal_code	Il codice postale del luogo in cui risiede attualmente l'utente a cui i dati di identificazione personale fanno riferimento.
resident_street	Il nome della via in cui risiede attualmente l'utente a cui i dati di identificazione personale fanno riferimento, compresi il numero civico ed eventuali affissi o suffissi.
personal_administrative_-number	Un valore assegnato all'utente a cui i dati di identificazione personale fanno riferimento che è univoco tra tutti i numeri amministrativi personali rilasciati dal fornitore di dati di identificazione personale. Qualora scelgano di includere tale attributo, gli Stati membri descrivono nei loro regimi di identificazione elettronica nell'ambito dei quali sono rilasciati i dati di identificazione personale la politica che applicano ai valori di tale attributo, comprese, se del caso, le condizioni specifiche per il trattamento di questo valore.
family_name_birth	Cognome/i dell'utente a cui i dati di identificazione personale fanno riferimento al momento della nascita.
given_name_birth	Nome/i, compresi secondi nomi, dell'utente a cui i dati di identificazione personale fanno riferimento al momento della nascita.
sex	Il valore deve essere uno dei seguenti: 0 = non noto; 1 = maschio; 2= femmina; 3= altro; 4 = inter; 5 = diverso; 6 = aperto; 9 = non applicabile. Per i valori 0, 1, 2 e 9 si applica la norma ISO/IEC 5218.
email_address	Indirizzo di posta elettronica dell'utente a cui i dati di identificazione personale fanno riferimento [conformemente all'RFC 5322 ([1])].

Identificatore dei dati	Definizione
`mobile_phone_number`	Numero di cellulare dell'utente a cui i dati di identificazione personale fanno riferimento, che inizia con il simbolo "+" indicante il prefisso internazionale, seguito dal prefisso del paese e da cifre.

([1]) P. Resnick, ed., *Internet Message Format*, RFC 5322, ottobre 2008.

2) Sezione 2: Insieme di dati di identificazione delle persone giuridiche

Tabella 3

Dati di identificazione personale obbligatori per le persone giuridiche

Identificatore dei dati
ragione sociale attuale
identificatore univoco costruito dallo Stato membro di invio conformemente alle specifiche tecniche ai fini dell'identificazione transfrontaliera e il più possibile persistente nel tempo

— Se un identificatore dei dati non è noto per la persona o non può essere rilasciato altrimenti nell'insieme di dati di identificazione personale, gli Stati membri utilizzano piuttosto un valore di attributo adeguato alla situazione.

Tabella 4

Dati di identificazione personale facoltativi per le persone giuridiche

Identificatore dei dati
indirizzo attuale
numero di partita IVA
numero di riferimento fiscale
identificativo unico europeo di cui alla direttiva (UE) 2017/1132 del Parlamento europeo e del Consiglio ([1])
identificativo della persona giuridica di cui al regolamento di esecuzione (UE) 2022/1860 della Commissione ([2])
numero di registrazione e identificazione degli operatori economici (EORI) di cui al regolamento di esecuzione (UE) n. 1352/2013 della Commissione ([3])
numero di accisa di cui all'articolo 2, punto 12), del regolamento (UE) n. 389/2012 del Consiglio ([4])

([1]) Direttiva (UE) 2017/1132 del Parlamento europeo e del Consiglio, del 14 giugno 2017, relativa ad alcuni aspetti di diritto societario, GU L 169 del 30.6.2017, pag. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Regolamento di esecuzione (UE) 2022/1860 della Commissione del 10 giugno 2022 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio per quanto riguarda le norme, i formati, la frequenza, i metodi e le modalità di segnalazione (GU L 262 del 7.10.2022, pag. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Regolamento di esecuzione (UE) n. 1352/2013 della Commissione, del 4 dicembre 2013, che stabilisce i formulari di cui al regolamento (UE) n. 608/2013 del Parlamento europeo e del Consiglio relativo alla tutela dei diritti di proprietà intellettuale da parte delle autorità doganali (GU L 341 del 18.12.2013, pag. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Regolamento (UE) n. 389/2012 del Consiglio, del 2 maggio 2012, relativo alla cooperazione amministrativa in materia di accise e che abroga il regolamento (CE) n. 2073/2004 (GU L 121 del 8.5.2012, pag. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) Sezione 3: Insieme di metadati relativi ai dati di identificazione personale

Tabella 5

Metadati relativi ai dati di identificazione personale

Identificatore dei dati	Definizione	Presenza
`issuing_authority`	Nome dell'autorità amministrativa che ha rilasciato i dati di identificazione personale o codice paese alpha-2 ISO 3166 del rispettivo Stato membro qualora non esista un'autorità distinta autorizzata a rilasciare i dati di identificazione personale.	Obbligatorio
`issuing_country`	Codice paese alpha-2, come specificato nella norma ISO 3166-1, del paese o territorio del fornitore dei dati di identificazione personale.	obbligatorio
`expiry_date`	Data (e se possibile ora) in cui scadrà il periodo di validità amministrativa dei dati di identificazione personale.	Facoltativo
`document_number`	Un numero per i dati di identificazione personale, assegnato dal fornitore di tali dati.	Facoltativo
`issuing_jurisdiction`	Codice di suddivisione del paese corrispondente alla giurisdizione in cui sono stati rilasciati i dati di identificazione personale, come specificato al punto 8 della norma ISO 3166-2:2020. La prima parte del codice è identica al valore per il paese di rilascio.	Facoltativo
`issuance_date`	Data, e se possibile ora, in cui è iniziato a decorrere il periodo di validità amministrativa dei dati di identificazione personale.	Facoltativo

4) Sezione 4: codifica degli attributi dei dati di identificazione delle persone fisiche

— I dati di identificazione delle persone fisiche devono essere rilasciati conformemente alle norme di cui all'allegato II del regolamento di esecuzione (UE) 2024/2979, punti 5 (formato SD-JWT VC) e 6 (formato ISO/IEC-mdoc) applicabili agli attestati elettronici di attributi. I punti 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 e 6.2.5 non devono applicarsi;

— la codifica dei dati di identificazione delle persone fisiche deve essere conforme alle specifiche tecniche di cui alle sezioni 4.1 e 4.2 del presente allegato.

4.1 Codifica dei dati di identificazione delle persone fisiche in formato ISO/IEC-mdoc

— Il tipo di attestato per i dati di identificazione personale in formato ISO/IEC mdoc deve essere "eu.europa.ec.eudi.pid.1". L'identificatore dello spazio dei nomi per gli attributi dei dati di identificazione personale di cui al presente allegato deve essere "eu.europa.ec.eudi.pid.1";

— se i dati di identificazione personale comprendono dati per i quali gli identificatori dei dati non sono stabiliti nel presente allegato, tali dati devono essere definiti all'interno di uno spazio dei nomi nazionale dei dati di identificazione personale che utilizza il formato generale eu.europa.ec.eudi.pid.[codice paese alpha-2 ISO 3166-1 o codice regione ISO 3166-2] seguito da un punto e da un numero di versione facoltativi;

— qualora sia utilizzato lo spazio dei nomi nazionale, il relativo regime, unitamente a tutti gli identificatori dei dati, le relative definizioni, presenza e i relativi formati di codifica, deve essere pubblicato conformemente all'articolo 8 del regolamento di esecuzione (UE) 2025/1569 della Commissione ([1]);

— i dati di identificazione personale e i relativi metadati di cui alle sezioni 1 e 3 del presente allegato devono essere inclusi negli elementi dei dati di identificazione personale ai sensi delle specifiche di formato ISO/IEC mdoc;

— il membro deviceKey [chiave dispositivo] all'interno del membro deviceKeyInfo [informazioni chiave dispositivo] dell'istanza del tipo MobileSecurityObject [oggetto sicurezza mobile] deve contenere una chiave pubblica;

— tale chiave pubblica deve corrispondere a una chiave privata conservata nel dispositivo crittografico sicuro per il portafoglio ("WSCD" – *wallet secure cryptographic device*) dell'utente del portafoglio;

— l'intestazione protetta della firma digitale CB-AdES che firma i dati di identificazione personale in formato ISO/IEC-mdoc deve contenere i parametri di intestazione x5u e x5t, entrambi specificati nell'RFC 9360 ([2]);

— l'algoritmo digest utilizzato nel parametro di intestazione x5t deve essere SHA-256;

— i requisiti per la codifica dei dati di identificazione personale in formato ISO/IEC-mdoc sono stabiliti nella tabella 6:

Tabella 6

Requisiti per la codifica dei dati di identificazione personale in formato ISO/IEC-mdoc

Identificatore dei dati	Identificatore dell'attributo	Formato di codifica
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) 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).

([2]) J. Schaad, *CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates* (https://datatracker.ietf.org/doc/rfc9360/).

Identificatore dei dati	Identificatore dell'attributo	Formato di codifica
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate o full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate o full-date

— La notazione del formato di codifica degli attributi specificati nella tabella 6 deve utilizzare i tipi di rappresentazione specificati nell'RFC 8610 ([3]), con i requisiti supplementari seguenti:

(a) un tstr deve essere codificato in UTF-8;

(b) un tstr deve supportare l'intero intervallo di valori Unicode;

(c) un tstr deve avere una lunghezza massima di 150 caratteri;

(d) una data deve essere codificata come specificato nell'RFC 8943 ([4]);

(e) una data completa deve essere interpretata come #6.1004(tstr), dove il tag 1004 corrisponde a quanto specificato nell'RFC 8943;

(f) un attributo tdate deve contenere una stringa data-ora come specificato nell'RFC 3339 ([5]);

(g) un attributo full-date deve contenere una stringa full-date come specificato nell'RFC 3339, conformemente all'RFC 8943;

(h) salvo diversa indicazione, una rappresentazione di una data negli attributi:

— non deve utilizzare frazioni di secondi;

— non deve applicare una differenza dell'ora locale rispetto al tempo universale coordinato (UTC – *Coordinated Universal Time*) e la differenza dell'ora specificata nell'RFC 3339 deve essere impostata su "Z";

(i) un numero intero con i tipi principali 0 e 1 deve essere il più piccolo possibile, come specificato nell'RFC 8949 ([6]), sezione 4.2;

(j) un place_of_birth deve contenere almeno una delle seguenti coppie di valori chiave: "country", "region" o "locality";

(k) l'espressione della lunghezza in un bstr, un tstr, un array o una mappa deve essere la più breve possibile, come specificato nell'RFC 8949, sezione 4.2;

([3]) C. Vigano e H. Birkholz, *Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures*, RFC 8610, giugno 2019.
([4]) M. Jones, A. Nadalin e J. Richter, *Concise Binary Object Representation (CBOR) Tags for Date*, RFC 8943, novembre 2020.
([5]) G. Klyne e C. Newman, *Date and Time on the Internet: Timestamps*, RFC 3339, luglio 2002.
([6]) C. Bormann e P. Hoffman, *Concise Binary Object Representation (CBOR)*, RFC 8949, dicembre 2020.

(l) l'attributo cittadinanza deve essere codificato come un array di codici paese alpha-2 come specificato nella norma ISO 3166-1. Se si utilizza la notazione CDDL come specificato nell'RFC 8610, la codifica di tale attributo deve essere:

— nationalities = [+ CountryCode];

— CountryCode = tstr ; codice paese alpha-2 di cui alla norma ISO 3166-1;

— qualora un utente del portafoglio a cui i dati di identificazione personale fanno riferimento abbia più cittadinanze e il fornitore di dati di identificazione personale attesti tali cittadinanze multiple, il fornitore di dati di identificazione personale può includere tutte le cittadinanze in questi ultimi dati;

— l'attributo place_of_birth deve essere codificato come un tipo place_of_birth. Se si utilizza la notazione CDDL come specificato nell'RFC 8610, la codifica di tale attributo deve essere:

place_of_birth =

{

? "country": tstr ; un unico codice paese alpha-2 di cui alla norma ISO 3166-1

? "region": tstr ; il nome di uno Stato, di una provincia, di un distretto o di un'area locale

? "locality": tstr ; il nome di un comune, di una città, di una località o di un paese

}

4.2 Requisiti per la codifica dei dati di identificazione personale in formato SD-JWT VC

— I dati di identificazione personale e i relativi metadati di cui alla presente sezione devono essere inclusi nei dati di identificazione personale come dichiarazioni ai sensi delle specifiche di formato SD-JWT VC;

— tutte le dichiarazioni presenti nei dati di identificazione personale rilasciati, di cui al precedente trattino, devono essere divulgabili individualmente in modo selettivo, fatta eccezione per le dichiarazioni definite come divulgabili in modo non selettivo in formato SD-JWT VC;

— la tabella 7 specifica la codifica dei nomi delle dichiarazioni che sono nomi pubblici;

— la tabella 8 specifica la codifica dei nomi delle dichiarazioni che sono specifici dei dati di identificazione personale;

— una stringa JSON utilizzata nei dati di identificazione personale codificati in formato SD-JWT VC deve essere codificata in formato UTF-8 e deve supportare l'intero intervallo di valori Unicode, salvo diversa indicazione esplicita nella tabella 8 o nei riferimenti ivi contenuti;

— le dichiarazioni JWT nbf e exp quali definite nell'RFC 7519 ([7]) devono essere utilizzate per esprimere il periodo di validità tecnica dei dati di identificazione personale conformi al formato SD-JWT VC;

([7]) J. Jones, *et al.*, *JSON Web Token (JWT)*, RFC 7519, maggio 2015.

— i dati di identificazione personale devono integrare la dichiarazione cnf quale definita nell'RFC 7800 ([8]), che deve essere una chiave pubblica generata da una chiave privata conservata nel WSCD dell'unità di portafoglio dell'utente del portafoglio.

— l'intestazione protetta della firma digitale che firma i dati di identificazione personale in formato SD-JWT VC deve contenere i parametri di intestazione x5u e x5t#S256, specificati nell'RFC 7515 ([9]).

Tabella 7

Requisiti per la codifica dei dati di identificazione personale in formato SD-JWT VC con l'utilizzo di nomi pubblici

Identificatore dei dati	Identificatore dell'attributo	Formato di codifica
`family_name`	`family_name`	Stringa
`given_name`	`given_name`	Stringa
`birth_date`	`birthdate`	Stringa, ISO 8601-1, formato AAAA-MM-GG
`birth_place`	`place_of_birth`	Struttura JSON
`nationality`	`nationalities`	Array di stringhe
`resident_address`	`address.formatted`	Stringa
`resident_country`	`address.country`	Stringa
`resident_state`	`address.region`	Stringa
`resident_city`	`address.locality`	Stringa
`resident_postal_code`	`address.postal_code`	Stringa
`resident_street`	`address.street_address`	Stringa
`family_name_birth`	`birth_family_name`	Stringa
`given_name_birth`	`birth_given_name`	Stringa
`email_address`	`email`	Stringa
`mobile_phone_number`	`phone_number`	Stringa
`portrait`	`picture`	Stringa; URL dei dati contenente un'immagine del volto codificata come base64 in formato JPEG

([8]) M. Jones, *et al.*, *Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)*, RFC 7800, aprile 2016.
([9]) M. Jones *et al.*, *JSON Web Signature (JWS)*, RFC 7515, maggio 2015.

Tabella 8

Requisiti per la codifica dei dati di identificazione personale in formato SD-JWT VC con l'utilizzo di nomi privati

Identificatore dei dati	Identificatore dell'attributo	Formato di codifica
`expiry_date`	`date_of_expiry`	Stringa, ISO 8601-1, formato AAAA-MM-GG
`issuance_date`	`date_of_issuance`	Stringa, ISO 8601-1, formato AAAA-MM-GG
`personal_administrative_number`	`personal_administrative_number`	Stringa
`sex`	`sex`	Numero
`issuing_authority`	`issuing_authority`	Stringa
`issuing_country`	`issuing_country`	Stringa
`document_number`	`document_number`	Stringa
`issuing_jurisdiction`	`issuing_jurisdiction`	Stringa

— Il tipo di base di dati di identificazione personale deve essere "urn:eudi:pid:1", incluso nella dichiarazione "vct". Tutti i dati di identificazione personale devono utilizzare tipi nello spazio dei nomi "urn:eudi:pid:";

— se tra i dati di identificazione personale figurano attributi non specificati nel presente allegato, tali attributi devono essere definiti all'interno di un tipo nazionale;

— qualora sia utilizzato il tipo nazionale, il relativo regime, unitamente a tutti gli identificatori dei dati, le relative definizioni e presenze e i relativi formati di codifica, deve essere definito in un regime pubblicato a norma dell'articolo 8 del regolamento di esecuzione (UE) 2025/1569.

5) Sezione 5: Dettagli dell'infrastruttura fiduciaria

L'elenco dei fornitori di dati di identificazione personale messo a disposizione dalla Commissione a norma del regolamento di esecuzione (UE) 2024/2980 deve consentire l'autenticazione dei dati di identificazione personale.»

ALLEGATO II

«*ALLEGATO I bis*

Meccanismi crittografici di cui all'articolo 5 *bis*

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]).»

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

ALLEGATO III

«*ALLEGATO I ter*

Specifiche tecniche per gli attestati di unità di portafoglio di cui all'articolo 6, paragrafo 2 *bis*

1) Un attestato di unità di portafoglio deve comprendere uno o più attestati di istanza di portafoglio e uno o più attestati di chiave.

2) L'attestato dell'istanza di portafoglio e gli attestati di chiave devono soddisfare i requisiti seguenti:

(a) Requisiti in materia di formato

— FR-WIA-1: un attestato di istanza di portafoglio deve essere un JSON Web Token (JWT), come specificato nell'RFC 7519 ([1]), firmato o sigillato dal fornitore del portafoglio mediante una firma JAdES baseline B compatta;

— FR-WIA-1.1: un attestato di istanza di portafoglio deve essere un attestato di portafoglio di cui all'appendice E del documento "OpenID for Verifiable Credential Issuance v1.0" ([2]) ("OID4VCI") ed esteso come specificato alle voci C-WIA-1 e C-WIA-2 in appresso;

— FR-KA-1: un attestato di chiave deve essere un JWT, come specificato nell'RFC 7519, firmato o sigillato dal fornitore del portafoglio mediante firma JAdES baseline B compatta;

— FR_KA_1.1: un attestato di chiave deve essere un attestato di chiave di cui all'appendice D dell'OID4VCI, esteso come specificato alle voci C_KA-1 e C_KA-2 in appresso.

(b) Requisiti in materia di trasporto

— TR-WIA-1: un'unità di portafoglio deve utilizzare un attestato di istanza di portafoglio durante il rilascio di dati di identificazione personale, di attestati elettronici di attributi qualificati o non qualificati oppure di attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per conto di detto organismo;

— TR-WIA-2: un fornitore del portafoglio deve verificare l'integrità dell'istanza di portafoglio e firmare o sigillare l'attestato di istanza di portafoglio;

— TR-WIA-2.1: se un fornitore del portafoglio rilascia un attestato di istanza di portafoglio, il tempo che intercorre tra il momento in cui detto fornitore ha verificato l'integrità dell'istanza di portafoglio e il momento che lo stesso indicherà nel parametro di intestazione "exp" [scadenza] dell'attestato di istanza di portafoglio rilasciato deve essere inferiore a 24 ore;

— TR-WIA-2.2: il fornitore del portafoglio deve garantire che un'unità di portafoglio contenga gli attestati di istanza di portafoglio necessari per il rilascio dei dati di identificazione personale e degli attestati elettronici di attributi;

— TR-WIA-3: durante il rilascio, un'unità di portafoglio deve inviare un attestato di istanza di portafoglio al server di autorizzazione nella richiesta di autorizzazione push e nella richiesta di token, come specificato nell'OID4VCI;

— TR-WIA-3.1: un'unità di portafoglio deve inviare l'attestato di istanza di portafoglio unitamente a una prova del possesso ("PoP" – *Proof-of-Possession*), di cui all'appendice E dell'OID4VCI;

— TR-WIA-3.2: un'unità di portafoglio deve inviare lo stesso attestato di istanza di portafoglio a un solo server di autorizzazione;

([1]) RFC 7519: *JSON Web Token (JWT)*, maggio 2015.
([2]) *OpenID for Verifiable Credential Issuance v1.0*, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: se un fornitore del portafoglio utilizza l'opzione "per-issuer reuse" [riutilizzo per singola entità che effettua il rilascio] specificata alla voce R_WIA_1, un'unità di portafoglio può inviare più volte un attestato di istanza di portafoglio allo stesso server di autorizzazione;

— TR-WIA-3.2.2: se un fornitore del portafoglio non si avvale dell'opzione "per-issuer reuse", un'unità di portafoglio deve utilizzare un attestato di istanza di portafoglio nell'ambito di al massimo una procedura di rilascio;

— TR-WIA-4: se riceve un attestato di istanza di portafoglio, un server di autorizzazione deve verificare la firma di tale attestato tramite la chiave pubblica presente nel certificato di firma incluso nel parametro "x5c" nell'intestazione JOSE dell'attestato di istanza di portafoglio;

— TR-WIA-4.1: il server di autorizzazione deve verificare altresì che tale certificato di firma possa essere verificato tramite un'ancora di fiducia presente nell'elenco dei fornitori di portafogli, di cui all'articolo 5 del regolamento di esecuzione (UE) 2024/2980, utilizzando potenzialmente certificati intermedi inclusi nel parametro x5c;

— TR-WIA-4.2: il server di autorizzazione deve verificare che l'attestato di istanza di portafoglio non sia scaduto;

— TR-WIA-4.3: il server di autorizzazione deve verificare la firma del PoP tramite la chiave pubblica presente nella dichiarazione "cnf";

— TR_KA-1: un'unità di portafoglio deve utilizzare un attestato di chiave durante il rilascio di dati di identificazione personale e durante il rilascio di attestati elettronici di attributi qualificati o non qualificati associati a un dispositivo oppure di attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per conto di detto organismo;

— TR_KA-1.1: un'unità di portafoglio non deve utilizzare un attestato di chiave durante il rilascio di attestati elettronici di attributi qualificati o non qualificati non associati a un dispositivo oppure di attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per conto di detto organismo;

— TR_KA-2: un fornitore del portafoglio deve fornire a un'unità di portafoglio attestati di chiave diversi per il WSCD dell'unità di portafoglio e per ciascuno dei suoi keystore;

— TR_KA-2.1: il fornitore del portafoglio deve firmare o sigillare un attestato di chiave dopo aver verificato che le chiavi attestate in detto attestato sono conservate nel WSCD dell'unità di portafoglio o nel keystore descritto nell'attestato di chiave;

— TR_KA-2.2: un attestato di chiave deve contenere almeno una chiave pubblica attestata. Il numero di chiavi presenti nell'attestato di chiave inviato a un'entità che rilascia le credenziali non dovrebbe superare la dimensione massima del lotto specificata da tale entità nei suoi metadati dell'entità che rilascia le credenziali; cfr. ETSI TS 119 472-3 ([3]), parametro "credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size";

— TR_KA-2.3: un fornitore del portafoglio deve includere una chiave pubblica (corrispondente a una chiave privata conservata nel WSCD o nel keystore dell'unità di portafoglio) nell'ambito di al massimo un attestato di chiave;

— TR_KA-2.4: un'unità di portafoglio deve utilizzare un attestato di chiave durante al massimo una procedura di rilascio di credenziali o di nuovo rilascio di credenziali;

— TR_KA-2.5: un fornitore del portafoglio deve garantire che un'unità di portafoglio sia in possesso degli attestati di chiave necessari per il rilascio dei dati di identificazione personale e degli attestati elettronici di attributi associati al dispositivo;

([3]) ETSI, *Electronic Signatures and Infrastructures (ESI); JAdES digital signatures;* Parte 3: *JAdES levels and baseline profiles*, ETSI TS 119 472-3, V1.1.1, marzo 2026.

— TR_KA-3: se necessario durante il rilascio, un'unità di portafoglio deve includere un attestato di chiave nel campo "proofs" [prove] di una richiesta di credenziali inviata all'entità che rilascia le credenziali, come specificato nell'OID4VCI, in una prova del tipo "jwt" o del tipo "attestation" [attestato];

— TR_KA_3.1: se un'unità di portafoglio include un attestato di chiave in un elemento "jwt", deve firmare o sigillare l'attestato di chiave utilizzando la chiave privata corrispondente alla chiave pubblica all'indice 0 dell'array "attested_keys" [chiavi attestate] all'interno dell'oggetto "key_attestation" [attestato di chiave];

— TR_KA-4: quando rilascia credenziali associate a un dispositivo, l'entità che rilascia le credenziali deve indicare nel parametro "proof_types_supported" [tipi di prove supportati] nei suoi metadati delle credenziali dell'entità che le rilascia, come specificato nella sezione 12.2.4 dell'OID4VCI, che supporta sia il tipo di prova "jwt" che il tipo di prova "attestation" per gli attestati di chiave che devono includere l'oggetto "key_attestation_required" [attestato di chiave necessario];

— TR_KA-4.1: se rilascia credenziali non associate a un dispositivo, l'entità che rilascia le credenziali deve omettere i parametri "proof_types_supported" e "cryptographic_binding_methods_supported" [metodi di associazione crittografica supportati] nei metadati dell'entità che rilascia le credenziali;

— TR_KA-5: se riceve un attestato di chiave in un tipo di prova "jwt" o "attestation", l'entità che rilascia le credenziali deve verificare la firma dell'attestato di chiave tramite la chiave pubblica presente nel certificato di firma incluso nel parametro "x5c" nell'intestazione JOSE dell'attestato di chiave, così come che tale certificato di firma sia associato a un'ancora di fiducia presente nell'elenco dei fornitori di portafogli, di cui all'articolo 5 del regolamento di esecuzione (UE) 2024/2980, utilizzando potenzialmente certificati intermedi inclusi nel parametro "x5c";

— TR_KA-6: se un'entità che rilascia le credenziali riceve un attestato di chiave in un tipo di prova "jwt", deve verificare la firma dell'elemento "jwt" tramite la chiave all'indice 0 dell'array "attested_keys" all'interno dell'oggetto "key_attestation" incluso nell'elemento "jwt";

— TR_KA-6.1: l'entità che rilascia le credenziali deve verificare che nel campo "nonce" dell'elemento "jwt" figuri un c_nonce valido risultante dal relativo nonce_endpoint, come specificato nell'OID4VCI;

— TR_KA-7: se un'entità che rilascia le credenziali riceve un attestato di chiave in un tipo di prova "attestation", deve verificare che l'oggetto "key_attestation" includa un c_nonce valido risultante dal relativo nonce_endpoint;

— TR_KA-8: un fornitore di dati di identificazione personale deve garantire che i dati di identificazione personale siano associati a una chiave pubblica che proviene da un attestato di chiave il quale menziona un WSCD.

(c) Requisiti in materia di contenuto

— C_WIA-1: in un attestato di istanza di portafoglio deve figurare quanto segue:

— la dichiarazione "wallet_name" [nome portafoglio] specificata nell'appendice E dell'OID4VCI, in cui il suo valore deve essere l'identificatore della soluzione di portafoglio reperibile nell'elenco dei fornitori di portafogli di cui all'articolo 5 del regolamento di esecuzione (UE) 2024/2980;

— una dichiarazione "wallet_version" ([4])[versione del portafoglio], che deve essere una stringa il cui valore deve essere la versione della soluzione di portafoglio;

— una dichiarazione "wallet_solution_certification_information" [informazioni sulla certificazione della soluzione di portafoglio], che deve essere un oggetto JSON contenente informazioni in merito all'organismo di valutazione della conformità che ha certificato la soluzione di portafoglio, il numero di certificazione, a seconda dei casi, e altri dettagli pertinenti per quanto concerne la certificazione;

([4]) Questa dichiarazione è definita nel presente regolamento di esecuzione della Commissione dato che non costituisce parte della specifica OID4VCI.

— una dichiarazione “client_status” [stato del client], contenente due sottocampi:

— “status”: un riferimento all’elenco di stato di cui all’appendice E dell’OID4VCI che rappresenta lo stato di revoca dell’istanza di portafoglio. Per il dettaglio cfr. sezione e);

— “exp”: una NumericDate [data in formato numerico], come specificata nell’RFC 7519, che definisce il termine fino al quale il fornitore del portafoglio manterrà lo stato di revoca nell’indice dell’elenco degli stati di cui alla voce “status”;

— la dichiarazione “exp” specificata nell’appendice E dell’OID4VCI;

— NOTA: la dichiarazione “client_status.status” [stato dello stato del client] in un attestato di istanza di portafoglio rappresenta lo stato di revoca dell’istanza di portafoglio, non lo stato di revoca dell’attestato stesso. Come descritto alla voce R_WIA-1, un fornitore del portafoglio può decidere di circoscrivere l’ambito di ciascun attestato di istanza di portafoglio a uno specifico server di autorizzazione sulla base del fatto che tutti gli attestati inviati a tale server contengono lo stesso valore di indice nella voce “client_status.status”;

— NOTA: il valore “idx” [indice] nella dichiarazione “status” può essere utilizzato come identificatore univoco (a coppie) dell’istanza di portafoglio e dell’unità di portafoglio;

— C_WIA-2: un attestato di istanza di portafoglio dovrebbe includere anche la dichiarazione “wallet_link” [collegamento al portafoglio] specificata nell’appendice E dell’OID4VCI e il valore di tale dichiarazione deve essere un URI al quale è possibile ottenere ulteriori informazioni in merito alla soluzione di portafoglio;

— C_WIA-3: un server di autorizzazione non deve interpretare il parametro “exp” nel primo livello di un attestato di istanza di portafoglio come la fine del periodo di mantenimento della revoca dell’istanza di portafoglio;

— NOTA: il parametro “exp” nel primo livello di un attestato di istanza di portafoglio indica la data di scadenza dell’attestato stesso;

— C_KA-1: in un attestato di chiave devono figurare:

— le dichiarazioni “key_storage” [conservazione chiave] e “user_authentication” [autenticazione utente] specificate nell’appendice D dell’OID4VCI;

— gli attributi “key_storage” e “user_authentication” devono avere il valore “iso_18045_high” [ISO 18045 elevato] quando un attestato di chiave menziona un WSCD;

— la dichiarazione “certification” [certificazione] di cui all’appendice D dell’OID4VCI, contenente un URL dal quale possono essere ottenute informazioni in merito alla certificazione ottenuta dal WSCD o dal keystore, indicativamente il regime come Common Criteria [criteri comuni] o GlobalPlatform [piattaforma globale], i requisiti valutati, quali il profilo di protezione applicabile, e il livello di valutazione;

— a partire da tali informazioni deve essere possibile stabilire se il sistema di conservazione della chiave è un WSCD;

— una dichiarazione “key_storage_status” [stato conservazione chiave], contenente due sottocampi:

— “status”: un riferimento all’elenco degli stati di cui all’appendice D.1 dell’OID4VCI. Il valore rappresenta lo stato di revoca del WSCD o del tipo di keystore utilizzato per conservare le chiavi attestate oppure, nell’opzione “per-key-attestation index” [indice di attestato per singola chiave], lo stato di revoca di un WSCD o di un keystore di una singola unità di portafoglio. Cfr. R_KA_1 per le opzioni disponibili per l’assegnazione di indici;

— “exp”: una NumericDate [data in formato numerico], come specificata nell’RFC 7519, che definisce il termine fino al quale il fornitore del portafoglio manterrà lo stato di revoca nell’indice dell’elenco degli stati di cui alla voce “status”;

— la dichiarazione “exp” di cui all’appendice D dell’OID4VCI;

— NOTA relativa al valore “idx” nella dichiarazione “key_storage_status.status” [stato dello stato conservazione chiave] in un attestato di chiave: se il fornitore del portafoglio utilizza l’opzione “type-shared index” [indice condiviso per tipo] (cfr. R_KA_1), tutti gli attestati di chiave per lo stesso tipo di WSCD o di keystore condividono lo stesso indice dell’elenco degli stati. Pertanto il valore “idx” non è univoco per singola unità di portafoglio. Al contrario, se il fornitore del portafoglio utilizza l’opzione “per-key-attestation index”, il valore “idx” è univoco per l’unità di portafoglio (o univoco a coppie per singola entità che rilascia le credenziali). In tutti i casi, tuttavia, un’entità che rilascia le credenziali non deve utilizzare il valore “idx” in un attestato di chiave come identificatore di unità di portafoglio, ma deve utilizzare piuttosto il valore “idx” in un attestato di istanza di portafoglio;

— C_KA-2: se un attestato di chiave è inviato con un tipo di prova “attestation”, deve includere anche un c_nonce valido di cui all’appendice F.3 dell’OID4VCI;

— C_KA-3: un’entità che rilascia le credenziali non deve interpretare il parametro “exp” nel primo livello di un attestato di chiave come la fine del periodo di mantenimento della revoca del WSCD o del keystore;

— NOTA: il parametro “exp” nel primo livello di un attestato di chiave indica la data di scadenza dell’attestato stesso.

(d) Requisiti in materia di ciclo di vita

— Il presente allegato specifica i parametri seguenti dei metadati dell’entità che rilascia le credenziali:

— “preferred_client_status_period”: OPTIONAL. [periodo preferito stato cliente. FACOLTATIVO]. Un numero intero che specifica il periodo residuo preferito di mantenimento dello stato dell’attestato di istanza di portafoglio che deve essere presentato dall’unità di portafoglio durante il rilascio, in secondi. Il periodo residuo di mantenimento dello stato è definito come il valore di “client_status.exp” [scadenza stato client] nell’attestato da cui viene sottratto il momento di ricezione dell’attestato;

— “preferred_key_storage_status_period”: OPTIONAL. [periodo preferito stato conservazione chiave. FACOLTATIVO]. Un numero intero che specifica il periodo residuo preferito di mantenimento dello stato dell’attestato di chiave che deve essere presentato dall’unità di portafoglio durante il rilascio, in secondi. Il periodo residuo di mantenimento dello stato è definito come il valore “key_storage_status.exp” [scadenza stato conservazione chiave] nell’attestato da cui viene sottratto il momento di ricezione dell’attestato;

— LC_WIA-1: un server di autorizzazione può comunicare le proprie preferenze per il periodo residuo di mantenimento dello stato negli attestati di istanza di portafoglio includendo il parametro dei metadati “preferred_client_status_period” nel relativo endpoint di metadati dell’entità che rilascia le credenziali, di cui alla sezione 12.2.2 dell’OID4VCI;

— LC_WIA-1.1: questo campo deve essere collocato al primo livello dei metadati dell’entità che rilascia le credenziali;

— LC_WIA_2: un server di autorizzazione non deve interpretare il parametro “exp” nel primo livello di un attestato di istanza di portafoglio come la fine del periodo di mantenimento della revoca dell’istanza di portafoglio;

— LC_WIA_3: se firma o sigilla un attestato di istanza di portafoglio, il fornitore del portafoglio deve mantenere in vigore lo stato di revoca dell’istanza di portafoglio in questione fino alla scadenza indicata nel campo “wallet_instance_status.exp” [scadenza stato istanza di portafoglio] che figura in tale attestato di istanza di portafoglio;

— LC_KA-1: se è necessario un attestato di chiave, un’entità che rilascia le credenziali può comunicare le proprie preferenze per il periodo residuo di mantenimento dello stato negli attestati di chiave includendo il parametro dei metadati “preferred_key_storage_status_period” di cui sopra nel relativo endpoint dei metadati dell’entità che rilascia le credenziali come specificato alla sezione 12.2.2 dell’OID4VCI;

— LC_KA-1.1: questo campo deve essere collocato all’interno dell’oggetto “key_attestations_required” come specificato alla sezione 12.2.4 dell’OID4VCI;

— LC_KA-2: un fornitore del portafoglio deve scegliere il periodo di validità tecnica degli attestati di chiave che rilascia;

— LC_KA-3: se firma o sigilla un attestato di chiave, il fornitore del portafoglio deve mantenere in vigore lo stato di revoca del WSCD pertinente o del keystore pertinente fino alla scadenza del termine "key_storage_status.exp" indicato in tale attestato di chiave;

— LC_GEN-1: un fornitore del portafoglio deve garantire che un'unità di portafoglio possa sempre presentare attestati di unità di portafoglio e attestati di chiave i cui valori "client_status.exp" e "key_storage_status.exp" (rispettivamente) siano fissati ad almeno 31 giorni nel futuro rispetto al momento della presentazione a un server di autorizzazione o a un'entità che rilascia le credenziali;

— *NOTA*: ciò garantisce che i fornitori di dati di identificazione personale possano fare affidamento sul concatenamento delle revoche senza essere costretti a rilasciare dati di identificazione personale di breve durata;

— LC_GEN-2: un fornitore del portafoglio deve garantire che un'unità di portafoglio recuperi i metadati dell'entità che rilascia le credenziali durante il rilascio;

  — LC_GEN_2.1: se tra tali metadati figura un campo "preferred_key_storage_status_period", l'unità di portafoglio deve inviare un attestato di chiave indicando un valore ("key_storage_status.exp" – momento attuale) – "preferred_key_storage_status_period" il più basso possibile ma non negativo. Qualora non sia disponibile un tale attestato di chiave, l'unità di portafoglio deve ottenere un nuovo attestato di chiave dal fornitore del portafoglio che soddisfi la condizione: "key_storage_-status.exp" – momento attuale ≥ "preferred_key_storage_status_period";

  — LC_GEN_2.2: se tra tali metadati figura un campo "preferred_client_status_period", l'unità di portafoglio deve inviare un attestato di istanza di portafoglio recante un valore ("client_status.exp" – momento attuale) – "preferred_client_status_period" il più basso possibile ma non negativo. Qualora non sia disponibile un tale attestato di istanza di portafoglio, l'unità di portafoglio deve richiedere al fornitore del portafoglio un nuovo attestato di istanza di portafoglio che soddisfi la condizione: "client_status.exp" – momento attuale ≥ "preferred_client_status_period";

— LC_GEN-3: il periodo di validità tecnica dei dati di identificazione personale deve terminare prima tanto del termine di cui al campo "client_status.exp" dell'attestato di istanza di portafoglio quanto di quello di cui al campo "key_storage_status.exp" dell'attestato di chiave inviato al fornitore di dati di identificazione personale nel contesto della procedura di rilascio;

— LC_GEN-4: un fornitore di dati di identificazione personale con un periodo di validità tecnica superiore a 24 ore deve verificare lo stato di revoca tanto dell'attestato di istanza di portafoglio quanto dell'attestato di chiave ricevuto durante il rilascio almeno una volta ogni 24 ore, durante il periodo di validità tecnica dei dati di identificazione personale. In caso di revoca di uno dei due attestati, il fornitore deve revocare i dati di identificazione personale.

(e) Prescrizioni in materia di revoca

— R_GEN-1: un fornitore del portafoglio deve utilizzare gli elenchi degli stati dei token (specificati nell'elenco degli stati dei token dell'IETF) come meccanismo di revoca tanto per gli attestati di chiave quanto per gli attestati di istanza di portafoglio, come specificato rispettivamente nelle appendici D ed E dell'OID4VCI;

— NOTA: al fine di migliorare la scalabilità dei suoi elenchi degli stati, un fornitore del portafoglio può utilizzare le ottimizzazioni seguenti:

  — suddivisione dell'elenco degli stati in più pacchetti, laddove i fornitori di portafogli abbiano un numero considerevole di utenti e abbiano rilasciato attestati. Esistono numerose strategie di suddivisione in pacchetti, ad esempio basate su una dimensione fissa o su un periodo di tempo. La strategia per la suddivisione in pacchetti è lasciata alla discrezione del fornitore del portafoglio. Possono essere prese in considerazione anche le dimensioni di un elenco degli stati per fini di scaricamento e la tutela della vita privata dell'utente;

  — gestione di più elenchi degli stati;

  — compressione di un elenco degli stati per ridurne le dimensioni;

— R_WIA-1: un fornitore del portafoglio può assegnare il medesimo valore alla dichiarazione “idx” nella dichiarazione “client_status.status” in tutti gli attestati di istanza di portafoglio che una determinata unità di portafoglio presenta allo stesso server di autorizzazione. Si tratta in questo caso dell’opzione “per-issuer reuse”. Qualora si ricorra a tale opzione:

  — R_WIA-1.1: l’unità di portafoglio deve tenere traccia del valore di indice utilizzato per ciascun server di autorizzazione con cui ha precedentemente interagito e deve richiedere un attestato di istanza di portafoglio contenente lo stesso valore di indice quando interagisce nuovamente con il medesimo server di autorizzazione;

  — R_WIA-1.2: se riceve una richiesta di attestato di istanza di portafoglio contenente un valore di indice specifico, un fornitore del portafoglio deve verificare che l’unità di portafoglio richiedente abbia ricevuto tale valore di indice in precedenza, prima di rilasciare un nuovo attestato di istanza di portafoglio con tale valore di indice;

  — R_WIA-1.3: l’unità di portafoglio non deve riutilizzare lo stesso valore di indice per interazioni con server di autorizzazione diversi;

— NOTA: se si utilizza l’opzione “per-issuer reuse”, il fornitore del portafoglio sarà in grado di determinare con quanti server di autorizzazione un’unità di portafoglio ha interagito e con quale frequenza interagisce con ciascuno di essi;

— R_WIA-2: nella sua politica in materia di tutela della vita privata, un fornitore del portafoglio deve documentare se fa o meno ricorso all’opzione “per-issuer reuse” per la revoca dell’istanza di portafoglio;

— R_WIA-3: se un fornitore del portafoglio non si avvale dell’opzione “per-issuer reuse”, il fornitore del portafoglio deve assegnare a ciascun attestato di istanza di portafoglio che rilascia un valore di indice nuovo non collegabile;

— R_WIA-4: se un’unità di portafoglio deve essere revocata, un fornitore del portafoglio deve revocare i valori di indice nella dichiarazione “client_status.status” in tutti gli attestati di istanza di portafoglio associati a tale unità di portafoglio;

— R_WIA-5: un fornitore del portafoglio deve tenere conto della portata della sua diffusione e dell’architettura sottostante nel determinare le dimensioni dei suoi elenchi degli stati di attestati di istanza di portafoglio, garantendo che siano sufficientemente ampie da prevenire correlazioni e da proteggere la vita privata degli utenti. Ove possibile, un elenco degli stati deve riguardare almeno 10 000 attestati;

— R_KA_1: un fornitore del portafoglio deve scegliere una delle opzioni seguenti di assegnazione dell’indice per la dichiarazione “key_storage_status.status” in un attestato di chiave:

  — opzione 1, denominata “type-shared index”, nel contesto della quale tutti gli attestati di chiave che attestano chiavi conservate nello stesso tipo di WSCD o di keystore contengono lo stesso valore di indice nel campo “key_storage_status.status”;

  — opzione 2, denominata “per-key-attestation index” [indice attestato per singola chiave], nel contesto della quale un attestato di chiave che attesta chiavi conservate in un WSCD o in un keystore individuale contiene un valore di indice univoco (a coppie) nel campo “key_storage_status.status”;

— NOTA: se un fornitore del portafoglio utilizza l’opzione 1, un’unica azione di revoca invalida tutti gli attestati di chiave del tipo interessato in tutte le unità di portafoglio. Inoltre, dato che tutti gli attestati di chiave per lo stesso tipo di WSCD o di keystore condividono un unico indice dell’elenco degli stati, il numero di voci in un elenco degli stati di attestati di chiave rispecchia il numero di tipi di WSCD o di keystore supportati dal fornitore del portafoglio, non il numero di unità di portafoglio installate. Le considerazioni in materia di tutela della vita privata che motivano le dimensioni minime dell’elenco degli stati per gli elenchi degli stati di istanze di portafoglio non si applicano pertanto agli elenchi degli stati di attestati di chiave di cui all’opzione 1, a condizione che vi sia un numero sufficiente di unità di portafoglio che utilizzano lo stesso tipo di WSCD o di keystore;

— NOTA: se un fornitore del portafoglio utilizza l’opzione 2, ciascun indice rappresenta lo stato di revoca del WSCD o del keystore specifico attestato in tale attestato di chiave;

— NOTA: se un fornitore del portafoglio si avvale dell’opzione 2, su richiesta dell’utente può essere revocato anche un WSCD o un keystore specifico;

— R_KA-2: se si avvale dell'opzione 2, il fornitore del portafoglio può utilizzare facoltativamente l'opzione "per-issuer reuse" descritta alla voce R_WIA-1. Se il fornitore del portafoglio ricorre a tale opzione, si devono applicare mutatis mutandis i requisiti di cui alle voci da R_WIA-1 a R_WIA-3;

— R_KA-3: se si avvale dell'opzione 2, il fornitore del portafoglio deve tenere conto della portata della sua diffusione e dell'architettura sottostante nel determinare le dimensioni dei suoi elenchi degli stati di attestati di chiave, garantendo che siano sufficientemente ampie da prevenire correlazioni e proteggere la vita privata degli utenti. Ove possibile, un elenco degli stati deve riguardare almeno 10 000 attestati di chiave;

— R_KA-4: se utilizza l'opzione 1 (indice condiviso per tipo), il fornitore del portafoglio deve revocare una voce "key_storage_status.status" soltanto se il tipo di WSCD o di keystore presenta una vulnerabilità in termini di sicurezza.

(f) Requisiti in materia di algoritmi di firma

— SA-1: per firmare gli attestati di istanza di portafoglio, gli attestati di chiave, le relative prove di possesso e gli elenchi degli stati dei token, occorre impiegare uno degli algoritmi seguenti:

  — ES256 (ECDSA con SHA-256 e P-256)

  — ES384 (ECDSA con SHA-384 e P-384)

  — ES512 (ECDSA con SHA-512 e P-521)

— SA-2: un fornitore del portafoglio deve scegliere quale degli algoritmi di cui al punto SA-1 utilizzerà;

— SA-3: un server di autorizzazione o un'entità che rilascia le credenziali (come specificato nell'OID4VCI) deve supportare tutti gli algoritmi di cui al punto SA-1.»

ALLEGATO IV

«*ALLEGATO II*

Elenco delle norme di cui all'articolo 8

Si applicano le specifiche tecniche di cui ai punti da 2 a 6 della norma ETSI TS 119 472-1 V1.2.1 (2026-02). Tali specifiche vanno lette considerando gli adattamenti seguenti:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* Parte 1: *Overview and common data structures*;

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles;* Parte 6: *Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers*;

— [25] Elenco degli stati dei token dell'IETF (TSL), draft-ietf-oauth-status-list-20: *Token Status List*, 20 aprile 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: quando un elemento di stato è utilizzato per dati di identificazione personale, attestati elettronici di attributi qualificati o attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto, detto elemento deve indicare soltanto se l'attestato è revocato o meno e non deve supportare altri valori di stato quali una sospensione;

— EAA-4.2.11.1-06.1: in caso di revoca di un attestato, quest'ultimo deve essere revocato in via definitiva.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: in caso di rilascio di attestati elettronici di attributi di breve durata con un periodo di validità pari o inferiore a 24 ore, la revoca non deve essere richiesta.

4) 4.6.3 requisiti per attestati elettronici di attributi (EAA – *electronic attestation of attributes*) dell'UE rilasciati da o per conto di un organismo pubblico responsabile di una fonte autentica (PuB-EAA)

— PuB-EAA-4.6.2-03: void.

— Pub-EAA-4.6.2-04: void.

— PuB-EAA-4.6.3-03: La firma digitale PuB-EAA dovrebbe contenere il certificato qualificato a sostegno della firma digitale PuB-EAA.

— PuB-EAA-4.6.3-04: Il certificato qualificato a sostegno della firma digitale PuB-EAA deve soddisfare i requisiti di cui al punto 8 della norma ETSI TS 119 412-6 v1.1.1 e deve contenere la dichiarazione QcType QcStatement quale definita nella norma ETSI EN 319 412-5 v2.5.1, con il valore id-etsi-qct-eidaspsbeaa definito come segue:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificato di cui all'articolo 45 septies, paragrafo 1, lettera b), a sostegno della firma elettronica qualificata o del sigillo elettronico qualificato dell'organismo del settore pubblico di cui all'articolo 3, punto 46), del regolamento (UE) n. 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: void.

— EAA-5.2.10.1-05: void.

— EAA-5.2.10.1-06: Il membro "status" può contenere il membro status_list come specificato al punto 6.2 del draft-ietf-oauth-status-list-20 dell'IETF [25].

— EAA-5.2.10.1-07: void.

— EAA-5.2.10.1-08: void.

— EAA-5.2.10.1-09: void.

— EAA-5.2.10.1-10: void.

— EAA-5.2.10.1-11: void.

— EAA-5.2.10.1-12: void.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: quando un attestato elettronico di attributi conforme alla norma ISO/IEC mdoc utilizza il meccanismo dell'elenco degli stati di attestati di cui all'EAA-6.2.10.1-02.2 o il meccanismo dell'elenco delle revoche di attestati di cui all'EAA-6.2.10.1-02.3, il relativo oggetto di sicurezza mobile ("MSO" – *Mobile Security Object*) deve contenere la struttura di stato, di cui all'EAA-6.2.10.1-17, che contiene informazioni in merito alla revoca dell'MSO;

— EAA-6.2.10.1-01.1: nell'attuare il meccanismo dell'elenco degli identificatori, l'elemento di stato deve contenere l'elemento identifier_list [elenco identificatori] di cui all'EAA-6.2.10.1-11;

— EAA-6.2.10.1-01.2: nell'attuare il meccanismo dell'elenco degli stati, l'elemento di stato deve contenere l'elemento status_list [elenco stati] di cui all'EAA-6.2.10.1-13;

— *NOTA:*

  — la struttura dello stato contiene un riferimento a un elenco delle revoche dell'MSO;

  — l'elenco delle revoche dell'MSO è una struttura COSE_Sign1 che indica se uno specifico MSO è revocato o meno;

  — la struttura dello stato contiene tutte le informazioni necessarie alla parte facente affidamento sul portafoglio affinché essa possa stabilire l'autenticità o meno dell'elenco delle revoche dell'MSO;

— EAA-6.2.10.1-02: il fornitore di dati di identificazione personale, il fornitore di attestati elettronici di attributi qualificati o il fornitore di attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto deve utilizzare uno dei metodi seguenti per la revoca dei dati di identificazione personale, degli attestati elettronici di attributi qualificati o degli attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto:

— EAA-6.2.10.1-02.1: se rilasciano attestati elettronici di attributi di breve durata aventi un periodo di validità pari o inferiore a 24 ore, la revoca non deve essere richiesta;

— EAA-6.2.10.1-02.2: utilizzare un meccanismo dell'elenco degli stati di attestati per codificare le informazioni in merito alla revoca come un elenco degli stati;

— EAA-6.2.10.1-02.2.1: il meccanismo dell'elenco degli stati revoca un MSO in base all'eventualità o meno che il bit nella posizione definita dall'entità che effettua il rilascio nell'MSO sia impostato su "vero" nell'elenco degli stati;

— EAA-6.2.10.1-02.2.2: il meccanismo dell'elenco degli stati è definito in dettaglio nella specifica relativa all'elenco degli stati dei token (draft-ietf-oauth-status-list-20);

— EAA-6.2.10.1-02.3: utilizzare un meccanismo dell'elenco delle revoche di attestati per codificare le informazioni in merito alla revoca come un elenco di identificatori;

— EAA-6.2.10.1-02.3.1: il meccanismo dell'elenco degli identificatori revoca un MSO in base all'eventualità o meno che l'identificatore definito dall'entità che effettua il rilascio nell'MSO sia presente nell'elenco degli identificatori;

— EAA-6.2.10.1-02.3.2: i requisiti EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 ed EAA-6.2.10.1-11 specificano il meccanismo dell'elenco degli identificatori, sulla base dei requisiti della specifica relativa all'elenco degli stati dei token, compresi gli aspetti comuni tra il meccanismo dell'elenco degli stati e il meccanismo dell'elenco degli identificatori;

— EAA-6.2.10.1-03: quando un elemento di stato è utilizzato per dati di identificazione personale, attestati elettronici di attributi qualificati o attestati elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto, si deve utilizzare esclusivamente lo stato "revoked" [revocato];

— EAA-6.2.10.1-03.1: per un elenco degli stati ciò implica che devono essere utilizzati soltanto i valori "valid" [valido] e "invalid" [non valido] di cui alla specifica relativa all'elenco degli stati dei token;

— EAA-6.2.10.1-03.2: per l'elenco degli identificatori, soltanto gli MSO revocati, anziché quelli temporaneamente sospesi, devono essere inseriti nell'elenco degli identificatori;

— EAA-6.2.10.1-04: in caso di revoca di un MSO, quest'ultimo deve essere revocato in via definitiva;

— EAA-6.2.10.1-05: la verifica dell'elenco delle revoche di MSO è facoltativa per la parte facente affidamento sul portafoglio e, se del caso, la verifica deve essere conforme ai requisiti di verifica di cui alla specifica relativa all'elenco degli stati dei token e ai requisiti in materia di struttura di stato di cui all'EAA-6.2.10.1-01;

— EAA-6.2.10.1-05.1: se una parte facente affidamento sul portafoglio deve essere in grado di verificare lo stato di revoca dei dati di identificazione personale o degli attestati elettronici di attributi, essa deve supportare tanto il meccanismo dell'elenco degli stati di attestati quanto il meccanismo dell'elenco delle revoche di attestati di cui all'EAA-6.2.10.1-02;

— EAA-6.2.10.1-06: i campi identifier_list e status_list nell'MSO possono contenere l'elemento del certificato;

— EAA-6.2.10.1-06.1: se l'elemento del certificato è presente, vi deve figurare un certificato contenente la chiave pubblica che ha firmato o sigillato il certificato di primo livello nell'elemento x5chain nella struttura dell'elenco delle revoche dell'MSO;

— EAA-6.2.10.1-06.1.1: l'istanza della parte facente affidamento sul portafoglio deve utilizzare tale certificato come ancora di fiducia per la verifica dell'elemento x5chain nella struttura dell'elenco delle revoche dell'MSO;

— EAA-6.2.10.1-06.2: se l'elemento del certificato non è presente, il certificato di primo livello dell'elemento x5chain nella struttura dell'elenco delle revoche dell'MSO deve essere firmato o sigillato tramite il certificato utilizzato per firmare il certificato nell'elemento x5chain dell'MSO;

— EAA-6.2.10.1-06.2.1: l'istanza della parte facente affidamento sul portafoglio deve utilizzare tale certificato come ancora di fiducia per la verifica dell'elemento x5chain nella struttura dell'elenco delle revoche dell'MSO;

— EAA-6.2.10.1-07: un elenco delle revoche dell'MSO deve essere attuato conformemente alla specifica relativa all'elenco degli stati dei token come token dell'elenco degli stati in formato CWT;

— EAA-6.2.10.1-08: per l'elenco delle revoche dell'MSO per il meccanismo dell'elenco degli identificatori e il meccanismo dell'elenco degli stati, si applicano i requisiti seguenti:

  — deve essere presente la dichiarazione "exp";

  — può essere presente la dichiarazione "ttl";

  — la dichiarazione "aggregation_uri" [URI aggregazione] nell'ambito della dichiarazione IdentifierList [elenco identificatori] o StatusList [elenco stati] può essere presente e il fornitore di dati di identificazione personale, il fornitore di attestati elettronici di attributi qualificati o il fornitore di attestati

elettronici di attributi forniti da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto può utilizzare la dichiarazione "aggregation_uri" per indicare il sostegno al meccanismo di aggregazione di cui alla specifica relativa all'elenco degli stati dei token;

— il CWT deve essere un oggetto COSE_Sign1 che utilizza uno degli algoritmi di firma seguenti per calcolare la firma:

(a) "ES256" (ECDSA con curva NIST P-256 e SHA-256);

(b) "ES384" (ECDSA con curva NIST P-384 e SHA-384);

(c) "ES512" (ECDSA con curva NIST P-521 e SHA-512);

(d) "ESB256" (ECDSA con curva brainpoolP256r1 e SHA-256);

(e) "ESB384" (ECDSA con curva brainpoolP384r1 e SHA-384);

(f) "ESB512" (ECDSA con curva brainpoolP512r1 e SHA-512);

— nel CWT deve figurare il campo x5chain nell'intestazione protetta che contiene il certificato o la catena di certificati ai fini della verifica della firma dell'elenco delle revoche dell'MSO;

— l'utilizzo esteso della chiave dell'identificatore dell'oggetto di cui alla specifica relativa all'elenco degli stati dei token può essere impiegato per l'elenco degli stati e il certificato di firma dell'elenco degli identificatori e le istanze della parte facente affidamento sul portafoglio possono supportare l'utilizzo esteso della chiave degli identificatori degli oggetti di cui alla specifica relativa all'elenco degli stati dei token e, per l'identificatore dell'oggetto, il fornitore di attestati elettronici qualificati di attributi o il fornitore di attestati elettronici di attributi forniti da un organismo del settore pubblico o per suo conto non devono rendere critico il campo relativo all'utilizzo esteso della chiave quando si ricorre all'OID per l'utilizzo esteso della chiave di cui alla specifica relativa all'elenco degli stati dei token;

— EAA-6.2.10.1-09: in deroga ai requisiti di cui alla specifica relativa all'elenco degli stati dei token, per il meccanismo dell'elenco degli identificatori si applicano i requisiti seguenti:

— il valore della dichiarazione "type" [tipo] deve essere "application/identifierlist+cwt";

— la dichiarazione "StatusList" non deve essere presente nella serie di dichiarazioni CWT;

— la struttura di "IdentifierList" definita nell'EAA-6.2.10.1-11 deve essere presente come dichiarazione nella serie di dichiarazioni CWT, con l'utilizzo della chiave 65530;

— EAA-6.2.10.1-10: la struttura di "IdentifierList" deve essere una struttura CBOR avente la notazione CDDL seguente:

```
IdentifierList = {

    "identifiers": { * Identifier => IdentifierInfo },

    ? "aggregation_uri": Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: se è presente l'identificatore nell'elemento "IdentifierList", l'MSO che contiene l'identificatore nell'elemento di stato è revocato;

— EAA-6.2.10.1-10.2: la dichiarazione "Aggregation_uri" è specificata nella sezione 9.2 della specifica relativa all'elenco degli stati dei token;

— EAA-6.2.10.1-10.3: il tipo di contenuto dell'elenco degli identificatori deve essere "application/identifierlist +cwt" come indicato nei requisiti di cui alla sezione 8.2 della specifica relativa all'elenco degli stati dei token;

— EAA-6.2.10.1-11: all'elemento "identifier_list" nell'MSO si applicano i requisiti seguenti (cfr. EAA-6.2.10.1-17);

— EAA-6.2.10.1-11.1: l'elemento "identifier_list" è una struttura CBOR avente la notazione CDDL seguente:

```
IdentifierListInfo = {

        "id": Identifier ,

        "uri": URI,

        ? "certificate": Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: al fine di evitare che sia utilizzato come correlazione tra presentazioni, l'identificatore deve essere univoco per ciascun MSO;

— EAA-6.2.10.1-12: all'elenco degli stati si applicano i requisiti seguenti:

  — EAA-6.2.10.1-12.1: l'elemento "bits" [bit] nella struttura "StatusList" deve essere impostato su 1;

— EAA-6.2.10.1-13: i requisiti seguenti si applicano all'elemento "status_list" nell'MSO (cfr. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: l'elemento "status_list" deve seguire i requisiti per la struttura "StatusListInfo" [informazioni elenco stati] di cui alla specifica relativa all'elenco degli stati dei token e deve essere aggiunto l'elemento facoltativo del certificato definito nell'EAA-6.2.10.1-06;

  — EAA-6.2.10.1-13.2: al fine di evitare che l'indice di stato sia una correlazione tra presentazioni, la combinazione di indice di stato e URI deve essere univoca per ciascun MSO;

— EAA-6.2.10.1-14: il fornitore del portafoglio deve utilizzare il secondo (EAA-6.2.10.1-02.2) o il terzo (EAA-6.2.10.1-02.3) dei metodi specificati nell'EAA-6.2.10.1-02 per la revoca di un attestato di istanza di portafoglio (WIA – *wallet instance attestation*) o per la revoca di un attestato di chiave (KA – *key attestation*);

— EAA-6.2.10.1-15: il fornitore del portafoglio deve attuare i meccanismi di revoca dell'attestato specificati nell'EAA-6.2.10.1-02 nella propria soluzione di portafoglio;

— EAA-6.2.10.1-16: il fornitore di dati di identificazione personale e il fornitore di attestati elettronici di attributi devono supportare tanto il meccanismo dell'elenco degli stati di attestati quanto il meccanismo dell'elenco delle revoche di attestati di cui all'EAA-6.2.10.1-02 ai fini della verifica dello stato di revoca di un attestato di istanza di portafoglio (WIA) e di un attestato di chiave (KA);

— EAA-6.2.10.1-17: la struttura di stato nell'MSO deve essere una struttura CBOR avente la notazione CDDL seguente:

Status = {

? “identifier_list”: IdentifierListInfo,

? “status_list”: StatusListInfo,

* tstr => RFU

}»

ALLEGATO V

«*ALLEGATO III*

Specifiche tecniche di cui all'articolo 10

— Specifiche tecniche:

  — punto 4.2.5 dell'ETSI TS 119 472-3 V1.1.1 (2026-03).»

ALLEGATO VI

L'allegato IV del regolamento di esecuzione (UE) 2024/2979 è così modificato:

1) il punto 1 è sostituito dal seguente:

«1. Formato obbligatorio per firme o sigilli:

a) PAdES (*PDF Advanced Electronic Signature*, firma elettronica avanzata per PDF) come specificato nella norma ETSI EN 319 142-1 V1.2.1 (2024-01); *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures;* Parte 1: *Building blocks and PAdES baseline signatures.*»;

2) il punto 3 è sostituito dal seguente:

«3. Interfaccia di programmazione di un'applicazione:
ETSI TS 119 432 v1.3.1 (2026-03) punti 6.4.3, A.6, A.7 e A.8.»

ALLEGATO VII

«ALLEGATO VI

Marchio di fiducia UE per i portafogli di identità digitale a colori



»

ALLEGATO VIII

«*ALLEGATO VII*

Marchio di fiducia UE per i portafogli di identità digitale in bianco e nero



»

ALLEGATO IX

«ALLEGATO VIII

Dati relativi al marchio di fiducia UE per i portafogli di identità digitale

Dati	Descrizione	Codifica	Stato
TrustMarkResourceURL	URL degli elementi grafici dei marchi di fiducia UE per i portafogli di identità digitale e risorse informative per gli utenti nell'interfaccia utente del portafoglio.	URL	Obbligatorio
ListOfCertifiedWalletsURL	URL dell'elenco pubblico delle soluzioni di portafoglio certificate nell'UE di cui al regolamento di esecuzione (UE) 2025/849 della Commissione ([1]).	URL	Obbligatorio
ListOfCertifiedWalletsQRCode	Codice QR contenente le informazioni di cui al dato ListOfCertifiedWalletsURL [URL dell'elenco dei portafogli certificati].	ISO-8859-1 Byte mode QR code	Facoltativo
WalletSolutionInfoPageURL	URL della pagina informativa della soluzione di portafoglio certificata nell'elenco della pagina delle soluzioni di portafoglio certificate ottenuto aggiungendo all'URL di cui al dato ListOfCertifiedWalletsURL un "?" e l'identificatore "WalletSolutionID" [identificatore della soluzione di portafoglio] della soluzione di portafoglio.	URL	Obbligatorio
WalletSolutionInfoPageQRCode	Codice QR contenente le informazioni di cui al dato WalletSolutionInfoPageURL [URL pagina informativa soluzioni di portafoglio].	ISO-8859-1 Byte mode QR code	Facoltativo
WalletVerifierToolURL*	URL dell'endpoint dello strumento di verifica dei portafogli */.well-known/ openid-credential-issuer* utilizzato per recuperare i metadati dei fornitori di attestati.	URL	Facoltativo.

([1]) Regolamento di esecuzione (UE) 2025/849 della Commissione, del 6 maggio 2025, recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda la trasmissione di informazioni alla Commissione e al gruppo di cooperazione in merito all'elenco dei portafogli europei di identità digitale certificati (GU L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).»

ALLEGATO X

L'allegato II del regolamento di esecuzione (UE) 2024/2980 è così modificato:

1) All'allegato II, sezione 1, punto 1, la lettera i) è sostituita dalla seguente:

«i) uno o più certificati conformi alla norma ETSI EN 319 412-2 V2.4.1 (2025-06) o alla norma ETSI EN 319 412-3 V1.3.1 (2023-09) che possono essere utilizzati per verificare la firma o il sigillo creati dal conservatore del registro sui dati del registro e per i quali i dati di identità certificati comprendono il nome del conservatore del registro e, se del caso, il numero di registrazione del conservatore del registro, come previsto rispettivamente alle lettere c) e d).»;

2) all'allegato II, sezione 2, punto 1, la lettera h) è sostituita dalla seguente:

«h) uno o più certificati conformi alla norma ETSI EN 319 412-2 V2.4.1 (2025-06) o alla norma ETSI EN 319 412-3 V1.3.1 (2023-09) che possono essere utilizzati per autenticare e convalidare gli attestati di unità di portafoglio rilasciati dal fornitore del portafoglio e per i quali i dati di identità certificati includono il nome e, se del caso, il numero di registrazione del fornitore del portafoglio, come specificato rispettivamente alle lettere a) e b);»;

3) all'allegato II, sezione 3, punto 1, la lettera h) è sostituita dalla seguente:

«h) uno o più certificati conformi alla norma ETSI EN 319 412-2 V2.4.1 (2025-06) o alla norma ETSI EN 319 412-3 V1.3.1 (2023-09) che possono essere utilizzati per verificare la firma o il sigillo creati dal fornitore di dati di identificazione personale sui dati di identificazione personale che fornisce e per i quali i dati di identità certificati comprendono il nome e, se del caso, il numero di registrazione del fornitore di dati di identificazione personale, come previsto rispettivamente alle lettere (a) e (b).»;

4) all'allegato II, sezione 4, punto 1, la lettera g) è sostituita dalla seguente:

«g) uno o più certificati conformi alla norma ETSI EN 319 412-2 V2.4.1 (2025-06) o alla norma ETSI EN 319 412-3 V1.3.1 (2023-09) che possono essere utilizzati per verificare la firma o il sigillo creato/a dal fornitore dei certificati di accesso delle parti facenti affidamento sul portafoglio sui certificati di accesso che fornisce alle parti facenti affidamento sul portafoglio, se del caso, unitamente alle informazioni necessarie per distinguere i certificati di accesso delle parti facenti affidamento sul portafoglio rispetto ad altri certificati.»;

5) nell'allegato II è aggiunta la sezione 5 come segue:

«5. Notifiche di informazioni sui fornitori di certificati di registrazione delle parti facenti affidamento sul portafoglio

1. Gli Stati membri forniscono alla Commissione le informazioni seguenti in merito ai fornitori di certificati di registrazione delle parti facenti affidamento sul portafoglio:

a) il nome del fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio;

b) se del caso, un numero di registrazione del fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio;

c) lo Stato membro in cui è stabilito il fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio;

d) l'indirizzo di posta elettronica di contatto e il numero di telefono di contatto del fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio per le questioni relative ai certificati di registrazione che fornisce alle parti facenti affidamento sul portafoglio;

e) se del caso, l'URL della pagina web del fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio contenente informazioni aggiuntive sul fornitore e sui certificati di registrazione che fornisce alle parti facenti affidamento sul portafoglio;

f) l'URL della pagina web contenente le politiche, i termini e le condizioni che si applicano alla fornitura e all'uso dei certificati di registrazione che fornisce alle parti facenti affidamento sul portafoglio;

g) uno o più certificati conformi alla norma ETSI EN 319 412-2 V2.4.1 (2025-06) o alla norma ETSI EN 319 412-3 V1.3.1 (2023-09) che possono essere utilizzati per verificare la firma o il sigillo creato/a dal fornitore dei certificati di registrazione delle parti facenti affidamento sul portafoglio sui certificati di registrazione che fornisce alle parti facenti affidamento sul portafoglio, se del caso, unitamente alle informazioni necessarie per distinguere i certificati di registrazione delle parti facenti affidamento sul portafoglio rispetto ad altri certificati.

2. Le informazioni di cui al punto 1 devono essere fornite per ciascun fornitore di certificati di registrazione delle parti facenti affidamento sul portafoglio.»

ALLEGATO XI

«ALLEGATO I

Protocolli e interfacce di cui all'articolo 4

Si applica la specifica tecnica ETSI TS 119 472-3 V1.1.1 (2026-03) con gli adeguamenti seguenti:

1) 4.1 General requirements

— GEN-REQ-4.1-05: void.

— NOTA: void.

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: uno degli elementi del parametro "issuer_info array deve contenere il certificato di registrazione del fornitore di informazioni di identificazione personale/attestati elettronici di attributi.

— ISS-MDATA-REG_CERT-4.2.3-07: void.

— ISS-MDATA-REG_CERT-4.2.3-08: void.

— ISS-MDATA-REG_CERT-4.2.3-09: void.

— ISS-MDATA-REG_CERT-4.2.3-10: void.

— ISS-MDATA-REG_CERT-4.2.3-11: void.

— ISS-MDATA-REG_CERT-4.2.3-12: void.

— ISS-MDATA-REG_CERT-4.2.3-13: void.

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: se il membro id ha il valore "arf_annex_ii" [ARF allegato II] e l'array mappato nell'etichetta "details" [dettagli] contiene il valore "once_only" [una volta soltanto] o il valore "per-relying-party" [per ciascuna parte facente affidamento], allora l'oggetto JSON che contiene tale array mappato nell'etichetta "details" deve contenere anche un numero JSON mappato nell'etichetta "reissue_trigger_unused" [attivatore di nuovo rilascio in caso di mancato utilizzo];

4) l'allegato A non si applica.»

ALLEGATO XII

«ALLEGATO II

Specifiche tecniche di cui all'articolo 5

Si deve applicare la specifica tecnica di cui all'allegato C della norma ISO/IEC 18013-7:2025.

Le specifiche tecniche di cui ai punti 4.1, 4.2, 5 e 6 della norma ETSI TS 119 472-2 V1.2.1 (2026-03) si devono applicare con gli adeguamenti seguenti, compreso l'inserimento di un nuovo punto 4.3:

1) 1 Scope

— Il presente documento specifica due profili di protocolli per consentire alle parti facenti affidamento (in appresso "RP" – *Relying Parties*) di richiedere presentazioni di attestati elettronici di attributi (in appresso "EAAPs" – *Presentations of Electronic Attestation of Attributes*) o dati di identificazione personale (in appresso: "PID" – *Personal Identification Data*) al portafoglio europeo di identità digitale e per consentire a quest'ultimo di inviare alle RP le EAAPs/PIDs richieste. Ciascuno dei profili supporta due meccanismi di trasmissione, ossia: mediato dall'interfaccia di programmazione di un'applicazione ("API" – *Application Programming Interface*) e non mediato dall'API, come illustrato di seguito:

(a) un profilo si basa su:

— ISO/IEC 18013-5 [10] solo per i meccanismi di trasmissione non mediati dall'API; e

— allegato C della norma ISO/IEC 18013-7 [16] per i meccanismi di trasmissione mediati dall'API.

Questo profilo è denominato profilo ISO/IEC-mdoc ed è definito al punto 5 del presente documento;

(b) un profilo si basa su:

OpenID4VC-HAIP [11] tanto per i meccanismi di trasmissione mediati dall'API quanto per quelli non mediati dall'API, come segue:

— sezioni 5, 5.1, 5.3, 7 e 8 di [11] per la trasmissione tramite reindirizzamenti o per i meccanismi di trasmissione non mediati dall'API; e

— sezioni 5, 5.2, 5.3, 7 e 8 di [11] per i meccanismi di trasmissione mediati dall'API.

Questo profilo è denominato profilo OpenID4VC-HAIP ed è definito al punto 6 del presente documento.

2) 2.1 Normative references

— [15] ISO 639: "Language code";

— [16] ISO/IEC 18013-7:2025 "*Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions*".

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: void.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: void.

— Note2: void.

— EAAP-ISO/IEC-mdoc-02: void.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: il portafoglio europeo di identità digitale deve supportare un'API di mediazione che supporta entrambi i protocolli di cui al punto 5.2 di [11] e nell'allegato C di [16].

— NOTA: se il dispositivo su cui è installato il portafoglio europeo di identità digitale non supporta entrambi i protocolli, tale requisito non può essere soddisfatto e determina una non conformità a causa dei sistemi operativi sottostanti e dei browser che non implementano le necessarie caratteristiche di interoperabilità.

— EAAP-API-GEN-02: il portafoglio europeo di identità digitale deve supportare un'API di mediazione almeno per i tipi di PID e EAA registrati nel catalogo di regimi di cui al regolamento di esecuzione (UE) 2025/1569 e almeno per tutti i formati di cui all'allegato II del regolamento di esecuzione (UE) 2024/2979.

— NOTA 1: se il sistema operativo sottostante, il browser, le API di mediazione o qualsiasi altro livello tecnico al di fuori del controllo del portafoglio europeo di identità digitale restringe/restringono, filtra/filtrano, preseleziona/preselezionano o limita/limitano in altro modo i formati delle credenziali e i tipi di PID e attestati elettronici di attributi registrati nel catalogo di regimi, questo requisito non può essere soddisfatto. Se tale restrizione impedisce al portafoglio europeo di identità digitale di supportare un tipo o un formato di credenziali registrato, la conseguente non conformità è attribuibile al fatto che tali sistemi operativi sottostanti, browser, API di intermediazione o altri livelli tecnici pertinenti non hanno fornito le caratteristiche di interoperabilità necessarie.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: il portafoglio europeo di identità digitale deve convalidare il certificato di registrazione della parte facente affidamento sul portafoglio ricevuto nella richiesta prima di presentare all'utente del portafoglio, per approvazione, qualsiasi PID o attestato elettronico di attributi richiesto.

— WRP-VALIDATION-02: se la convalida del certificato di registrazione della parte facente affidamento sul portafoglio non ha esito positivo, anche nei casi in cui il certificato è scaduto, revocato, non rilasciato da un fornitore di fiducia valido di certificati di registrazione delle parti facenti affidamento sul portafoglio, presenta un formato non valido o non può essere verificato a livello crittografico, il portafoglio europeo di identità digitale deve avvertire l'utente del portafoglio che non è stato possibile convalidare la parte facente affidamento sul portafoglio e non deve presentare la richiesta convalidata correttamente. L'utente del portafoglio deve approvare esplicitamente la richiesta della parte facente affidamento sul portafoglio. Il silenzio o il ricorso a caselle preselezionate non sono sufficienti ai fini dell'approvazione esplicita.

— WRP-VALIDATION-03: il fornitore del portafoglio stabilisce, sulla base della propria analisi dei rischi e della propria politica in materia di sicurezza, se e a quali condizioni le verifiche di convalida specifiche non andate a buon fine possono essere aggirate dall'utente del portafoglio.

— WRP-OVERASKING-01: il portafoglio europeo di identità digitale deve confrontare gli attestati e gli attributi richiesti dalla parte facente affidamento sul portafoglio con gli attestati e gli attributi registrati nel certificato di registrazione della parte facente affidamento sul portafoglio.

— WRP-OVERASKING-02: qualora la parte facente affidamento sul portafoglio richieda PID o attestati elettronici di attributi o dichiarazioni che non sono coperti dal certificato di registrazione della parte facente affidamento sul portafoglio, il portafoglio europeo di identità digitale deve avvertire chiaramente l'utente del portafoglio prima di effettuare qualsiasi divulgazione di dati. L'avvertimento deve indicare che la parte facente affidamento sul portafoglio chiede più informazioni rispetto a quelle per le quali ha effettuato la registrazione. L'utente del portafoglio deve approvare esplicitamente la richiesta della parte facente affidamento sul portafoglio. Il silenzio o il ricorso a caselle preselezionate non sono sufficienti ai fini dell'approvazione esplicita.

— WRP-OVERASKING-03: il fornitore del portafoglio stabilisce, sulla base della propria analisi dei rischi, della propria politica in materia di sicurezza e del diritto applicabile, se l'utente del portafoglio può continuare nonostante tale avvertimento, se è possibile divulgare soltanto il sottoinsieme di dati richiesti oggetto del certificato di registrazione oppure se la richiesta deve essere respinta.

7) 5.1 Introduction

— Il punto 5 e i suoi sottopunti definiscono un profilo per un protocollo che consente a una RP di richiedere EAAPs o PIDs al portafoglio europeo di identità digitale e a quest'ultimo di inviare a detta RP le EAAPs/PIDs richieste utilizzando un meccanismo di trasmissione non mediato dall'API, basato sulla norma ISO/IEC 18013-5 [10] oppure un meccanismo di trasmissione mediato dall'API, basato sull'allegato C della norma ISO/IEC 18013-7 [16], per trasferire le strutture di dati definite nella norma ISO/IEC 18013-5 [10] opportunamente incapsulate;

— il resto del punto 5 è organizzato come segue:

  — il punto 5.2 definisce i requisiti in materia di supporto del profilo e dei meccanismi di trasmissione da parte delle RPs e del portafoglio europeo di identità digitale;

  — il punto 5.3 definisce i requisiti specifici per il meccanismo di trasmissione non mediato dall'API;

  — il punto 5.4 e i suoi sottopunti definiscono i requisiti specifici per il meccanismo di trasmissione mediato dall'API.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: le unità di portafoglio, i fornitori di PID, i fornitori di attestati, i fornitori di portafogli e le parti facenti affidamento sul portafoglio non devono supportare il recupero tramite server come specificato nella norma ISO/IEC 18013-5 [10] per la richiesta e la presentazione di PID o attributi di attestati.

— ISO/IEC 18013-SUPPORT-02: il portafoglio europeo di identità digitale deve soddisfare i requisiti di cui ai punti 5.3 e 5.4 del presente documento.

— ISO/IEC 18013-SUPPORT-04: una parte facente affidamento dovrebbe attuare il profilo di cui al punto 5.4 del presente documento.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: le richieste di dispositivi inviate ai portafogli europei di identità digitale devono contenere la coppia di valori chiave "requestInfo" specificata al punto 8.3.2.1.2.1 del documento [10]. Il valore di questa coppia deve essere del tipo "RequestInfo".

— ISO/IEC 18013-5-REQ-05: il tipo "RequestInfo" deve corrispondere alla definizione di CDDL riportata di seguito.

```
RequestInfo = {

    "euWrprc": bstr ; contiene un certificato di registrazione (cfr. requisiti di seguito)

}
```

— ISO/IEC 18013-5-REQ-06: il membro "requestInfo" menzionato contiene un membro con etichetta "euWrprc".

— ISO/IEC 18013-5-REQ-07: il valore di "euWrprc" deve essere un certificato di registrazione codificato CBOR.

— ISO/IEC 18013-5-REQ-08: void.

— NOTA 3: void.

— ISO/IEC 18013-5-REQ-09: void.

— ISO/IEC 18013-5-REQ-10: void.

— ISO/IEC 18013-5-REQ-11: void.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Il presente punto definisce i requisiti per il tipo di messaggio "DeviceResponse" [risposta dispositivo], comuni ai due tipi di meccanismi di trasmissione (quello mediato dall'API e quello non mediato dall'API).

— NOTA 1: se ci si avvale di un meccanismo non mediato dall'API basato sulla norma ISO/IEC 18013-5 [10], una risposta EAAP è esattamente un'istanza di "DeviceResponse" come delineato al presente punto; se si ricorre a un meccanismo mediato dall'API basato sull'allegato C della norma ISO/IEC 18013-7 [16], l'istanza di "DeviceRequest" è incapsulata come specificato nell'allegato C del documento [16].

— ISO/IEC 18013-5-RESP-02: il fornitore di dati di identificazione personale e di attestati elettronici di attributi non deve includere elementi di dati nella mappa “KeyAuthorizations” [autorizzazioni chiavi] nell’oggetto di sicurezza mobile dei dati di identificazione personale e degli attestati elettronici di attributi che rilascia, fatta eccezione per gli elementi di dati forniti dalla parte facente affidamento sul portafoglio nei dati relativi alle transazioni contenuti nella richiesta mdoc, che devono essere firmati o sigillati dall’unità di portafoglio utilizzando la chiave privata dei dati di identificazione personale o degli attestati elettronici di attributi.

— NOTA 2: di conseguenza, le unità di portafoglio non possono presentare alcun elemento di dati firmato da dispositivo alle parti facenti affidamento sul portafoglio, fatta eccezione per i dati relativi alla firma che la parte facente affidamento sul portafoglio ha fornito, ad esempio nei casi d’uso per l’autenticazione sicura dell’utente.

— NOTA 3: la norma ISO/IEC 18013-5:2021 non specifica in che modo le parti facenti affidamento sul portafoglio possano includere dati relativi alle transazioni in una richiesta mdoc. L’inclusione di dati relativi alle transazioni in una richiesta mdoc deve avvenire con l’aggiunta di specifiche tecniche.

— ISO/IEC 18013-5-RESP-03: i fornitori di dati di identificazione personale non devono consentire alla chiave privata dei dati di identificazione personale di firmare gli elementi di dati forniti dalla parte facente affidamento sul portafoglio nei dati relativi alle transazioni presenti nella richiesta mdoc.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

Il presente punto definisce i requisiti per il meccanismo di trasmissione mediato dall’API in relazione ai requisiti definiti nell’allegato C del documento [16].

— ISO/IEC 18013-7-API-01: il profilo che supporta le presentazioni mediate dall’API deve essere conforme ai requisiti di cui all’allegato C della norma ISO/IEC 18013-7 [16], come ulteriormente delineato ai punti 5.3 e 5.4 del presente documento.

— ISO/IEC 18013-7-API-02: tutti i requisiti obbligatori definiti nell’allegato C del documento [16] si devono applicare come ulteriormente delineato ai punti 5.3 e 5.4 del presente documento.

— ISO/IEC 18013-7-API-03: tutti i requisiti facoltativi definiti nell’allegato C del documento [16] devono rimanere facoltativi, salvo diversa indicazione nel presente documento.

12) 5.4.2 Additional requirements

— Il presente punto specifica requisiti supplementari per il meccanismo di trasmissione mediato dall’API.

— ISO/IEC 18013-ADD-API-01: il portafoglio europeo di identità digitale deve divulgare per impostazione predefinita la presenza di tutti i tipi di attestati elettronici di attributi conservati all’API di mediazione che funziona conformemente all’allegato C del documento [16], ma non deve divulgare gli attributi e i loro valori in tali attestati elettronici di attributi.

— NOTA 1: la restrizione relativa al valore di attributo si applica anche se tale divulgazione migliorerebbe i servizi forniti dal sistema operativo al portafoglio europeo di identità digitale, ad esempio la selezione degli attestati nel contesto dell’API di mediazione;

— vi sono le considerazioni relative ai sistemi operativi e ai browser che esulano dal controllo degli implementatori, che possono essere prese in considerazione come indicato nelle note da 2 a 4:

— NOTA 2: una richiesta di presentazione da parte di una parte facente affidamento sul portafoglio che supporta l’allegato C del documento [16] può essere elaborata dal browser e/o dal sistema operativo al fine di cercare attestati elettronici di attributi disponibili, per prevenire frodi nei confronti dell’utente o per fini di risoluzione di problemi;

— NOTA 3: si prevede che il browser e/o il sistema operativo elaborino/elabori una richiesta di presentazione formulata da una parte facente affidamento sul portafoglio che supporta l’allegato C del documento [16] ai fini della sicurezza degli utenti;

— NOTA 4: si prevede che una richiesta di presentazione formulata da una parte facente affidamento sul portafoglio che supporta l'allegato C del documento [16] non sia trattata dal browser e/o dal sistema operativo per fini di analisi di mercato (anche come finalità secondaria) o per finalità interne del browser e/o del sistema operativo.

— ISO/IEC 18013-ADD-API-02: se un portafoglio europeo di identità digitale cancella, su richiesta dell'utente, PID o EAA divulgati in precedenza all'API di mediazione che funziona in modo conforme all'allegato C del documento [16], il portafoglio europeo di identità digitale deve divulgare all'API di mediazione il fatto che esso non conserva più tali PID o EAA.

— ISO/IEC 18013-ADD-API-03: se l'utente disinstalla il proprio portafoglio europeo di identità digitale, quest'ultimo deve divulgare all'API di mediazione che funziona conformemente all'allegato C del documento [16] il fatto che detto portafoglio non conserva più alcun PID o EAA divulgato in precedenza.

— ISO/IEC 18013-ADD-API-04: il portafoglio europeo di identità digitale deve fornire un'impostazione utente globale per disabilitare la divulgazione di EAA conservati attraverso un'API di mediazione che funziona come specificato nella norma ISO/IEC 18013-ADD-API-01. Quando tale impostazione è disattivata, il portafoglio europeo di identità digitale non deve pubblicizzare né rispondere alle richieste di presentazione o di rilascio mediate dall'API.

— ISO/IEC 18013-ADD-API-05: i portafogli europei di identità digitale devono verificare nei flussi tra dispositivi, utilizzando l'API di mediazione, che il dispositivo che interagisce sia in stretta prossimità fisica rispetto al portafoglio europeo di identità digitale e, ai fini dello svolgimento della verifica della prossimità fisica, utilizzano un canale di comunicazione locale sicuro, diretto e mediato dall'utente, come una tecnologia di comunicazione senza fili a corto raggio.

— NOTA: il CTAP 2.3 consente di utilizzare il BLE (*Bluetooth Low Energy*) per effettuare la verifica della prossimità fisica ravvicinata e, se implementato da entrambi i dispositivi, consente altresì di trasportare i dati tra i dispositivi attraverso tecnologie di trasmissione a corto raggio. L'esecuzione tanto della verifica della prossimità fisica quanto del trasferimento di dati tra i due dispositivi utilizzando un canale di comunicazione locale abilitato dal CTAP 2.3 dovrebbe essere preferita dai sistemi operativi sottostanti, dai browser, dalle API di mediazione o da qualsiasi altro livello tecnico al di fuori del controllo del portafoglio europeo di identità digitale rispetto al ricorso a servizi di tunnelling ibrido del CTAP.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: il portafoglio europeo di identità digitale deve soddisfare i requisiti specificati al punto 6.5 del presente allegato.

— OIDFVP-HAIP-SUPPORT-03: il portafoglio europeo di identità digitale non dovrebbe supportare il meccanismo basato sui reindirizzamenti di cui al punto 6.4 per i flussi di presentazione tra dispositivi.

— NOTA 3: l'utilizzo di questo meccanismo è vulnerabile ad attacchi, quali la fissazione della sessione. Spetta alle parti facenti affidamento sul portafoglio attenuare tali attacchi. L'attuazione di questo meccanismo non dovrebbe determinare una non conformità.

— OIDFVP-HAIP-SUPPORT-05: una parte facente affidamento sul portafoglio deve soddisfare i requisiti specificati al punto 6.5 del presente allegato.

— NOTA 5: void.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: si devono applicare tutti i requisiti obbligatori di cui ai punti 5, 5.3, 7 e 8 di HAIP [11].

— NOTA 1: "sezione 5 di HAIP [11]" fa riferimento soltanto ai requisiti direttamente sotto l'intestazione della sezione 5. Sono escluse le sezioni 5.1, 5.2 e 5.3.

— OIDFVP-HAIP-GEN-03: se il presente allegato modifica un requisito in OpenID4VC-HAIP [11], deve prevalere il requisito modificato specificato nel presente allegato.

— NOTA 2: ciò consentirebbe, ad esempio, di convertire in obbligatorio un requisito facoltativo desunto da OpenID4VC-HAIP [11] o di estendere i requisiti obbligatori.

— OIDFVP-HAIP-GEN-04: quando il formato dell'attestato richiesto è conforme al documento [10], le parti facenti affidamento e i portafogli europei di identità digitale devono essere conformi al profilo "ISO mdocs" di cui alla sezione 6 del documento [11].

— NOTA 3: per fini di chiarezza: il "profilo dei mdocs ISO" in HAIP implica che le parti facenti affidamento e i portafogli europei di identità digitale devono soddisfare i requisiti applicabili di cui all'allegato B.2 del documento [7].

— OIDFVP-HAIP-GEN-05: quando il formato dell'attestato richiesto è conforme al documento [2], le parti facenti affidamento sul portafoglio e i portafogli europei di identità digitale devono essere conformi al profilo "IETF SD-JWT VCs" di cui alla sezione 6 del documento [11].

— NOTA 4: per fini di chiarezza: il "profilo IETF SD-JWT VCs" implica che le parti facenti affidamento sul portafoglio e i portafogli europei di identità digitale devono soddisfare i requisiti di cui all'allegato B.3 del documento [7], nonché i requisiti di cui alla sezione 6.1 del documento [11].

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: void.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: void.

— OIDFVP-HAIP-COMMON-REQ-RO-03: void.

— OIDFVP-HAIP-COMMON-REQ-RO-04: void.

— OIDFVP-HAIP-COMMON-REQ-RO-05: void.

— OIDFVP-HAIP-COMMON-REQ-RO-06: void.

— OIDFVP-HAIP-COMMON-REQ-RO-07: void.

— OIDFVP-HAIP-COMMON-REQ-RO-08: void.

— OIDFVP-HAIP-COMMON-REQ-RO-09: void.

— OIDFVP-HAIP-COMMON-REQ-RO-10: void.

— OIDFVP-HAIP-COMMON-REQ-RO-11: void.

— OIDFVP-HAIP-COMMON-REQ-RO-12: void.

— Nota 2: void.

— OIDFVP-HAIP-COMMON-REQ-RO-13: Uno degli elementi del parametro "verifier_info" deve includere il certificato di registrazione.

— OIDFVP-HAIP-COMMON-REQ-RO-23: il certificato "foglia" di cui alla sezione 5.9.3 dell'OpenID4VP da utilizzare con l'x509_hash Client Identifier Prefix [prefisso identificatore client hash x509] deve essere un certificato di accesso della RP come specificato nella norma ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: void.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: void.

— NOTA: void.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: il portafoglio europeo di identità digitale deve divulgare per impostazione predefinita la presenza di tutti i tipi di attestati elettronici di attributi conservati all'API di mediazione che funziona conformemente al punto 5.2 del documento [11], ma non deve divulgare gli attributi e i loro valori in tali attestati elettronici di attributi.

— OIDFVP-HAIP-ADD-API-04: se supporta un'API di mediazione che funziona come specificato in OIDFVP-HAIP-ADD-API-01, il portafoglio europeo di identità digitale deve fornire un'impostazione utente globale per disabilitare la divulgazione degli EAA conservati tramite l'API di mediazione. Quando tale impostazione è configurata per disabilitare la divulgazione, il portafoglio europeo di identità digitale dovrebbe successivamente consentire all'utente di selezionare i singoli attestati da divulgare all'API di mediazione.

— OIDFVP-HAIP-ADD-API-05: i portafogli europei di identità digitale devono verificare nei flussi tra dispositivi, utilizzando l'API di mediazione, che il dispositivo che interagisce sia in stretta prossimità fisica rispetto al portafoglio europeo di identità digitale e, ai fini dello svolgimento della verifica della prossimità fisica, utilizzano un canale di comunicazione locale sicuro, diretto e mediato dall'utente, come una tecnologia di comunicazione senza fili a corto raggio.

— NOTA 5: il CTAP 2.3 consente di utilizzare il BLE per effettuare la verifica di prossimità fisica ravvicinata e, se implementato da entrambi i dispositivi, consente altresì di trasportare i dati tra i dispositivi attraverso tecnologie di trasmissione a corto raggio. L'esecuzione tanto della verifica della prossimità fisica quanto del trasferimento di dati tra i due dispositivi utilizzando un canale di comunicazione locale abilitato dal CTAP 2.3 dovrebbe essere preferita dai sistemi operativi sottostanti, dai browser, dalle API di mediazione o da qualsiasi altro livello tecnico al di fuori del controllo del portafoglio europeo di identità digitale rispetto al ricorso a servizi di tunnelling ibrido del CTAP.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: tutti i requisiti specificati nel presente documento applicabili alle strutture di richiesta dispositivo e risposta dispositivo specificate nella norma ISO/IEC 18013-5 si applicano anche quando il portafoglio europeo di identità digitale riceve una richiesta di presentazione ISO/IEC mdoc attraverso un meccanismo di trasmissione mediato dall'API specificato al punto C.1 del documento [16].»