2024/2979

4.12.2024

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

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) Il quadro europeo relativo a un'identità digitale istituito dal regolamento (UE) n. 910/2014 costituisce un componente essenziale per la creazione di un ecosistema per l'identità digitale sicuro e interoperabile in tutta l'Unione. Con i portafogli europei di identità digitale («portafogli») quali suo elemento fondamentale, il quadro mira a facilitare l'accesso ai servizi in tutti gli Stati membri, da parte di persone fisiche e giuridiche, garantendo nel contempo la protezione dei dati personali e della vita privata.

(2) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]) e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([3]) si applicano a tutte le attività di trattamento di dati personali ai sensi del presente regolamento.

(3) L'articolo 5 *bis*, paragrafo 23, del regolamento (UE) n. 910/2014 incarica la Commissione, se necessario, di stabilire le specifiche e le procedure pertinenti. Tale obiettivo è conseguito mediante quattro regolamenti di esecuzione riguardanti protocolli e interfacce [regolamento di esecuzione (UE) 2024/2982 della Commissione ([4])], integrità e funzionalità di base [regolamento di esecuzione (UE) 2024/2979 della Commissione ([5])], dati di identificazione personale e attestati elettronici di attributi [regolamento di esecuzione (UE) 2024/2977 della Commissione ([6])], nonché notifiche alla Commissione [regolamento di esecuzione (UE) 2024/2980 della Commissione ([7])]. Il presente regolamento stabilisce i requisiti pertinenti per l'integrità e le funzionalità di base dei portafogli europei di identità digitale.

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

([2]) 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).

([3]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

(4) La Commissione valuta periodicamente tecnologie, pratiche, norme o specifiche tecniche nuove. Al fine di garantire il massimo livello di armonizzazione tra gli Stati membri per lo sviluppo e la certificazione dei portafogli, le specifiche tecniche di cui al presente regolamento si fondano sul lavoro svolto sulla base della 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 ([8]), in particolare l'architettura e il quadro di riferimento. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([9]), la Commissione dovrebbe riesaminare e aggiornare il presente regolamento di esecuzione, se necessario, per mantenerlo allineato agli sviluppi globali, all'architettura e al quadro di riferimento e per seguire le migliori pratiche nel mercato interno.

(5) Al fine di garantire una comunicazione precisa, la differenziazione tecnica ed una chiara attribuzione delle responsabilità è necessario distinguere tra i vari componenti e le varie configurazioni di portafogli. La soluzione di portafoglio dovrebbe essere intesa come il sistema completo fornito da un fornitore del portafoglio e necessario per il funzionamento del portafoglio. La soluzione dovrebbe comprendere i componenti software e hardware, come pure i servizi, le impostazioni e le configurazioni necessari per garantire un corretto funzionamento del portafoglio. Una soluzione di portafoglio può essere ubicata sui dispositivi e negli ambienti dell'utente e nella struttura backend del fornitore. L'unità di portafoglio dovrebbe essere intesa come un setup specifico della soluzione di portafoglio per un singolo utente e dovrebbe includere l'applicazione installata su un dispositivo o in un ambiente dell'utente del portafoglio con cui detto utente interagisce direttamente («istanza di portafoglio») e le caratteristiche di sicurezza necessarie a proteggere i dati e le transazioni dell'utente. Tali caratteristiche di sicurezza dovrebbero comportare software o hardware speciali per criptare e proteggere le informazioni sensibili. L'istanza di portafoglio dovrebbe essere parte dell'unità di portafoglio e consentire all'utente del portafoglio di accedere alle funzionalità del proprio portafoglio.

(6) Le applicazioni crittografiche sicure per il portafoglio in qualità di componenti specializzati distinti all'interno di un'unità di portafoglio sono necessarie non soltanto ai fini della protezione di risorse critiche, quali le chiavi crittografiche private, ma anche per la fornitura di funzionalità fondamentali, quali la presentazione di attestati elettronici di attributi. L'uso di specifiche tecniche comuni può facilitare l'accesso dei fornitori di portafogli a elementi sicuri integrati. Le applicazioni crittografiche sicure per il portafoglio possono essere fornite in vari modi e a vari tipi di dispositivi crittografici sicuri per il portafoglio. Qualora applicazioni crittografiche sicure per il portafoglio personalizzate siano fornite dai fornitori di portafoglio come applet Java Card a elementi sicuri integrati, i fornitori di portafogli dovrebbero seguire le norme elencate nell'allegato I o specifiche tecniche equivalenti.

(7) Le unità di portafoglio devono consentire ai fornitori di dati di identificazione personale o di attestati elettronici di attributi di verificare di stare rilasciando tali dati o attestati a unità di portafoglio autentiche dell'utente del portafoglio.

(8) Al fine di garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita, i portafogli dovrebbero essere dotati di tecniche di rafforzamento della tutela della vita privata all'avanguardia disponibili. Tali caratteristiche dovrebbero prevedere la possibilità che i portafogli possano essere utilizzati senza che l'utente del portafoglio sia tracciabile tra diverse parti facenti affidamento sul portafoglio, se del caso nello scenario di utilizzo. Ad esempio i fornitori di portafogli dovrebbero prendere in considerazione misure di rafforzamento della tutela della vita privata all'avanguardia in relazione agli attestati di unità di portafoglio, quali l'utilizzo di attestati di unità di portafoglio effimeri o il rilascio per lotti. Inoltre le politiche di divulgazione incorporate dovrebbero mettere in guardia gli utenti del portafoglio contro la divulgazione inadeguata o illegale di attributi a partire da attestati elettronici di attributi.

(9) Gli attestati di unità di portafoglio dovrebbero consentire alle parti -facenti affidamento sul portafoglio che richiedono attributi alle unità di portafoglio di verificare lo stato di validità dell'unità di portafoglio con cui stanno comunicando, in quanto gli attestati di unità di portafoglio devono essere revocati quando un'unità di portafoglio non è più considerata valida. Le informazioni concernenti lo stato di validità delle unità di portafoglio dovrebbero essere rese disponibili in modo interoperabile, al fine di garantire che possano essere utilizzate da tutte le parti facenti affidamento sul portafoglio. Inoltre, nei casi in cui gli utenti del portafoglio abbiano perso le loro unità di portafoglio o non abbiano più il controllo sulle stesse, i fornitori di portafogli dovrebbero consentire agli utenti del portafoglio di chiedere la revoca della loro unità di portafoglio. Per garantire la tutela della vita privata e impedire i collegamenti gli Stati membri dovrebbero impiegare tecniche di tutela della vita privata anche per l'attestato di unità di portafoglio. Potrebbero essere utilizzati attestati di unità di portafoglio multipli per diverse finalità, che divulghino solo le minime informazioni pertinenti concernenti il portafoglio necessarie per una transazione, oppure potrebbe essere limitata la durata dell'attestato di unità di portafoglio come alternativa all'utilizzo degli identificatori di revoca.

([8]) GU L 210 del 14.6.2021, pag. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) Al fine di garantire che tutti i portafogli siano tecnicamente in grado di ricevere e presentare dati di identificazione personale e attestati elettronici di attributi nel contesto di scenari transfrontalieri senza compromettere l'interoperabilità, i portafogli dovrebbero supportare tipi predeterminati di formati di dati e divulgazione selettiva. Come stabilito nel regolamento (UE) n. 910/2014, la divulgazione selettiva è un concetto che conferisce al proprietario dei dati il potere di divulgare solo alcune parti di un insieme di dati più ampio, affinché il soggetto ricevente ottenga solo le informazioni necessarie per la prestazione di un servizio richiesto da un utente. Poiché i portafogli devono consentire all'utente di divulgare selettivamente gli attributi, le norme elencate nell'allegato II dovrebbero essere attuate in modo da consentire questa caratteristica dei portafogli. Inoltre i portafogli possono supportare altri formati e altre funzionalità al fine di facilitare casi d'uso specifici.

(11) La registrazione delle transazioni costituisce uno strumento importante per garantire la trasparenza, sotto forma di una panoramica delle transazioni fornita all'utente del portafoglio. Inoltre le registrazioni dovrebbero essere utilizzate per consentire una condivisione rapida e agevole di determinate informazioni, su richiesta dell'utente del portafoglio, con le autorità di controllo competenti istituite a norma dell'articolo 51 del regolamento (UE) 2016/679, in caso di comportamento sospetto delle parti facenti affidamento sul portafoglio.

(12) Affinché un utente del portafoglio possa firmare elettronicamente, a detto utente del portafoglio dovrebbe essere rilasciato un certificato qualificato, collegato a un dispositivo per la creazione di una firma elettronica qualificata. L'utente del portafoglio dovrebbe avere accesso a un'applicazione per la creazione di una firma. Mentre il rilascio di certificati qualificati è un servizio erogato da prestatori di servizi fiduciari qualificati, i fornitori di portafogli o altre entità dovrebbero poter fornire gli altri componenti. Ad esempio i dispositivi per la creazione di una firma elettronica qualificata possono essere gestiti da prestatori di servizi fiduciari qualificati sotto forma di un servizio oppure possono essere presenti a livello locale in relazione al dispositivo dell'utente del portafoglio, ad esempio sotto forma di una smart card. Analogamente, le applicazioni per la creazione di firme possono essere integrate nell'istanza di portafoglio, essere un'applicazione separata sul dispositivo dell'utente del portafoglio oppure essere fornite a distanza.

(13) Gli oggetti di esportazione e portabilità dei dati possono registrare i dati di identificazione personale e gli attestati elettronici di attributi che sono stati rilasciati a una specifica unità di portafoglio. Tali oggetti consentono agli utenti del portafoglio di estrarre i dati pertinenti dalla loro unità di portafoglio al fine di rafforzare il loro diritto alla portabilità dei dati. I fornitori di portafogli sono incoraggiati a utilizzare le medesime soluzioni tecniche anche per attuare processi di backup e recupero per le unità di portafoglio, consentendo di recuperare le unità di portafoglio perse o di trasferire informazioni da un fornitore del portafoglio a un altro, se del caso e nella misura in cui ciò possa essere fatto senza pregiudicare il diritto alla protezione dei dati e la sicurezza dell'ecosistema per l'identità digitale.

(14) La generazione di pseudonimi specifici per le parti facenti affidamento sul portafoglio dovrebbe consentire agli utenti del portafoglio di autenticarsi senza fornire informazioni non necessarie alle parti facenti affidamento sul portafoglio. Come stabilito nel regolamento (UE) n. 910/2014, gli utenti del portafoglio non devono essere ostacolati nell'accesso ai servizi sotto pseudonimo, laddove non vi sia alcun obbligo giuridico di identità giuridica per l'autenticazione. I portafogli devono pertanto comprendere una funzionalità per la generazione di pseudonimi scelti e gestiti dall'utente, per l'autenticazione quando accede a servizi online. L'attuazione delle specifiche di cui all'allegato V dovrebbe consentire tali funzionalità di conseguenza. Inoltre le parti facenti affidamento sul portafoglio non devono chiedere agli utenti di fornire dati diversi da quelli indicati per l'uso previsto dei portafogli nel registro delle parti facenti affidamento sulla certificazione. Gli utenti del portafoglio dovrebbero poter verificare i dati di registrazione delle parti facenti affidamento sulla certificazione in qualsiasi momento.

(15) Come stabilito nel regolamento (UE) 2024/1183, gli Stati membri non devono limitare, direttamente o indirettamente, l'accesso ai servizi pubblici o privati da parte di persone fisiche o giuridiche che scelgono di non utilizzare portafogli e devono mettere a disposizione soluzioni alternative adeguate.

(16) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([10]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 30 settembre 2024.

([10]) 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).

(17) Le misure di cui al presente regolamento sono conformi al parere del comitato di cui all'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

Il presente regolamento stabilisce le norme relative all'integrità e alle funzionalità di base dei portafogli, da aggiornare periodicamente per tenere conto degli sviluppi tecnologici, della normazione e del lavoro svolto sulla base della raccomandazione (UE) 2021/946 della Commissione, in particolare dell'architettura e del quadro di riferimento.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) «applicazione crittografica sicura per il portafoglio»: un'applicazione che gestisce risorse critiche tramite un collegamento alle funzioni crittografiche e non crittografiche fornite dal dispositivo crittografico sicuro per il portafoglio e l'uso di tali funzioni;

(2) «unità di portafoglio»: una configurazione unica di una soluzione di portafoglio che comprende istanze di portafoglio, applicazioni crittografiche sicure per il portafoglio e dispositivi crittografici sicuri per il portafoglio forniti da un fornitore del portafoglio a un singolo utente del portafoglio;

(3) «risorse critiche»: risorse all'interno di un'unità di portafoglio o ad essa relative, di importanza tale che un'eventuale compromissione della loro disponibilità, riservatezza o integrità avrebbe un effetto estremamente grave e debilitante sulla possibilità di fare affidamento sull'unità di portafoglio;

(4) «fornitore di dati di identificazione personale»: la persona fisica o giuridica responsabile del rilascio e della revoca dei dati di identificazione personale e che garantisce che i dati di identificazione personale di un utente siano associati crittograficamente a un'unità di portafoglio;

(5) «utente del portafoglio»: un utente che ha il controllo dell'unità di portafoglio;

(6) «parte facente affidamento sul portafoglio»: una parte facente affidamento che intende fare affidamento sulle unità di portafoglio per la prestazione di servizi pubblici o privati mediante interazione digitale;

(7) «fornitore del portafoglio»: una persona fisica o giuridica che fornisce soluzioni di portafoglio;

(8) «attestato di unità di portafoglio»: un oggetto di dati che descrive i componenti dell'unità di portafoglio o consente la loro autenticazione e convalida;

(9) «politica di divulgazione incorporata»: un insieme di norme, incorporato in un attestato elettronico di attributi dal suo fornitore, che indica le condizioni che una parte facente affidamento sul portafoglio deve soddisfare per accedere all'attestato elettronico di attributi;

(10) «istanza di portafoglio»: l'applicazione installata e configurata su un dispositivo o su un ambiente di un utente del portafoglio, che fa parte di un'unità di portafoglio, e che l'utente del portafoglio utilizza per interagire con l'unità di portafoglio;

(11) «soluzione di portafoglio»: una combinazione di software, hardware, servizi, impostazioni e configurazioni, comprese le istanze di portafoglio, una o più applicazioni crittografiche sicure per il portafoglio e uno o più dispositivi crittografici sicuri per il portafoglio;

(12) «dispositivo crittografico sicuro per il portafoglio»: un dispositivo resistente alle manomissioni che fornisce un ambiente collegato all'applicazione crittografica sicura per il portafoglio e da essa utilizzato per proteggere le risorse critiche e fornire funzioni crittografiche per l'esecuzione sicura di operazioni critiche;

(13) «operazione crittografica del portafoglio»: un meccanismo crittografico necessario nel contesto dell'autenticazione dell'utente del portafoglio e del rilascio o della presentazione di dati di identificazione personale o di attestati elettronici di attributi;

(14) «certificato di accesso della parte facente affidamento sul portafoglio»: un certificato per sigilli elettronici o firme elettroniche che autenticano e convalidano la parte facente affidamento sul portafoglio, rilasciato da un fornitore di certificati di accesso della parte facente affidamento sul portafoglio;

(15) «fornitore di certificati di accesso della parte facente affidamento sul portafoglio»: una persona fisica o giuridica incaricata da uno Stato membro di rilasciare certificati di accesso delle parti facenti affidamento alle parti facenti affidamento sul portafoglio registrate in tale Stato membro.

CAPO II

INTEGRITÀ DEI PORTAFOGLI EUROPEI DI IDENTITÀ DIGITALE

Articolo 3

Integrità dell'unità di portafoglio

1. Le unità di portafoglio non eseguono alcuna funzionalità di cui all'articolo 5 *bis*, paragrafo 4, del regolamento (UE) n. 910/2014, eccetto l'autenticazione dell'utente del portafoglio per l'accesso all'unità di portafoglio, fino a quando l'unità di portafoglio non abbia autenticato con successo l'utente del portafoglio.

2. Per ciascuna unità di portafoglio, i fornitori di portafogli appongono una firma o un sigillo su almeno un attestato di unità di portafoglio conforme ai requisiti di cui all'articolo 6. Il certificato utilizzato per firmare o sigillare l'attestato di unità di portafoglio è rilasciato sulla base di un certificato che figura nell'elenco di fiducia di cui al regolamento di esecuzione (UE) 2024/2980.

Articolo 4

Istanze di portafoglio

1. Per gestire le risorse critiche le istanze di portafoglio utilizzano almeno un dispositivo crittografico sicuro per il portafoglio.

2. I fornitori di portafogli garantiscono l'integrità, l'autenticità e la riservatezza della comunicazione tra le istanze di portafoglio e le applicazioni crittografiche sicure per il portafoglio.

3. Se le risorse critiche riguardano l'esecuzione dell'identificazione elettronica ad un livello di garanzia elevato, le operazioni crittografiche del portafoglio o altre operazioni di trattamento di risorse critiche sono effettuate conformemente ai requisiti per le caratteristiche e la progettazione dei mezzi di identificazione elettronica a un livello di garanzia elevato, come stabilito nel regolamento di esecuzione (UE) 2015/1502 della Commissione ([11]).

Articolo 5

Applicazioni crittografiche sicure per il portafoglio

1. I fornitori di portafogli garantiscono che le applicazioni crittografiche sicure per il portafoglio:

a) effettuino operazioni crittografiche del portafoglio che coinvolgono risorse critiche diverse da quelle necessarie per l'autenticazione dell'utente del portafoglio da parte dell'unità di portafoglio soltanto nei casi in cui tali applicazioni abbiano autenticato con successo gli utenti del portafoglio;

([11]) Regolamento di esecuzione (UE) 2015/1502 della Commissione, dell'8 settembre 2015, relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 235 del 9.9.2015, pag. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) laddove autentichino gli utenti del portafoglio nel contesto della realizzazione dell'identificazione elettronica ad un livello di garanzia elevato, effettuino l'autenticazione degli utenti del portafoglio in conformità ai requisiti per le caratteristiche e la progettazione di mezzi di identificazione elettronica a un livello di garanzia elevato, come stabilito nel regolamento di esecuzione (UE) 2015/1502;

c) siano in grado di generare in modo sicuro chiavi crittografiche nuove;

d) siano in grado di effettuare la cancellazione sicura di risorse critiche;

e) siano in grado di generare una prova del possesso di chiavi private;

f) proteggano le chiavi private generate da tali applicazioni crittografiche sicure per il portafoglio durante l'esistenza delle chiavi stesse;

g) soddisfino i requisiti per le caratteristiche e la progettazione di mezzi di identificazione elettronica a un livello di garanzia elevato, come stabilito nel regolamento di esecuzione (UE) 2015/1502;

h) siano gli unici componenti in grado di eseguire operazioni crittografiche del portafoglio e qualsiasi altra operazione con risorse critiche nel contesto della realizzazione di un'identificazione elettronica ad un livello di garanzia elevato.

2. Qualora decidano di fornire un'applicazione crittografica sicura per il portafoglio a un elemento sicuro integrato, i fornitori di portafogli basano la loro soluzione tecnica sulle specifiche tecniche elencate nell'allegato I o su altre specifiche tecniche equivalenti.

Articolo 6

Autenticità e validità dell'unità di portafoglio

1. I fornitori di portafogli garantiscono che ciascuna unità di portafoglio contenga attestati di unità di portafoglio.

2. I fornitori di portafogli garantiscono che gli attestati di unità di portafoglio di cui al paragrafo 1 contengano chiavi pubbliche e che le corrispondenti chiavi private siano protette da un dispositivo crittografico sicuro per il portafoglio.

3. I fornitori di portafogli:

a) informano gli utenti del portafoglio in merito ai loro diritti e obblighi in relazione alla loro unità di portafoglio;

b) forniscono meccanismi, indipendenti dalle unità di portafoglio, per l'identificazione e l'autenticazione sicure degli utenti del portafoglio;

c) garantiscono che gli utenti del portafoglio abbiano il diritto di chiedere la revoca dei loro attestati di unità di portafoglio, utilizzando i meccanismi di autenticazione di cui alla lettera(b).

Articolo 7

Revoca degli attestati di unità di portafoglio

1. I fornitori di portafogli sono le uniche entità in grado di revocare gli attestati di unità di portafoglio per le unità di portafoglio che hanno fornito.

2. I fornitori di portafogli stabiliscono una politica pubblicamente disponibile che specifichi le condizioni e le tempistiche per la revoca degli attestati di unità di portafoglio.

3. Qualora abbiano revocato gli attestati di unità di portafoglio, i fornitori di portafogli informano gli utenti del portafoglio interessati entro 24 ore dalla revoca delle loro unità di portafoglio, indicando altresì il motivo della revoca e le conseguenze per l'utente del portafoglio. Tali informazioni sono fornite in maniera concisa, facilmente accessibile e utilizzando un linguaggio semplice e chiaro.

4. Qualora abbiano revocato gli attestati di unità di portafoglio, i fornitori di portafogli rendono pubblicamente disponibili lo stato di validità dell'attestato di unità di portafoglio secondo modalità che ne preservano la riservatezza e descrivono l'ubicazione di tali informazioni nell'attestato di unità di portafoglio.

CAPO III

FUNZIONALITÀ E CARATTERISTICHE DI BASE DEI PORTAFOGLI EUROPEI DI IDENTITÀ DIGITALE

Articolo 8

Formati per i dati di identificazione personale e per gli attestati elettronici di attributi

I fornitori di portafogli garantiscono che le soluzioni di portafoglio supportino l'utilizzo di dati di identificazione personale e attestati elettronici di attributi rilasciati in conformità all'elenco di norme di cui all'allegato II.

Articolo 9

Registrazioni di transazioni

1. Indipendentemente dal fatto che una transazione sia completata o meno, le istanze di portafoglio registrano tutte le transazioni con le parti facenti affidamento sul portafoglio e altre unità di portafoglio, comprese l'apposizione di firme e sigilli elettronici.

2. Tra le informazioni registrate figurano come minimo:

a) l'ora e la data della transazione;

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 o, nel caso di altre unità di portafoglio, le informazioni pertinenti desunte dall'attestato di unità di portafoglio;

c) il tipo o i tipi di dati richiesti e presentati nel contesto della transazione;

d) nel caso di transazioni non completate, il motivo di tale mancato completamento.

3. I fornitori di portafogli garantiscono l'integrità, l'autenticità e la riservatezza delle informazioni registrate.

4. Le istanze di portafoglio registrano le segnalazioni inviate dall'utente del portafoglio alle autorità di protezione dei dati attraverso la loro unità di portafoglio.

5. Le registrazioni di cui ai paragrafi 1 e 2 sono accessibili al fornitore del portafoglio, ove necessario per la prestazione di servizi di portafoglio, sulla base di un consenso preventivo esplicito prestato dall'utente del portafoglio.

6. Le registrazioni di cui ai paragrafi 1 e 2 rimangono accessibili fintantoché ciò è richiesto dal diritto dell'Unione o dal diritto interno.

7. I fornitori di portafogli consentono agli utenti del portafoglio di esportare le informazioni registrate di cui al paragrafo 2.

Articolo 10

Divulgazione incorporata

1. I fornitori di portafogli garantiscono che gli attestati elettronici di attributi con politiche di divulgazione incorporate comuni di cui all'allegato III possano essere trattati dalle unità di portafoglio che forniscono.

2. Le istanze di portafoglio sono in grado di elaborare e presentare tali politiche di divulgazione incorporate di cui al paragrafo 1 in combinazione con i dati ricevuti dalla parte facente affidamento sul portafoglio.

3. Le istanze di portafoglio verificano se la parte facente affidamento sul portafoglio soddisfa i requisiti della politica di divulgazione incorporata e informano l'utente del portafoglio in merito all'esito di tale verifica.

Articolo 11

Firme e sigilli elettronici qualificati

1. I fornitori di portafogli garantiscono che gli utenti del portafoglio possano ricevere certificati qualificati per firme elettroniche qualificate o sigilli elettronici qualificati collegati a dispositivi per la creazione di firme qualificate o sigilli qualificati che sono locali, esterne/i o remote/i in relazione alle istanze di portafoglio.

2. I fornitori di portafogli garantiscono che le soluzioni di portafoglio siano in grado di interfacciarsi in modo sicuro con uno dei tipi seguenti di dispositivi per la creazione di firme qualificate o sigilli qualificati: dispositivi per la creazione di firme qualificate o sigilli qualificati locali, esterni o gestiti a distanza ai fini dell'utilizzo dei certificati qualificati di cui al paragrafo 1.

3. I fornitori di portafogli garantiscono che gli utenti del portafoglio che sono persone fisiche dispongano, quanto meno per fini non professionali, di un accesso gratuito alle applicazioni per la creazione di firme che consentono la creazione di firme elettroniche qualificate gratuite utilizzando i certificati di cui al paragrafo 1.

Articolo 12

Applicazioni per la creazione di firme

1. Le applicazioni per la creazione di firme utilizzate dalle unità di portafoglio possono essere fornite da fornitori di portafogli, da prestatori di servizi fiduciari o da parti facenti affidamento sul portafoglio.

2. Le applicazioni per la creazione di firme dispongono delle funzioni seguenti:

a) apposizione di una firma o di un sigillo su dati forniti dall'utente del portafoglio;

b) apposizione di una firma o di un sigillo su dati forniti dalla parte facente affidamento sulla certificazione;

c) creazione di firme o sigilli come minimo nei formati obbligatori di cui all'allegato IV;

d) informazione degli utenti del portafoglio in merito al risultato del processo di creazione della firma o del sigillo.

3. Le applicazioni per la creazione di firme possono essere integrate in istanze di portafoglio o essere esterne a queste ultime. Qualora facciano affidamento su dispositivi qualificati per la creazione di firme a distanza e siano integrate nelle istanze di portafoglio, le applicazioni per la creazione di firme supportano l'interfaccia di programmazione di un'applicazione di cui all'allegato IV.

Articolo 13

Esportazione e portabilità dei dati

Laddove tecnicamente fattibile e fatta eccezione per i casi di risorse critiche, le unità di portafoglio supportano l'esportazione sicura e la portabilità dei dati personali dell'utente del portafoglio al fine di consentire a quest'ultimo di migrare verso un'unità di portafoglio di una soluzione di portafoglio diversa in un modo che assicuri un livello di garanzia elevato di cui al regolamento di esecuzione (UE) 2015/1502.

Articolo 14

Pseudonimi

1. Le unità di portafoglio supportano la generazione di pseudonimi per gli utenti del portafoglio conformemente alle specifiche tecniche di cui all'allegato V.

2. Le unità di portafoglio supportano la generazione, su richiesta di una parte facente affidamento sul portafoglio, di uno pseudonimo specifico e unico per tale parte e forniscono detto pseudonimo alla parte facente affidamento sul portafoglio o da solo, o in combinazione con qualsiasi dato di identificazione personale o attestato elettronico di attributi richiesto da tale parte.

CAPO IV

DISPOSIZIONI FINALI

Articolo 15

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 28 novembre 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

ELENCO DELLE NORME DI CUI ALL'ARTICOLO 5

— SAM.01 Secured Applications for Mobile - Requirements for support 3 third party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

ALLEGATO II

ELENCO DELLE NORME DI CUI ALL'ARTICOLO 8

— ISO/IEC 18013-5:2021

— *Verifiable Credentials Data Model 1.1, W3C Recommendation,* 3 marzo 2022.

ALLEGATO III

ELENCO DELLE POLITICHE DI DIVULGAZIONE INCORPORATE COMUNI DI CUI ALL'ARTICOLO 10

1. «Nessuna politica» indica che non si applica alcuna politica agli attestati elettronici di attributi.
2. La politica «solo le parti facenti affidamento sulla certificazione autorizzate» indica che gli utenti del portafoglio possono divulgare attestati elettronici di attributi solo a parti facenti affidamento sulla certificazione autenticate, che sono esplicitamente elencate nelle politiche di divulgazione.
3. «Root of trust specifica» indica che gli utenti del portafoglio dovrebbero divulgare lo specifico attestato elettronico di attributi soltanto alle parti facenti affidamento sul portafoglio autenticate con certificati di accesso di dette parti derivati da una root specifica (o da un elenco di root specifiche) o da certificati intermedi.

ALLEGATO IV

FORMATI PER FIRME E SIGILLI DI CUI ALL'ARTICOLO 12

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 V1.1.1 (2016-04); *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; par*te 1: *Building blocks and PAdES baseline signatures*.

2. Elenco dei formati facoltativi per firme o sigilli:

   a) XAdES come specificato nella norma ETSI EN 319 132-1 V1.2.1 (2022-02) *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; par*te 1: *Building blocks and XAdES baseline signatures (XAdES)* per firme in formato XML;

   b) JAdES come specificato nella norma ETSI TS 119 182-1 V1.2.1 (2024-07) *Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; par*te 1: *Building blocks and JAdES baseline signatures* per firme in formato JSON;

   c) CAdES (*CMS Advanced Electronic Signature*) come specificato nella norma ETSI EN 319 122-1 V1.3.1 (2023-06) *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; par*te 1: *Building blocks and CAdES baseline signatures* per firme in formato CMS;

   d) ASiC (*Associated Signature Container*) come specificato nella norma ETSI EN 319 162-1 V1.1.1 (2016-04) *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); par*te 1: *Building blocks and ASiC baseline containers* e norma ETSI EN 319 162-2 V1.1.1 (2016-04) *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); par*te 2: *Additional ASiC containers*' per la firma di contenitori.

3. Interfaccia di programmazione di un'applicazione:

   — *Cloud Signature Consortium (CSC)*, specifica v2.0 (20 aprile 2023).

ALLEGATO V

SPECIFICHE TECNICHE PER LA GENERAZIONE DI PSEUDONIMI DI CUI ALL'ARTICOLO 14

Specifiche tecniche:

— *Web Authentication – Level 2, W3C Recommendation*, 8 aprile 2021, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.