2024/2981

4.12.2024

# REGOLAMENTO DI ESECUZIONE (UE) 2024/2981 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 la certificazione 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 *quater*, paragrafo 6,

considerando quanto segue:

(1) A norma dell'articolo 5 *quater* del regolamento (UE) n. 910/2014, la certificazione dei portafogli europei di identità digitale («portafogli») deve essere effettuata conformemente ai requisiti funzionali, di cibersicurezza e di protezione dei dati al fine di garantire un livello elevato di sicurezza e fiducia nei portafogli. Tali requisiti di certificazione devono essere armonizzati in tutti gli Stati membri al fine di evitare la frammentazione del mercato e di creare un quadro solido.

(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) 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 ([4]), in particolare l'architettura e il quadro di riferimento che ne fanno parte. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([5]), 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.

(4) Al fine di attestare la conformità ai requisiti di cibersicurezza inclusi nel quadro di certificazione, la certificazione delle soluzioni di portafoglio dovrebbe fare riferimento, laddove disponibili e pertinenti, a sistemi europei di certificazione della cibersicurezza istituiti a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([6]). In assenza di tali sistemi, o quando essi coprono parzialmente i requisiti di cibersicurezza, il presente regolamento stabilisce i requisiti generali applicabili ai sistemi nazionali di certificazione, che riguardano i requisiti funzionali, di cibersicurezza e di protezione dei dati.

([1]) GU L 257 del 28.8.2014, pag. 73, ELI: https://eur-lex.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]) GU L 210 del 14.6.2021, pag. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Conformemente all'articolo 5 *bis*, paragrafo 11, del regolamento (UE) n. 910/2014, i portafogli devono essere certificati rispetto a un livello di garanzia elevato di cui al medesimo regolamento, nonché al regolamento di esecuzione (UE) 2015/1502 della Commissione ([7]). Tale livello di garanzia deve essere conseguito dalla soluzione di portafoglio nel complesso. A norma del presente regolamento, alcuni componenti della soluzione di portafoglio possono essere certificati a un livello di garanzia inferiore, a condizione che ciò sia debitamente giustificato e non pregiudichi il livello di garanzia elevato raggiunto dalla soluzione complessiva.

(6) Tutti i sistemi nazionali di certificazione dovrebbero individuare un titolare del sistema che sarà competente per lo sviluppo e la manutenzione del sistema di certificazione. Il titolare del sistema può essere un organismo di valutazione della conformità, un organismo governativo o un'autorità governativa, un'associazione di categoria, un gruppo di organismi di valutazione della conformità o qualsiasi organismo adeguato e può essere diverso dall'organismo che gestisce il sistema nazionale di certificazione.

(7) L'oggetto della certificazione dovrebbe includere i componenti software della soluzione di portafoglio, come l'istanza di portafoglio. L'applicazione crittografica sicura per il portafoglio (WSCA), il dispositivo crittografico sicuro per il portafoglio (WSCD) e le piattaforme su cui tali componenti software sono eseguiti, pur facendo parte dell'ambiente operativo, dovrebbero essere inclusi nell'oggetto della certificazione soltanto quando sono forniti dalla soluzione di portafoglio. In altri casi, e in particolare quando tali dispositivi e piattaforme sono forniti da utenti finali, i fornitori dovrebbero stabilire ipotesi sull'ambiente operativo della soluzione di portafoglio, anche su tali dispositivi e piattaforme, e attuare misure per confermare che tali ipotesi sono verificate nella pratica. Al fine di garantire la protezione delle risorse critiche attraverso l'hardware e il software di sistema utilizzati per gestire e proteggere le chiavi crittografiche create, conservate o trattate dal dispositivo crittografico sicuro per il portafoglio, quest'ultimo dispositivo deve soddisfare norme rigorose di certificazione, come indicato nelle norme internazionali quali la valutazione EAL4 dei criteri comuni (*Common Criteria*) di cui al regolamento di esecuzione (UE) 2024/482 ([8]) e l'analisi metodica avanzata della vulnerabilità, comparabile all'AVA_VAN.5. Tali norme di certificazione dovrebbero essere utilizzate al più tardi quando la certificazione della conformità dei portafogli è effettuata a seguito dell'adozione a norma del regolamento (UE) 2019/881 di un sistema europeo di certificazione della cibersicurezza.

(8) I portafogli interamente mobili, sicuri e di facile utilizzo sono supportati dalla disponibilità di soluzioni standardizzate e certificate come resistenti alle manomissioni, quali elementi sicuri integrati, dispositivi esterni quali smartcard, o piattaforme SIM integrate nei dispositivi mobili. È importante garantire l'accesso tempestivo agli elementi sicuri integrati per i mezzi e i portafogli nazionali di identificazione elettronica e coordinare gli sforzi degli Stati membri in questo settore. Il gruppo di cooperazione per l'identità digitale europea istituito a norma dell'articolo 46 *sexies*, paragrafo 1, del regolamento (UE) n. 910/2014 («gruppo di cooperazione») dovrebbe pertanto istituire un sottogruppo dedicato a tal fine. Consultando i portatori di interessi pertinenti, il sottogruppo dovrebbe concordare una tabella di marcia comune per l'accesso agli elementi sicuri integrati che la Commissione dovrà prendere in considerazione per la relazione di riesame del regolamento (UE) n. 910/2014. Al fine di agevolare la diffusione del portafoglio a livello nazionale, la Commissione dovrebbe inoltre, in cooperazione con gli Stati membri, elaborare e aggiornare costantemente un manuale per i casi d'uso nell'ambito del quadro di architettura e di riferimento.

(9) L'oggetto della certificazione dei sistemi nazionali di certificazione dovrebbe comprendere altresì i processi utilizzati per fornire e gestire la soluzione di portafoglio, anche se la definizione o l'esecuzione di tali processi è subappaltata a terzi. Al fine di dimostrare che i processi soddisfano i requisiti dei sistemi, come elementi di prova si possono utilizzare le informazioni sulla garanzia, a condizione che si faccia ricorso a un'analisi della dipendenza per determinare se tali informazioni sulla garanzia sono sufficienti. Le informazioni sulla garanzia si presentano in numerose forme diverse, tra cui relazioni e certificati di conformità, che possono essere privati, nazionali, europei o internazionali, basati su norme o su specifiche tecniche. L'obiettivo dell'analisi della dipendenza è valutare la qualità delle informazioni di garanzia disponibili sui componenti del portafoglio.

([7]) 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).

([8]) Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Secondo le procedure stabilite a tal fine, il gruppo di cooperazione dovrebbe essere in grado di formulare pareri e raccomandazioni sui progetti di sistemi nazionali di certificazione che gli sono presentati. Tali sistemi nazionali di certificazione dovrebbero essere specifici per l'architettura del portafoglio e dovrebbero esistere profili specifici per ciascuna architettura specifica supportata.

(11) Al fine di garantire una comprensione comune e un approccio armonizzato alla valutazione dei rischi più critici che potrebbero incidere sulla fornitura e sul funzionamento dei portafogli, è opportuno predisporre un registro dei rischi e delle minacce di cui si dovrebbe tenere conto nella progettazione di soluzioni di portafoglio indipendentemente dalla loro architettura specifica. Nell'individuare i rischi che dovrebbero essere inclusi in tale registro, si dovrebbero tenere a mente gli obiettivi in materia di cibersicurezza descritti nel regolamento (UE) n. 910/2014, quali la riservatezza, l'integrità e la disponibilità della soluzione di portafoglio, nonché la tutela della vita privata degli utenti e della riservatezza dei dati. La debita considerazione dei rischi e delle minacce inclusi in tale registro dei rischi dovrebbe costituire parte dei requisiti dei sistemi nazionali di certificazione. Per tenere conto della continua evoluzione del panorama delle minacce, il registro dei rischi dovrebbe essere mantenuto e aggiornato periodicamente, in collaborazione con il gruppo di cooperazione.

(12) Nel momento in cui istituiscono i loro sistemi di certificazione, i titolari dei sistemi dovrebbero effettuare una valutazione dei rischi al fine di affinare e integrare i rischi e le minacce elencati nel registro con rischi e minacce specifici dell'architettura o dell'attuazione della soluzione di portafoglio. Nella valutazione dei rischi si dovrebbe esaminare in che modo i rischi e le minacce applicabili possano essere trattati in modo adeguato. I fornitori di portafogli dovrebbero integrare la valutazione dei rischi del sistema al fine di individuare eventuali rischi e minacce specifici per la loro attuazione e proporre misure di trattamento adeguate per la valutazione da parte dell'organismo di certificazione.

(13) Al fine di dimostrare che un'architettura di una soluzione di portafoglio soddisfa i requisiti di sicurezza applicabili, ciascun sistema o profilo specifico dell'architettura dovrebbe contenere quanto meno una descrizione dell'architettura della soluzione di portafoglio, un elenco di requisiti di sicurezza applicabili all'architettura della soluzione di portafoglio, un piano di valutazione per confermare che una soluzione di portafoglio basata su tale architettura soddisfa tali requisiti e una valutazione dei rischi. I sistemi nazionali di certificazione dovrebbero imporre ai fornitori di portafogli di dimostrare in che modo la progettazione della soluzione di portafoglio che forniscono corrisponde all'architettura di riferimento e specificare i controlli di sicurezza e i piani di convalida per la soluzione di portafoglio specifica. I sistemi nazionali di certificazione dovrebbero inoltre definire un'attività di valutazione della conformità al fine di verificare che la progettazione del portafoglio rispecchi adeguatamente l'architettura di riferimento del profilo selezionato. I sistemi nazionali di certificazione dovrebbero rispettare le prescrizioni di cui all'articolo 51 del regolamento (UE) 2019/881, fatta eccezione per le lettere e) ed f), relative alla registrazione.

(14) Per quanto riguarda la certificazione dei prodotti, è opportuno consentire l'uso di certificati di conformità rilasciati nel contesto del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni («EUCC») e di certificati di conformità rilasciati nel quadro di sistemi nazionali di certificazione nel contesto dell'accordo sul riconoscimento reciproco del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (Senior Officials Group — Information Systems Security — SOG-IS). Inoltre, altri sistemi nazionali di certificazione dovrebbero poter essere utilizzati per componenti di prodotti meno sensibili, quali quelli stabiliti secondo la norma CEN EN 17640 per la metodologia di valutazione della cibersicurezza a durata fissa.

(15) Il marchio di fiducia UE per i portafogli di identità digitale («marchio di fiducia») dovrebbe essere utilizzato per indicare in modo chiaro, semplice e riconoscibile che un portafoglio è stato fornito conformemente al regolamento (UE) n. 910/2014. Dovrebbe pertanto essere considerato un marchio di conformità per una soluzione di portafoglio certificata nel contesto di sistemi nazionali di certificazione. I sistemi nazionali di certificazione non dovrebbero definire altri marchi di conformità.

(16) Al fine di scoraggiare le frodi, i sistemi nazionali di certificazione dovrebbero definire le azioni da intraprendere qualora la certificazione nel contesto del sistema sia dichiarata in modo fraudolento.

(17) Per garantire una gestione efficiente delle notifiche di vulnerabilità, i fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite dovrebbero definire e attuare processi per valutare la gravità e l'impatto potenziale delle vulnerabilità. I sistemi nazionali di certificazione dovrebbero fissare una soglia oltre la quale l'organismo di certificazione deve essere notificato. Tale obbligo di notifica non dovrebbe incidere sui criteri stabiliti dalla legislazione in materia di protezione dei dati e dalle autorità di protezione dei dati degli Stati membri per la notifica di violazioni dei dati personali. Si potrebbero stabilire possibili sinergie tra la notifica obbligatoria della violazione o della compromissione delle soluzioni di portafoglio e la notifica di violazioni dei dati personali a norma del regolamento (UE) 2016/679. La valutazione da parte dell'organismo di certificazione di una relazione sull'analisi dell'impatto delle vulnerabilità non dovrebbe pregiudicare la valutazione, svolta da un'autorità di protezione dei dati, di una valutazione d'impatto sulla protezione dei dati a norma degli articoli 35 e 36 del regolamento (UE) 2016/679.

(18) I fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite dovrebbero notificare al titolare del sistema le giustificazioni delle eccezioni alla valutazione delle vulnerabilità richiesta per la valutazione del dispositivo crittografico sicuro per il portafoglio (WSCD) e dell'applicazione crittografica sicura per il portafoglio (WSCA), come stabilito all'allegato IV.

(19) La cancellazione di un certificato di conformità potrebbe avere gravi conseguenze, quali la revoca di tutte le unità di portafoglio installate. Di conseguenza gli organismi di certificazione dovrebbero prendere in considerazione la cancellazione soltanto laddove sia probabile che una vulnerabilità non sanata incida in modo significativo sull'affidabilità della soluzione di portafoglio o sull'affidabilità di un'altra soluzione di portafoglio.

(20) È opportuno istituire un processo specifico per l'aggiornamento dei sistemi nazionali di certificazione per gestire la transizione tra versioni successive dei sistemi, in particolare in relazione alle azioni che il titolare del certificato deve intraprendere per quanto concerne le future valutazioni, attività di manutenzione, di ricertificazione e valutazioni speciali.

(21) Al fine di agevolare la trasparenza, i fornitori di portafogli dovrebbero condividere pubblicamente le informazioni di sicurezza concernenti la loro soluzione di portafoglio.

(22) Qualora i sistemi nazionali di certificazione si basino su informazioni sulla garanzia provenienti da altri sistemi di certificazione o fonti, dovrebbe essere effettuata un'analisi della dipendenza al fine di verificare che la documentazione concernente la garanzia, ad esempio le relazioni in materia di garanzia e i certificati di conformità, sia disponibile e adeguata per la soluzione di portafoglio e il regime di identificazione elettronica nel contesto del quale detta soluzione è fornita. Tale analisi della dipendenza dovrebbe essere basata sulla valutazione dei rischi della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita. La valutazione dovrebbe stabilire se la documentazione in materia di garanzia disponibile per una determinata soluzione di portafoglio e il regime di identificazione elettronica nel contesto del quale detta soluzione è fornita sia adeguata per fornire garanzie corrispondenti al livello di valutazione desiderato. Nel corso della valutazione sarebbe inoltre opportuno aggiornare l'analisi delle dipendenze o riesaminarla completamente, se necessario.

(23) Gli organismi di certificazione dovrebbero rilasciare certificati di conformità nel contesto dei sistemi nazionali di certificazione, unitamente a una relazione di certificazione pubblicamente disponibile, di cui all'articolo 5 *quinquies*, paragrafo 2, lettera a), del regolamento (UE) n. 910/2014. La relazione di valutazione della certificazione associata dovrebbe essere messa a disposizione del gruppo di cooperazione.

(24) I sistemi nazionali di certificazione dovrebbero prevedere una valutazione di sorveglianza annuale al fine di garantire che i processi relativi alla gestione e alla manutenzione dei portafogli funzionino in modo efficace, ossia che funzionino come definito nelle politiche che stabiliscono i processi. La valutazione delle vulnerabilità biennale è un obbligo derivante dal regolamento (UE) n. 910/2014 atto a garantire che la soluzione di portafoglio continui a coprire adeguatamente i rischi e le minacce di cibersicurezza individuati nel registro dei rischi, compresa qualsiasi evoluzione del panorama delle minacce. Le nozioni di valutazioni di sorveglianza, valutazioni di ricertificazione e valutazioni speciali dovrebbero essere conformi alla norma EN ISO/IEC 17021-1:2015.

(25) Un ciclo di certificazione termina con la scadenza del certificato di conformità o con il rilascio di un certificato di conformità nuovo a seguito di una valutazione di ricertificazione avente esito positivo. La valutazione di ricertificazione dovrebbe contemplare una valutazione di tutti i componenti dell'oggetto della certificazione, compresa una valutazione dell'efficacia e, se del caso, una valutazione delle vulnerabilità. Durante la ricertificazione dovrebbe essere possibile riutilizzare i risultati di valutazioni precedenti concernenti i componenti che non sono cambiati.

(26) Quando è adottato un sistema europeo di certificazione della cibersicurezza, i sistemi nazionali di certificazione aventi il medesimo ambito di applicazione dovrebbero cessare di rilasciare certificazioni dopo un periodo di transizione di cui all'articolo 57, paragrafo 1, del regolamento (UE) 2019/881.

(27) I sistemi nazionali di certificazione dovrebbero basarsi su quadri esistenti e riutilizzare elementi di prova, se del caso, al fine di garantire l'armonizzazione e l'interoperabilità. Gli Stati membri possono concludere accordi per il riutilizzo transfrontaliero di sistemi di certificazione o di parti degli stessi. La Commissione europea e l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), in collaborazione con il gruppo di cooperazione, dovrebbero sostenere gli Stati membri nello sviluppo e nel mantenimento dei loro sistemi nazionali di certificazione, garantendo la condivisione delle conoscenze e delle migliori pratiche.

(28) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([9]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 30 settembre 2024.

(29) Le misure di cui al presente regolamento sono conformi al parere del comitato di cui all'articolo 48, paragrafo 1, 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 fissa norme di riferimento e stabilisce specifiche e procedure per la creazione di un quadro solido per la certificazione dei portafogli, da aggiornare periodicamente per tenere conto degli sviluppi tecnologici, della normazione e del lavoro svolto sulla base della raccomandazione (UE) 2021/946 relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale, in particolare dell'architettura e del quadro di riferimento.

*Articolo 2*

**Definizioni**

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «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;

2) «titolare del sistema»: un'organizzazione responsabile dello sviluppo e del mantenimento di un sistema di certificazione;

3) «oggetto della certificazione»: prodotti, processi e servizi, o una loro combinazione, ai quali si applicano i requisiti specificati;

4) «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;

5) «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;

([9]) 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).

6) «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;

7) «registro dei rischi»: un registro delle informazioni pertinenti per il processo di certificazione riguardanti i rischi individuati;

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

9) «organismo di certificazione»: un organismo terzo di valutazione della conformità che gestisce sistemi di certificazione;

10) «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;

11) «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;

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

13) «incidente»: un incidente quale definito all'articolo 6, punto 6, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([10]);

14) «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.

## CAPO II

## SISTEMI NAZIONALI DI CERTIFICAZIONE

### *Articolo 3*

### Istituzione di sistemi nazionali di certificazione

1. Gli Stati membri assegnano un titolare del sistema a ciascun sistema nazionale di certificazione.

2. L'oggetto della certificazione definita nei sistemi nazionali di certificazione è costituito dalla fornitura e dal funzionamento di soluzioni di portafoglio e dei regimi di identificazione elettronica nel contesto dei quali dette soluzioni sono fornite.

3. Conformemente al regolamento di esecuzione (UE) 2015/1502, l'oggetto della certificazione nei sistemi nazionali di certificazione comprende gli elementi seguenti:

a) i componenti software, comprese le impostazioni e le configurazioni di una soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale le soluzioni di portafoglio sono fornite;

b) i componenti e le piattaforme hardware su cui i componenti software di cui al punto b) vengono eseguiti o da cui tali componenti dipendono per operazioni critiche, nei casi in cui tali componenti sono forniti direttamente o indirettamente dalla soluzione di portafoglio e dal regime di identificazione elettronica nel contesto del quale detta soluzione è fornita e quando sono necessari per soddisfare il livello di garanzia desiderato per tali componenti software. Qualora i componenti e le piattaforme hardware non siano forniti dal fornitore del portafoglio, i sistemi nazionali di certificazione formulano ipotesi per la valutazione dei componenti hardware e delle piattaforme nell'ambito del quale può essere fornita resistenza nei confronti di aggressori con un potenziale di attacco elevato in linea con il regolamento di esecuzione (UE) 2015/1502 della Commissione, e specificano le attività di valutazione volte a confermare tali ipotesi di cui all'allegato IV;

([10]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) i processi che supportano la fornitura e il funzionamento di una soluzione di portafoglio, compresa la procedura di onboarding degli utenti di cui all'articolo 5 *bis* del regolamento (UE) n. 910/2014, che riguardano almeno la registrazione, la gestione dei mezzi elettronici e l'organizzazione a norma dell'allegato I, sezioni 2.1, 2.2 e 2.4, del regolamento di esecuzione (UE) 2015/1502.

4. I sistemi nazionali di certificazione comprendono una descrizione dell'architettura specifica delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite. Qualora coprano più di un'architettura specifica, i sistemi nazionali di certificazione prevedono un profilo per ciascuna architettura specifica.

5. Per ciascun profilo, i sistemi nazionali di certificazione stabiliscono almeno quanto segue:

a) l'architettura specifica di una soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita;

b) i controlli di sicurezza associati ai livelli di garanzia di cui all'articolo 8 del regolamento (UE) n. 910/2014;

c) un piano di valutazione elaborato conformemente alla sezione 7.4.1 della norma EN ISO/IEC 17065:2012;

d) i requisiti di sicurezza necessari per affrontare i rischi e le minacce di cibersicurezza che figurano nel registro dei rischi di cui all'allegato I del presente regolamento, fino al livello di garanzia richiesto, e al fine di conseguire, se del caso, gli obiettivi definiti all'articolo 51 del regolamento (UE) 2019/881;

e) una mappatura dei controlli di cui alla lettera b) del presente paragrafo in relazione ai componenti dell'architettura;

f) una descrizione del modo in cui i controlli di sicurezza, la mappatura, i requisiti di sicurezza e il piano di valutazione di cui alle lettere da b) a c) consentono ai fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale tali soluzioni sono fornite di affrontare adeguatamente i rischi e le minacce di cibersicurezza individuati nel registro dei rischi di cui alla lettera d), fino al livello di garanzia richiesto sulla base di una valutazione dei rischi per affinare e integrare i rischi e le minacce elencati nel registro dei rischi con rischi e minacce specifici dell'architettura.

6. Il piano di valutazione di cui al paragrafo 5, lettera c), elenca le attività di valutazione da includere nella valutazione di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite.

7. L'attività di valutazione di cui al paragrafo 6 impone ai fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite di fornire informazioni che soddisfino i requisiti di cui all'allegato II.

*Articolo 4*

**Requisiti generali**

1. I sistemi nazionali di certificazione coprono i requisiti funzionali, di cibersicurezza e in materia di protezione dei dati utilizzando, se disponibili e applicabili, i sistemi di certificazione seguenti:

a) sistemi europei di certificazione della cibersicurezza istituiti a norma del regolamento (UE) 2019/881, compreso l'EUCC;

b) sistemi nazionali di certificazione della cibersicurezza contemplati dall'EUCC, conformemente all'articolo 49 del regolamento di esecuzione (UE) 2024/482.

2. I sistemi nazionali di certificazione possono inoltre fare riferimento, se disponibili e applicabili, a:

a) altri sistemi nazionali di certificazione pertinenti;

b) norme internazionali, europee e nazionali;

c) specifiche tecniche che soddisfano le prescrizioni di cui all'allegato II del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([11]).

3. I sistemi nazionali di certificazione:

a) specificano gli elementi di cui alla sezione 6.5 della norma EN ISO/IEC 17067:2013;

b) sono attuati come un sistema di tipo 6, conformemente alla sezione 5.3.8 della norma EN ISO/IEC 17067:2013.

4. I sistemi nazionali di certificazione rispettano i requisiti seguenti:

a) soltanto i fornitori di cui all'articolo 5 *bis*, paragrafo 2, del regolamento (UE) n. 910/2014 sono idonei a ottenere il rilascio di certificati nel contesto dei sistemi nazionali di certificazione;

b) soltanto il marchio di fiducia è utilizzato come marchio di conformità;

c) i fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite includono riferimenti al regolamento (UE) n. 910/2014 e al presente regolamento quando fanno riferimento al sistema;

d) i fornitori di soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite completano la valutazione dei rischi del regime di cui all'articolo 3, paragrafo 5, lettera f), per individuare i rischi e le minacce specifici per la loro attuazione e propongono misure di trattamento adeguate per tutti i rischi e le minacce pertinenti;

e) le responsabilità e l'azione legale sono stabilite e includono riferimenti alla legislazione nazionale applicabile, che definisce le responsabilità e le possibili azioni legali, qualora la certificazione nel contesto del sistema sia utilizzata in modo fraudolento.

5. La valutazione di cui al paragrafo 4, lettera d), è condivisa con l'organismo di certificazione ai fini della valutazione.

*Articolo 5*

**Gestione degli incidenti e delle vulnerabilità**

1. I sistemi nazionali di certificazione contengono requisiti in materia di gestione degli incidenti e delle vulnerabilità conformemente ai paragrafi da 2 a 9.

2. Il titolare di un certificato di conformità di una soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale tale soluzione è fornita notificano senza indebito ritardo al proprio organismo di certificazione qualsiasi violazione o compromissione della soluzione di portafoglio o del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita che possa incidere sul suo rispetto dei requisiti di cui ai sistemi nazionali di certificazione.

3. Il titolare di un certificato di conformità stabilisce, mantiene e applica una politica e procedure di gestione delle vulnerabilità, tenendo conto delle procedure stabilite nelle norme europee e internazionali esistenti, compresa la norma EN ISO/IEC 30111:2019.

4. Il titolare del certificato di conformità notifica all'organismo di certificazione emittente le vulnerabilità e le modifiche che incidono sulla soluzione di portafoglio, sulla base di criteri definiti relativi all'impatto di tali vulnerabilità e modifiche.

5. Il titolare del certificato di conformità prepara una relazione sull'analisi dell'impatto delle vulnerabilità per qualsiasi vulnerabilità che incida sui componenti software della soluzione di portafoglio. Tale relazione contiene le informazioni seguenti:

a) l'impatto della vulnerabilità sulla soluzione di portafoglio certificata;

b) i possibili rischi associati alla prossimità o alla probabilità di un attacco;

([11]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) l'eventualità o meno che sia possibile porre rimedio alla vulnerabilità utilizzando i mezzi disponibili;

d) nei casi in cui sia possibile porre rimedio alla vulnerabilità utilizzando i mezzi disponibili, i possibili modi per porre rimedio a detta vulnerabilità.

6. Qualora sia richiesta la notifica di cui al paragrafo 4, il titolare del certificato di conformità trasmette senza indebito ritardo la relazione sull'analisi dell'impatto delle vulnerabilità di cui al paragrafo 5 all'organismo di certificazione.

7. Il titolare di un certificato di conformità stabilisce, mantiene e applica una politica di gestione delle vulnerabilità che soddisfa i requisiti di cui all'allegato I della legge sulla ciberresilienza ([12]).

8. I sistemi nazionali di certificazione stabiliscono obblighi di divulgazione delle vulnerabilità applicabili agli organismi di certificazione.

9. Il titolare di un certificato di conformità deve divulgare e registrare qualsiasi vulnerabilità pubblicamente nota e sanata nella soluzione di portafoglio o in uno degli archivi online di cui all'allegato V.

*Articolo 6*

**Mantenimento dei sistemi nazionali di certificazione**

1. I sistemi nazionali di certificazione prevedono un processo di riesame periodico del loro funzionamento. Tale processo mira a confermarne l'adeguatezza e a individuare gli aspetti da migliorare, tenendo conto dei riscontri forniti dai portatori di interessi.

2. I sistemi nazionali di certificazione comprendono disposizioni relative al loro mantenimento. Tale processo comprende come minimo i requisiti seguenti:

a) norme per la governance della definizione e dei requisiti dei sistemi nazionali di certificazione;

b) la fissazione di scadenze per il rilascio di certificati a seguito dell'adozione di versioni aggiornate dei sistemi nazionali di certificazione, tanto per i nuovi certificati di conformità quanto per quelli rilasciati in precedenza;

c) un riesame periodico dei sistemi nazionali di certificazione, al fine di garantire che i requisiti dei sistemi nazionali di certificazione siano applicati in modo coerente, tenendo conto quanto meno degli aspetti seguenti:

— richieste di chiarimenti rivolte al titolare del sistema in relazione ai requisiti del sistema nazionale di certificazione;

— riscontro fornito da portatori di interessi e altre parti interessate;

— reattività del titolare del sistema di certificazione nazionale alle richieste di informazioni;

d) norme per il monitoraggio dei documenti di riferimento e delle procedure per l'evoluzione delle versioni di riferimento dei sistemi nazionali di certificazione, compresi almeno i periodi di transizione;

e) un processo per garantire la copertura dei rischi e delle minacce di cibersicurezza più recenti elencati nel registro dei rischi di cui all'allegato I del presente regolamento;

f) un processo di gestione di altre modifiche nel contesto dei sistemi nazionali di certificazione.

([12]) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. I sistemi nazionali di certificazione prevedono requisiti per lo svolgimento di valutazioni sui prodotti attualmente certificati entro un determinato periodo di tempo dopo la revisione del sistema, o dopo la pubblicazione di nuove specifiche o norme, o di nuove versioni delle stesse, cui devono conformarsi le soluzioni di portafoglio e il regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite.

CAPO III

**REQUISITI RELATIVI AI TITOLARI DEI SISTEMI**

*Articolo 7*

**Requisiti generali**

1. I titolari dei sistemi elaborano e mantengono sistemi nazionali di certificazione e ne disciplinano le attività.

2. I titolari dei sistemi possono subappaltare a terzi i loro compiti, in tutto o in parte. In caso di subappalto a un soggetto privato, i titolari dei sistemi definiscono i doveri e le responsabilità di tutte le parti stipulando un contratto. I titolari dei sistemi restano responsabili di tutte le attività subappaltate svolte dai loro subcontraenti.

3. I titolari dei sistemi svolgono le loro attività di monitoraggio, se del caso, almeno sulla base delle informazioni seguenti:

a) informazioni provenienti da organismi di certificazione, organismi nazionali di accreditamento e autorità di vigilanza del mercato pertinenti;

b) informazioni derivanti da audit e indagini propri o di altre autorità;

c) reclami e ricorsi pervenuti a norma dell'articolo 15.

4. I titolari dei sistemi informano il gruppo di cooperazione in merito alle revisioni dei sistemi nazionali di certificazione. Tale notifica fornisce al gruppo di cooperazione informazioni adeguate ai fini della formulazione di raccomandazioni ai titolari dei sistemi e di pareri sui sistemi nazionali di certificazione aggiornati.

CAPO IV

**REQUISITI RELATIVI AI FORNITORI DI SOLUZIONI DI PORTAFOGLIO E DEI REGIMI DI IDENTIFICAZIONE ELETTRONICA NEL CONTESTO DEI QUALI DETTE SOLUZIONI SONO FORNITE**

*Articolo 8*

**Requisiti generali**

1. I sistemi nazionali di certificazione prevedono requisiti di cibersicurezza basati su una valutazione dei rischi di ciascuna architettura specifica supportata. Tali requisiti di cibersicurezza mirano a trattare i rischi e le minacce per la cibersicurezza individuati, come stabilito nel registro dei rischi di cui all'allegato I.

2. In linea con l'articolo 5 *bis*, paragrafo 23, del regolamento (UE) n. 910/2014, i sistemi nazionali di certificazione esigono che le soluzioni di portafoglio e i regimi di identificazione elettronica nel contesto dei quali dette soluzioni sono fornite siano resistenti nei confronti degli aggressori con un potenziale di attacco elevato per il livello di garanzia elevato di cui al regolamento di esecuzione (UE) 2015/1502.

3. I sistemi nazionali di certificazione stabiliscono criteri di sicurezza, tra cui figurano i requisiti seguenti:

a) il regolamento sulla ciberresilienza, se del caso, oppure i requisiti che soddisfano gli obiettivi di sicurezza di cui all'articolo 51 del regolamento (UE) 2019/881;

b) la definizione e l'attuazione di politiche e procedure relative alla gestione dei rischi associati al funzionamento di una soluzione di portafoglio, comprese l'individuazione e la valutazione dei rischi e l'attenuazione dei rischi individuati;

c) la definizione e l'attuazione di politiche e procedure relative alla gestione delle modifiche e alla gestione delle vulnerabilità conformemente all'articolo 5 del presente regolamento;

d) la definizione e l'attuazione di politiche e procedure di gestione delle risorse umane, compresi i requisiti in materia di competenza, affidabilità, esperienza, formazione in materia di sicurezza e qualifiche del personale coinvolto nello sviluppo o nel funzionamento della soluzione di portafoglio;

e) i requisiti relativi all'ambiente operativo della soluzione di portafoglio, anche sotto forma di ipotesi sulla sicurezza dei dispositivi e delle piattaforme su cui sono eseguiti i componenti software della soluzione di portafoglio, compresi i dispositivi crittografici sicuri per il portafoglio e, ove applicabile e pertinente, i requisiti di valutazione della conformità atti a confermare che tali ipotesi sono verificate sui dispositivi e sulle piattaforme pertinenti;

f) per ciascuna ipotesi non corroborata da un certificato di conformità o da altre informazioni di garanzia accettabili, una descrizione del meccanismo utilizzato dal fornitore del portafoglio per applicare l'ipotesi, nonché una giustificazione del fatto che il meccanismo è sufficiente a garantire che l'ipotesi in questione sia verificata;

g) la definizione e l'attuazione di misure volte a garantire l'uso di una versione attualmente certificata della soluzione di portafoglio.

4. I sistemi nazionali di certificazione contengono requisiti funzionali relativi ai meccanismi di aggiornamento per ogni componente software delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite per le operazioni che figurano nell'allegato III.

5. I sistemi nazionali di certificazione esigono che il richiedente la certificazione fornisca o metta altrimenti a disposizione dell'organismo di certificazione le informazioni e la documentazione seguenti:

a) prove relative alle informazioni di cui all'allegato IV, punto 1, compresi, se necessario, i dettagli sulla soluzione di portafoglio e sul relativo codice sorgente, tra cui:

— *informazioni sull'architettura:* per ciascun componente della soluzione di portafoglio (compresi i componenti di prodotto, processo e servizio), una descrizione delle sue proprietà essenziali di sicurezza, comprese le sue dipendenze esterne;

— *controlli e livelli di garanzia:* per ciascun controllo di sicurezza della soluzione di portafoglio, una descrizione del controllo e del livello di garanzia richiesto, sulla base dell'allegato del regolamento di esecuzione (UE) 2015/1502, che stabilisce una serie di specifiche tecniche e procedure che si applicano ai vari controlli attuati dai mezzi di identificazione elettronica;

— *mappatura dei controlli relativi ai componenti dell'architettura:* una descrizione del modo in cui i controlli del portafoglio sono attuati utilizzando i diversi componenti della soluzione di portafoglio, sulla base di una logica che spieghi il motivo per cui è richiesto un determinato livello di garanzia, così come del modo in cui il controllo è attuato con tutti gli aspetti di sicurezza richiesti al livello adeguato;

— *motivazione e giustificazione della copertura dei rischi:* una giustificazione degli elementi seguenti:

— mappatura dei controlli dei componenti;

— idoneità del piano di valutazione proposto a coprire adeguatamente tutti i controlli;

— la copertura conseguita dai controlli dei rischi e delle minacce di cibersicurezza identificati nel registro dei rischi, completati dai controlli dei rischi e delle minacce specifici per l'attuazione, al livello di garanzia adeguato;

b) le informazioni elencate nell'allegato V;

c) un elenco completo dei certificati di conformità e di altre informazioni sulla garanzia utilizzati come prova durante le attività di valutazione;

d) qualsiasi altra informazione pertinente per le attività di valutazione.

CAPO V

**REQUISITI RELATIVI AGLI ORGANISMI DI CERTIFICAZIONE**

*Articolo 9*

**Requisiti generali**

1. Gli organismi di certificazione sono accreditati dagli organismi nazionali di accreditamento designati a norma del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([13]) conformemente alla norma EN ISO/IEC 17065:2012, a condizione che soddisfino i requisiti stabiliti nei sistemi nazionali di certificazione conformemente al paragrafo 2.

2. Ai fini dell'accreditamento, gli organismi di certificazione soddisfano tutti i seguenti requisiti di competenza:

a) conoscenze dettagliate e tecniche in merito alle architetture pertinenti di una soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, nonché delle minacce e dei rischi pertinenti per tali architetture;

b) conoscenza in merito alle soluzioni di sicurezza disponibili e alle loro proprietà a norma dell'allegato del regolamento di esecuzione (UE) 2015/1502;

c) conoscenza delle attività svolte in virtù dei certificati di conformità applicati ai componenti della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, in quanto oggetto della certificazione;

d) conoscenze dettagliate in merito al sistema nazionale di certificazione applicabile istituito conformemente al capo II.

3. Gli organismi di certificazione svolgono le loro attività di vigilanza in particolare sulla base delle informazioni seguenti:

a) informazioni provenienti dagli organismi nazionali di accreditamento e dalle autorità di vigilanza del mercato pertinenti;

b) informazioni derivanti da audit e indagini propri o di altre autorità;

c) reclami e ricorsi pervenuti a norma dell'articolo 15.

*Articolo 10*

**Subappalto**

Gli organismi di certificazione possono subappaltare a terzi le attività di valutazione di cui all'articolo 13. Qualora le attività di valutazione siano oggetto di subappalto, i sistemi nazionali di certificazione stabiliscono quanto segue:

1) tutti i subappaltatori dell'organismo di certificazione che esegue le attività di valutazione soddisfano, se del caso e in funzione delle attività da svolgere, i requisiti di norme armonizzate quali EN ISO/IEC 17025:2017 per le prove, EN ISO/IEC 17020:2012 per le ispezioni, EN ISO/IEC 17021-1:2015 per l'audit ed EN ISO/IEC 17029:2019 per la convalida e la verifica;

2) gli organismi di certificazione si assumono la responsabilità di tutte le attività di valutazione esternalizzate ad altri organismi e dimostrano di aver adottato misure adeguate durante il loro accreditamento, anche facendo affidamento sull'accreditamento dei loro subappaltatori, se del caso;

3) il grado di ottenimento del previo accordo all'esternalizzazione da parte dei titolari dei sistemi o del cliente la cui soluzione di portafoglio è certificata nel quadro del sistema di certificazione.

([13]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

*Articolo 11*

**Notifica all'organismo di vigilanza**

Gli organismi di certificazione notificano all'organismo di vigilanza di cui all'articolo 46 *bis*, paragrafo 1, del regolamento (UE) n. 910/2014 il rilascio, la sospensione e l'annullamento dei certificati di conformità delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite.

*Articolo 12*

**Gestione degli incidenti e delle vulnerabilità**

1. Gli organismi di certificazione sospendono senza indebito ritardo il certificato di conformità delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite dopo aver confermato che la violazione o compromissione della sicurezza notificata incide sulla conformità rispetto ai requisiti dei sistemi nazionali di certificazione nell'ambito della soluzione di portafoglio o del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita.

2. Gli organismi di certificazione annullano il certificato di conformità sospeso a seguito di una violazione o compromissione della sicurezza cui non è stato posto rimedio tempestivamente.

3. Gli organismi di certificazione annullano tempestivamente i certificati di conformità qualora a una vulnerabilità individuata non sia stato posto rimedio tempestivamente in modo proporzionato alla sua gravità e al suo potenziale impatto, conformemente all'articolo 5 *quater*, paragrafo 4, e all'articolo 5 *sexies*, paragrafo 2, del regolamento (UE) n. 910/2014.

CAPO VI

**ATTIVITÀ DI VALUTAZIONE DELLA CONFORMITÀ**

*Articolo 13*

**Attività di valutazione**

1. I sistemi nazionali di certificazione prevedono metodi e procedure che gli organismi di valutazione della conformità devono utilizzare nello svolgimento delle loro attività di valutazione conformemente alla norma EN ISO/IEC 17065:2012, che riguardano quanto meno gli aspetti seguenti:

a) i metodi e le procedure per lo svolgimento delle attività di valutazione, comprese quelle relative al dispositivo crittografico sicuro per il portafoglio, di cui all'allegato IV;

b) l'audit dell'attuazione della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, sulla base del registro dei rischi di cui all'allegato I e integrato, ove necessario, da rischi specifici per l'attuazione;

c) le attività di collaudo funzionale basate, laddove disponibili e adeguate, su serie di prove definite in base a norme o specifiche tecniche;

d) la valutazione dell'esistenza e dell'idoneità dei processi di manutenzione, compresa quanto meno la gestione delle versioni, la gestione degli aggiornamenti e la gestione delle vulnerabilità;

e) la valutazione dell'efficacia operativa dei processi di manutenzione, compresa quanto meno la gestione delle versioni, la gestione degli aggiornamenti e la gestione delle vulnerabilità;

f) l'analisi della dipendenza messa a disposizione dal fornitore del portafoglio, compresa una metodologia atta a valutare l'accettabilità delle informazioni sulla garanzia, che comprende gli elementi di cui all'allegato VI;

g) la valutazione delle vulnerabilità, al livello adeguato, comprendente:

— un riesame della progettazione della soluzione di portafoglio e, se del caso, del suo codice sorgente;

— lo svolgimento di prove della resistenza della soluzione di portafoglio nei confronti di aggressori con un potenziale di attacco «elevato» ai sensi della sezione 2.2.1 dell'allegato del regolamento di esecuzione (UE) 2015/1502;

h) la valutazione dell'evoluzione del panorama delle minacce e del suo impatto sulla copertura dei rischi da parte della soluzione di portafoglio, al fine di stabilire quali attività di valutazione siano necessarie in relazione ai vari componenti della soluzione di portafoglio.

2. I sistemi nazionali di certificazione contemplano una valutazione volta a stabilire se l'attuazione delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite corrispondono all'architettura di cui all'articolo 3, paragrafo 5, lettera a), nonché una valutazione volta a stabilire se il piano di valutazione proposto unitamente all'attuazione corrisponde al piano di valutazione di cui all'articolo 3, paragrafo 5, lettera c).

3. I sistemi nazionali di certificazione stabiliscono norme in materia di campionamento, al fine di evitare il ripetersi di attività di valutazione identiche e di concentrarsi su attività specifiche di una determinata variante. Tali norme di campionamento consentono di effettuare prove funzionali e di sicurezza soltanto su un campione di varianti di un componente obiettivo di una soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita e su un campione di dispositivi obiettivo. I sistemi nazionali di certificazione impongono a tutti gli organismi di certificazione di giustificare il ricorso al campionamento.

4. I sistemi nazionali di certificazione richiedono la valutazione, da parte dell'organismo di certificazione, dell'applicazione crittografica sicura per il portafoglio sulla base dei metodi e delle procedure di cui all'allegato IV.

*Articolo 14*

**Attività di certificazione**

1. I sistemi nazionali di certificazione stabiliscono un'attività di attestazione ai fini del rilascio di un certificato di conformità, conformemente alla sezione V, lettera a), della norma EN ISO/IEC 17067:2013, tabella 1, tenendo conto degli aspetti seguenti:

a) il contenuto del certificato di conformità di cui all'allegato VII;

b) il modo in cui i risultati della valutazione devono essere comunicati nella relazione pubblica di certificazione, comprendente almeno una sintesi del piano preliminare di audit e convalida di cui all'allegato VIII;

c) il contenuto dei risultati della valutazione riportati nella relazione di valutazione della certificazione, compresi gli elementi di cui all'allegato VIII.

2. La relazione di valutazione della certificazione può essere messa a disposizione del gruppo di cooperazione e della Commissione.

*Articolo 15*

**Reclami e ricorsi**

I sistemi nazionali di certificazione prevedono procedure o riferimenti alla legislazione nazionale applicabile che definiscono il meccanismo per presentare e gestire efficacemente reclami e ricorsi in relazione all'attuazione del sistema di certificazione stesso o a un certificato di conformità rilasciato. Tali procedure prevedono la comunicazione al reclamante di informazioni sullo stato di avanzamento del procedimento e sulla decisione adottata, nonché informazioni al reclamante sul diritto a un ricorso giurisdizionale effettivo. I sistemi nazionali di certificazione esigono che tutti i reclami e i ricorsi che non sono stati o non possono essere risolti dall'organismo di certificazione siano rinviati al titolare del sistema per la valutazione e la risoluzione.

*Articolo 16*

**Attività di vigilanza**

1. I sistemi nazionali di certificazione impongono agli organismi di certificazione di attuare attività di vigilanza consistenti nella valutazione dei processi in combinazione con prove o ispezioni casuali.

2. I sistemi nazionali di certificazione prevedono l'obbligo per i titolari dei sistemi di monitorare il rispetto, da parte degli organismi di certificazione, dei loro obblighi a norma del regolamento (UE) n. 910/2014 e dei sistemi nazionali di certificazione, se del caso.

3. I sistemi nazionali di certificazione prevedono l'obbligo per gli organismi di certificazione di monitorare quanto segue:

a) il rispetto, da parte dei titolari di un certificato di conformità rilasciato nell'ambito di sistemi nazionali di certificazione, dei loro obblighi in materia di certificazione a norma del regolamento (UE) n. 910/2014 e dei sistemi nazionali di certificazione;

b) la conformità della soluzione di portafoglio certificata ai requisiti stabiliti nei sistemi nazionali di certificazione.

*Articolo 17*

**Conseguenze della non conformità**

I sistemi nazionali di certificazione stabiliscono le conseguenze della non conformità di una soluzione di portafoglio certificata e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita ai requisiti di cui al presente regolamento. Tra tali conseguenze figurano gli aspetti seguenti:

1) l'obbligo per l'organismo di certificazione di informare il titolare del certificato di conformità e di chiedere a quest'ultimo di applicare misure correttive;

2) l'obbligo per l'organismo di certificazione di informare altre autorità di vigilanza del mercato pertinenti qualora la non conformità riguardi la legislazione dell'Unione pertinente;

3) le condizioni per l'attuazione di azioni correttive da parte del titolare del certificato di conformità;

4) le condizioni per la sospensione di un certificato di conformità da parte dell'organismo di certificazione e per il ripristino di tale certificato una volta sanata la non conformità;

5) le condizioni per l'annullamento di un certificato di conformità da parte dell'organismo di certificazione;

6) le conseguenze della non conformità da parte dell'organismo di certificazione ai requisiti del sistema nazionale di certificazione.

CAPO VII

**CICLO DI CERTIFICAZIONE**

*Articolo 18*

**Ciclo di certificazione**

1. La validità dei certificati di conformità rilasciati nell'ambito dei sistemi nazionali di certificazione è soggetta ad attività di valutazione periodiche svolte dall'organismo di certificazione conformemente ai requisiti di cui all'allegato IX.

2. I sistemi nazionali di certificazione prevedono un processo per la ricertificazione delle soluzioni di portafoglio e del regime di identificazione elettronica nel contesto del quale dette soluzioni sono fornite, su richiesta del titolare del certificato di conformità prima della scadenza del certificato di conformità iniziale. Tale processo di ricertificazione comprende una valutazione completa della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, compresa una valutazione delle vulnerabilità, secondo i principi di cui all'allegato IX.

3. I sistemi nazionali di certificazione prevedono un processo di gestione delle modifiche di una soluzione di portafoglio certificata e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita. Tale processo contempla norme volte a stabilire se una modifica debba essere oggetto di una valutazione speciale di cui al paragrafo 4 o della verifica dell'efficacia operativa dei processi di manutenzione di cui all'allegato IV.

4. I sistemi nazionali di certificazione prevedono un processo di valutazione speciale conformemente alla norma EN ISO/IEC 17065:2012. Tale processo di valutazione speciale contempla una selezione delle attività da svolgere al fine di affrontare la questione specifica che ha determinato l'avvio della valutazione speciale.

5. I sistemi nazionali di certificazione stabiliscono norme relative all'annullamento di un certificato di conformità.

CAPO VIII

**CONSERVAZIONE DELLE REGISTRAZIONI E PROTEZIONE DELLE INFORMAZIONI**

*Articolo 19*

**Conservazione delle registrazioni**

1. I sistemi nazionali di certificazione prevedono requisiti per gli organismi di certificazione relativi a un sistema di registrazione di tutte le informazioni pertinenti prodotte in relazione alle attività di valutazione della conformità da essi svolte, compresi i dati rilasciati e ricevuti dai fornitori di soluzioni di portafoglio e dei regimi di identificazione elettronica nel contesto dei quali dette soluzioni sono fornite. Le registrazioni di tali informazioni sono conservate in modo sicuro. Le registrazioni possono essere conservate elettronicamente e rimangono accessibili per tutto il tempo prescritto dal diritto dell'Unione o dal diritto nazionale e per almeno cinque anni dopo l'annullamento o la scadenza del certificato di conformità pertinente.

2. I sistemi nazionali di certificazione stabiliscono requisiti affinché il titolare del certificato di conformità conservi le informazioni seguenti in modo sicuro ai fini del presente regolamento e per almeno cinque anni dopo l'annullamento o la scadenza del certificato di conformità pertinente:

a) registrazioni delle informazioni fornite all'organismo di certificazione o a uno qualsiasi dei suoi subappaltatori durante il processo di certificazione;

b) campioni di componenti hardware inclusi nell'ambito di applicazione della certificazione per la soluzione di portafoglio.

3. I sistemi nazionali di certificazione impongono al titolare del certificato di conformità di mettere le informazioni di cui al paragrafo 1, su richiesta, a disposizione dell'organismo di certificazione o dell'organismo di vigilanza di cui all'articolo 46 *bis*, paragrafo 1, del regolamento (UE) n. 910/2014.

*Articolo 20*

**Protezione delle informazioni**

Nell'ambito dei sistemi nazionali di certificazione, tutte le persone o organizzazioni cui è concesso l'accesso a informazioni nello svolgimento delle attività nell'ambito del sistema nazionale di certificazione sono tenute a garantire la sicurezza e la protezione dei segreti commerciali e di altre informazioni riservate, nonché a preservare i diritti di proprietà intellettuale, e ad adottare le misure tecniche e organizzative necessarie e adeguate al fine di garantire tale riservatezza.

CAPO IX

**DISPOSIZIONI FINALI**

*Articolo 21*

**Transizione verso un sistema europeo di certificazione della cibersicurezza**

Il presente regolamento è soggetto a riesame all'adozione del primo sistema europeo di certificazione della cibersicurezza per le soluzioni di portafoglio e dei regimi di identificazione elettronica nel contesto dei quali dette soluzioni sono fornite, con l'obiettivo di tenere conto del contributo di tale sistema europeo di certificazione della cibersicurezza alla certificazione generale delle soluzioni di portafoglio e dei regimi di identificazione elettronica nel contesto dei quali dette soluzioni sono fornite.

*Articolo 22*

**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*

**REGISTRO DEI RISCHI PER I PORTAFOGLI EUROPEI DI IDENTITÀ DIGITALE**

**Introduzione**

Il registro dei rischi descrive i rischi e le minacce principali per la sicurezza e la tutela della vita privata che si applicano ai portafogli e che devono essere adeguatamente affrontati nel contesto di ogni architettura e nell'attuazione dei portafogli. I **rischi di livello elevato** (sezione I) sono correlati all'uso di portafogli da parte degli utenti e delle parti facenti affidamento sulla certificazione e sono associati a minacce dirette rivolte contro le risorse dei portafogli. Sono inoltre individuati alcuni **rischi a livello di sistema** (sezione II) per i portafogli, che in genere deriverebbero da una combinazione di minacce che si applicano all'intero sistema di portafoglio.

| Tipo di rischio | Identificativo del rischio | Titoli dei rischi correlati |
|---|---|---|
| **Rischi di livello elevato per i portafogli** | R1 | Creazione o uso di un'identità elettronica esistente |
| | R2 | Creazione o uso di un'identità elettronica falsa |
| | R3 | Creazione o uso di attributi falsi |
| | R4 | Furto di identità |
| | R5 | Furto di dati |
| | R6 | Divulgazione di dati |
| | R7 | Manipolazione di dati |
| | R8 | Perdita di dati |
| | R9 | Transazione non autorizzata |
| | R10 | Manipolazione di transazioni |
| | R11 | Ripudio |
| | R12 | Divulgazione di dati relativi a transazioni |
| | R13 | Perturbazione del servizio |
| | R14 | Sorveglianza |
| **Rischi correlati al sistema** | SR1 | Sorveglianza su larga scala |
| | SR2 | Danni alla reputazione |
| | SR3 | Non conformità giuridica |

Il registro individua inoltre **minacce tecniche** (sezione III) riguardanti l'attuazione della soluzione di portafoglio. Tali minacce sono connesse ai rischi di livello elevato, nel senso che ciascuna di esse potrebbe essere utilizzata per determinare numerosi rischi di livello elevato.

| Tipo di minaccia | Identificativo della minaccia | Titoli delle minacce correlate | Sottocategorie di minacce |
|---|---|---|---|
| **Minacce tecniche** | TT1 | Attacchi fisici | 1.1. *Furto* |
| | | | 1.2. *Fuga di informazioni* |
| | | | 1.3. *Manomissione* |
| | TT2 | Errori e configurazioni errate | 2.1. *Errori commessi nella gestione di un sistema informatico* |
| | | | 2.2. *Errori a livello di applicazione o errori nell'utilizzo* |
| | | | 2.3. *Errori in termini di sviluppo e tempi e configurazioni errate dei sistemi* |

| Tipo di minaccia | Identificativo della minaccia | Titoli delle minacce correlate | Sottocategorie di minacce |
|---|---|---|---|
| | TT3 | Uso di risorse inaffidabili | 3.1. *Uso errato o configurazione errata dei componenti del portafoglio* |
| | TT4 | Guasto e indisponibilità | 4.1. *Guasto o disfunzione di apparecchiature, dispositivi o sistemi* |
| | | | 4.2. *Perdita di risorse* |
| | | | 4.3. *Perdita di servizi di assistenza* |
| | TT5 | Azioni malevole | 5.1. *Intercettazione di informazioni* |
| | | | 5.2. *Phishing e spoofing* |
| | | | 5.3. *Riproduzione di messaggi* |
| | | | 5.4. *Attacco di forza bruta* (brute force) |
| | | | 5.5. *Vulnerabilità del software* |
| | | | 5.6. *Attacchi alla catena di approvvigionamento* |
| | | | 5.7. *Malware* |
| | | | 5.8. *Previsione di numeri casuali* |

Infine, il registro **elenca le minacce dirette per i portafogli** e ciascuna di esse è associata a una selezione (non esaustiva) dei rischi (sezione IV).

*SEZIONE I*

***Rischi di livello elevato per i portafogli***

**R1. Creazione o uso di un'identità elettronica esistente**

Si definisce creazione o uso di un'identità elettronica la creazione, in un portafoglio, di un'identità elettronica che esiste nel mondo reale ed è assegnata a un altro utente. In sostanza, questo rischio comporta il rischio di furto di identità (R4) e di transazioni non autorizzate (R9).

**R2. Creazione o uso di un'identità elettronica falsa**

Si definisce creazione o uso di un'identità elettronica falsa la creazione, in un portafoglio, di un'identità elettronica che non esiste nel mondo reale.

**R3. Creazione o uso di attributi falsi**

Si definisce creazione o uso di attributi falsi la creazione o l'uso di attributi che non possono essere convalidati per essere rilasciati dal fornitore dichiarato e non possono essere affidabili.

**R4. Furto di identità**

Si definisce furto di identità l'acquisizione non autorizzata dell'unità di portafoglio o la perdita di fattori di autenticazione che consentono di assumere l'identità di una persona.

**R5. Furto di dati**

Si definisce furto di dati un'estrazione non autorizzata di dati. Il furto di dati è inoltre associato a minacce quali l'intercettazione di dati (acquisizione non autorizzata di dati in transito) e la decifratura di dati (decodifica non autorizzata di dati crittografati), che in alcuni casi possono portare alla divulgazione di dati (R6).

**R6. Divulgazione di dati**

Si definisce divulgazione di dati l'esposizione non autorizzata di dati personali, comprese categorie particolari di dati personali. Il rischio di violazione della vita privata è molto simile se considerato dal punto di vista della tutela della vita privata piuttosto che della sicurezza.

**R7. Manipolazione di dati**

Si definisce manipolazione di dati la modifica non autorizzata di dati.

**R8. Perdita di dati**

Si definisce perdita di dati la situazione in cui i dati conservati nel portafoglio vanno persi a causa di un uso improprio o di un'azione malevola. Tale rischio è spesso un rischio secondario della manipolazione di dati (R7) o della perturbazione del servizio (R13), quando i dati non possono essere ripristinati in tutto o in parte.

**R9. Transazione non autorizzata**

Si definiscono transazioni non autorizzate le attività operative svolte senza l'autorizzazione dell'utente del portafoglio o senza che quest'ultimo ne sia a conoscenza. In numerosi casi, una transazione non autorizzata può comportare il furto di identità (R4) o la divulgazione di dati (R6). Riguarda anche transazioni non autorizzate quali l'uso improprio di chiavi crittografiche.

**R10. Manipolazione di transazioni**

Si definisce manipolazione di transazioni la modifica non autorizzata di operazioni nel portafoglio. La manipolazione di transazioni è un attacco all'integrità ed è connessa a una violazione dell'integrità dei dati.

**R11. Ripudio**

Si definisce ripudio una situazione nella quale un portatore di interessi può negare di aver compiuto un'azione o di essere coinvolto in una transazione e altri portatori di interessi non dispongono di elementi di prova adeguati per contraddirlo.

**R12. Divulgazione di dati relativi a transazioni**

Si definisce divulgazione di dati relativi a transazioni la divulgazione di informazioni relative a informazioni concernenti una transazione tra portatori di interessi.

**R13. Perturbazione del servizio**

Si definisce perturbazione del servizio una interruzione o un peggioramento del normale funzionamento del portafoglio. Un tipo specifico di perturbazione del servizio è considerata l'esclusione dell'utente, definita come l'impossibilità per un utente di accedere al proprio account o portafoglio.

**R14. Sorveglianza**

Si definisce sorveglianza, o monitoraggio, il tracciamento o l'osservazione non autorizzato/a delle attività, delle comunicazioni o dei dati di un utente del portafoglio. La sorveglianza è spesso legata all'inferenza, definita come la deduzione di informazioni sensibili o personali da dati apparentemente innocui.

*SEZIONE II*

***Rischi correlati al sistema***

Tali rischi non sono utilizzati nell'elenco delle minacce, in quanto costituiscono solitamente una conseguenza di molteplici minacce, ripetute in modo tale da minacciare l'intero sistema.

**SR1. Sorveglianza su larga scala**

Si definisce sorveglianza su larga scala il tracciamento o l'osservazione delle attività di numerosi utenti attraverso la comunicazione o i dati del portafoglio a loro corrispondenti. La sorveglianza su larga scala è spesso associata alla sorveglianza (R14) e all'inferenza su scala globale, nel contesto delle quali informazioni concernenti numerosi utenti sono combinate al fine di dedurre dati sensibili o personali in merito agli utenti o di individuare tendenze statistiche che possono essere utilizzate per progettare ulteriori attacchi.

**SR2. Danni alla reputazione**

Si definisce danno alla reputazione il danno causato alla reputazione di un'organizzazione o di un organismo governativo. I danni alla reputazione deriveranno anche da altri rischi quando una violazione o un incidente è oggetto di copertura da parte dei media, i quali presentano l'organizzazione in modo sfavorevole. I danni alla reputazione possono comportare ulteriori rischi, quali la perdita di fiducia, dovuta a dubbi ragionevoli nutriti dagli utenti, e la perdita di ecosistema, quando l'intero ecosistema collassa.

**SR3. Non conformità giuridica**

Si definisce non conformità giuridica una situazione nella quale non è possibile rispettare le leggi, le normative o le norme pertinenti. Nel contesto di un portafoglio, poiché la sicurezza e la riservatezza della soluzione rappresentano obblighi giuridici, è probabile che tutte le minacce portino a una qualche forma di non conformità giuridica.

*SEZIONE III*

***Minacce tecniche***

Le minacce tecniche non sono tutte legate a rischi specifici sui portafogli, in quanto molte di esse costituiscono mezzi che potrebbero essere utilizzati per attuare attacchi corrispondenti a numerosi rischi diversi.

**TT1. Attacchi fisici**

1.1. *Furto*

Si definisce furto un furto di dispositivi in grado di alterare il corretto funzionamento del portafoglio (nel caso in cui il dispositivo sia rubato e l'unità di portafoglio non sia adeguatamente protetta). Ciò può contribuire a numerosi rischi, tra cui il furto di identità (R4), il furto di dati (R5) e transazioni non autorizzate (R9).

1.2. *Fuga di informazioni*

Si definisce fuga di informazioni un accesso non autorizzato, un'esposizione di informazioni o una condivisione dopo un accesso fisico al portafoglio. Ciò può contribuire in particolare alla divulgazione di dati (R6) e al furto di dati (R5).

1.3. *Manomissione*

Si definisce manomissione una violazione dell'integrità di uno o più componenti dell'unità di portafoglio o dei componenti su cui si basa l'unità di portafoglio, ad esempio il dispositivo utente o il suo sistema operativo. Ciò può contribuire in particolare alla manipolazione di dati (R7), alla perdita di dati (R8) e alla manipolazione di transazioni (R10). Quando la manomissione riguarda componenti software, può contribuire a numerosi rischi.

**TT2. Errori e configurazioni errate**

2.1. *Errori commessi nella gestione di un sistema informatico*

Si definiscono errori commessi nella gestione di un sistema informatico: la fuga di informazioni, la condivisione delle stesse o i danni causati dall'uso improprio di risorse informatiche da parte degli utenti (mancanza di conoscenza delle caratteristiche dell'applicazione) o da una configurazione o una gestione impropria delle risorse informatiche.

2.2. *Errori a livello di applicazione o errori nell'utilizzo*

Si definiscono errori a livello di applicazione o errori nell'utilizzo le disfunzioni dell'applicazione dovute a un errore nell'applicazione stessa o a un errore commesso da uno degli utenti (utenti del portafoglio e parti facenti affidamento sulla certificazione).

2.3. *Errori in termini di sviluppo e tempi e configurazioni errate dei sistemi*

Si definiscono errori in termini di sviluppo e tempi e configurazioni errate dei sistemi le disfunzioni o vulnerabilità causate da risorse informatiche o processi operativi sviluppati o configurati in modo errato (specifiche inadeguate dei prodotti informatici, utilizzabilità inadeguata, interfacce non sicure, flussi inadeguati di politiche e procedure, errori di progettazione).

**TT3. Uso di risorse inaffidabili**

Si definisce uso di risorse inaffidabili un'attività che provoca danni non intenzionali dovuti a rapporti fiduciari mal definiti, come riporre fiducia in un prestatore terzo senza disporre di garanzie sufficienti.

3.1. *Uso errato o configurazione errata dei componenti del portafoglio*

Si definisce uso errato o configurazione errata dei componenti del portafoglio un danno non intenzionale ai componenti del portafoglio dovuto a un uso errato o una configurazione errata da parte degli utenti del portafoglio o di sviluppatori non sufficientemente formati oppure dovuto alla mancanza di adattamento ai cambiamenti nel panorama delle minacce, in genere all'uso di componenti di terzi vulnerabili o di piattaforme di runtime.

**TT4. Guasto e indisponibilità**

4.1. *Guasto o disfunzione di apparecchiature, dispositivi o sistemi*

SI definisce guasto o disfunzione di apparecchiature un danno non intenzionale alle risorse informatiche dovuto a un guasto o a una disfunzione dell'apparecchiatura in questione, compresi l'infrastruttura del fornitore e i dispositivi dell'utente.

4.2. *Perdita di risorse*

Si definisce perdita di risorse una indisponibilità o una disfunzione dovuta ad indisponibilità di tali risorse, ad esempio di parti necessarie per la manutenzione.

4.3. *Perdita di servizi di assistenza*

Si definisce perdita di servizi di assistenza una indisponibilità o una disfunzione dovuta all'indisponibilità dei servizi di assistenza necessari per il corretto funzionamento del sistema, compresa la connettività di rete dell'infrastruttura del fornitore e del dispositivo dell'utente.

**TT5. Azioni malevole**

5.1. *Intercettazione di informazioni*

Si definisce intercettazione di informazioni l'acquisizione di informazioni protette in modo non adeguato nella trasmissione, compresi gli attacchi «man-in-the-middle» (MITM).

5.2. *Phishing e spoofing*

Si definisce *phishing* l'acquisizione di informazioni fornite dall'utente a seguito di un'interazione ingannevole, spesso associata allo *spoofing* di mezzi di comunicazione e siti web legittimi. Tali minacce sono rivolte all'utente e in genere contribuiscono al furto di identità (R4) e a transazioni non autorizzate (R9), spesso attraverso il furto di dati (R5) o la divulgazione di dati (R6).

5.3. *Riproduzione di messaggi*

Si definisce riproduzione di messaggi il riutilizzo di messaggi precedentemente intercettati al fine di effettuare transazioni non autorizzate, spesso a livello di protocollo. Tale minaccia tecnica contribuisce principalmente a transazioni non autorizzate, che possono quindi comportare altri rischi, a seconda della transazione.

5.4. *Attacco di forza bruta (brute force)*

Si definisce attacco di forza bruta una violazione della sicurezza, spesso della riservatezza, commessa effettuando un gran numero di interazioni fino a quando le risposte non forniscono informazioni preziose.

5.5. *Vulnerabilità del software*

La minaccia relativa alle vulnerabilità del software è una violazione della sicurezza dovuta allo sfruttamento di una vulnerabilità del software presente nei componenti del portafoglio o nei componenti software e hardware utilizzati nell'attuazione del portafoglio, comprese le vulnerabilità pubblicate e quelle non pubblicate («zero day»).

5.6. *Attacchi alla catena di approvvigionamento*

Si definisce attacco alla catena di approvvigionamento una violazione della sicurezza attraverso attacchi commessi nei confronti di un prestatore del fornitore del portafoglio o dei suoi utenti al fine di consentire ulteriori attacchi al portafoglio stesso.

5.7. *Malware*

Si definisce malware una violazione della sicurezza dovuta ad applicazioni malevole che compiono azioni indesiderate e illegittime sul portafoglio.

5.8. *Previsione di numeri casuali*

Si definisce previsione di numeri casuali la possibilità di attacchi di forza bruta mediante previsione parziale o completa di numeri generati in modo casuale.

*SEZIONE IV*

***Minacce per i portafogli***

Quest'ultima sezione presenta una selezione di scenari tipici di minaccia specifici per i portafogli, che sono mappati in relazione ai rischi di livello elevato correlati principali di cui sopra. Nell'elenco figurano minacce che devono essere gestite, tuttavia non si tratta di un elenco esaustivo delle minacce, che dipende in larga misura dall'architettura della soluzione di portafoglio selezionata e dall'evoluzione del panorama delle minacce. Inoltre, nella valutazione dei rischi e nelle misure proposte, il fornitore del portafoglio può essere responsabile soltanto per i componenti rientranti nell'ambito di applicazione della certificazione (*).

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata* (*) | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR1 | Un aggressore può revocare pseudonimi senza un giustificato motivo. | Creazione o uso di un'identità elettronica falsa (R2) |
| TR2 | Un aggressore può rilasciare identità elettroniche inventate che non esistono. | Creazione o uso di un'identità elettronica falsa (R2) |
| TR3 | Un aggressore può iniziare a rilasciare dati di identificazione personale (*personal identification data* — PID) non autorizzati. | Creazione o uso di un'identità elettronica falsa (R2) |
| TR4 | Un aggressore può fare sì che un amministratore inserisca un fornitore di PID errato nell'elenco di fiducia di fornitori di PID. | Creazione o uso di un'identità elettronica falsa (R2) |
| TR5 | Un aggressore può aggirare il servizio di controllo dell'identità a distanza. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR6 | Un aggressore può aggirare il servizio di controllo dell'identità fisico. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR7 | Un aggressore può aggirare i servizi di controllo dell'identità correlati all'uso di un certificato (qualificato) remoto. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR8 | Un aggressore può ottenere accesso a un portafoglio che non è vincolato a una persona. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR9 | Un aggressore può eludere i controlli tecnici e procedurali per creare PID errati. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR10 | Un aggressore può attivare un portafoglio nuovo su un dispositivo crittografico sicuro per il portafoglio (*wallet secure cryptographic device* – WSCD) non valido. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2) |
| TR11 | Un aggressore può aggirare il servizio di controllo dell'identità correlato all'uso di un mezzo di identificazione elettronica esistente. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |
| TR12 | Un aggressore può eludere la verifica da parte del fornitore di PID del fatto che il portafoglio sia controllato dall'utente e determinare il rilascio di PID nel contesto di un portafoglio compromesso soggetto a controllo da parte dell'aggressore. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR13 | Un aggressore può ottenere PID validi nel contesto di un'unità di portafoglio non valida. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |
| TR14 | Un fornitore di PID può rilasciare identità inventate in casi in cui l'identità è correlata a una persona esistente. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |
| TR15 | Un aggressore può collegare PID al portafoglio errato perché il fornitore di PID non è in grado di collegare i PID al portafoglio corretto. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |
| TR16 | Un aggressore può far sì che l'utente approvi l'attivazione di una nuova unità/istanza di portafoglio sotto il controllo dell'aggressore, che acquisisce il successivo controllo anche degli attestati. | Creazione o uso di un'identità elettronica esistente (R1)/creazione o uso di un'identità elettronica falsa (R2)/furto di identità (R4)/transazione non autorizzata (R9) |
| TR17 | Un aggressore può rilasciare PID di un altro Stato per accedere ai dati/alle risorse digitali di cittadini interessati. | Creazione o uso di un'identità elettronica esistente (R1)/furto di identità (R4)/ transazione non autorizzata (R9) |
| TR18 | Un aggressore può eludere i controlli tecnici e procedurali per creare attestati elettronici di attributi (qualificati) [(Q)EAA — *(qualified) electronic attestation of attributes*] falsi. | Creazione o uso di attributi falsi (R3) |
| TR19 | Un aggressore può presentare (Q)EAA che non sono stati validamente rilasciati a favore dello stesso. | Creazione o uso di attributi falsi (R3) |
| TR20 | Un aggressore può attaccare il meccanismo di associazione crittografica del portafoglio tra i PID e un (Q)EAA che non dovrebbe essere rilasciato a favore dello stesso. | Creazione o uso di attributi falsi (R3) |
| TR21 | Un aggressore può utilizzare un (Q)EAA in un portafoglio, sebbene la controparte fisica di tale (Q)EAA sia scaduta o non valida. | Creazione o uso di attributi falsi (R3) |
| TR22 | Un aggressore può eludere la verifica da parte del fornitore di (Q)EAA del fatto che il portafoglio sia controllato dall'utente e determinare il rilascio di (Q)EAA nel contesto di un portafoglio compromesso soggetto a controllo da parte dell'aggressore. | Creazione o uso di attributi falsi (R3) |
| TR23 | Un aggressore può falsificare gli attestati elettronici di attributi. | Creazione o uso di attributi falsi (R3) |
| TR24 | Un aggressore può inserire attestati elettronici di attributi falsificati in un portafoglio. | Creazione o uso di attributi falsi (R3) |
| TR25 | Il portafoglio può presentare attributi a una parte facente affidamento sulla certificazione senza l'approvazione di un utente. | Divulgazione di dati (R6) |
| TR26 | PID, (Q)EAA o pseudonimi possono essere presentati a una parte facente affidamento sulla certificazione sbagliata. | Divulgazione di dati (R6) |
| TR27 | Un aggressore può avviare un rinnovo malevolo dell'attestato elettronico di attributi. | Divulgazione di dati (R6) |
| TR28 | Un aggressore può indurre un utente ad approvare erroneamente una richiesta di attestati elettronici di attributi (*phishing* o altro). | Divulgazione di dati (R6) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR29 | Un aggressore può determinare una fuga di attributi dal portafoglio e identificare l'utente del portafoglio in una situazione in cui l'identificazione non è richiesta/consentita. | Divulgazione di dati (R6) |
| TR30 | Un aggressore può eludere i controlli tecnici e procedurali per estrarre dati. | Divulgazione di dati (R6) |
| TR31 | Una richiesta può trapelare a favore di un aggressore. | Divulgazione di dati (R6) |
| TR32 | Un aggressore può venire a conoscenza della politica di divulgazione incorporata per gli attributi e presentare attributi contenuti nella richiesta corrente presentata da unità di portafoglio. | Divulgazione di dati (R6) |
| TR33 | Un aggressore può estrarre registrazioni o parti delle stesse. | Divulgazione di dati (R6) |
| TR34 | Un aggressore può sapere se un portafoglio è installato sul medesimo dispositivo che utilizza o su un altro e ottenere informazioni al riguardo. | Divulgazione di dati (R6) |
| TR35 | Un aggressore può ottenere un fattore di conoscenza utilizzato per l'autenticazione dell'utente nell'applicazione crittografica sicura per il portafoglio (*wallet secure cryptographic application* — WSCA). | Divulgazione di dati (R6) |
| TR36 | L'attestato elettronico di attributi relativo a una persona presentato nel contesto di più transazioni con una parte facente affidamento sulla certificazione, o tra diverse parti facenti affidamento sulla certificazione, consente involontariamente di associare più transazioni alla persona pertinente. | Divulgazione di dati (R6) |
| TR37 | Un elenco pubblico di revoca di attestati/di revoca di parti facenti affidamento sulla certificazione può contenere informazioni sull'uso dell'attestato da parte dell'utente (ad esempio ubicazione, indirizzo IP...). | Divulgazione di dati (R6) |
| TR38 | Non essendo in grado di dimostrare il consenso dell'utente per attributi condivisi, le parti facenti affidamento sulla certificazione possono compromettere l'integrità delle registrazioni. | Divulgazione di dati (R6) |
| TR39 | Un aggressore può tracciare illecitamente gli utenti del portafoglio utilizzando identificatori univoci/tracciabili. | Divulgazione di dati (R6)/sorveglianza (R14) |
| TR40 | Una parte facente affidamento sulla certificazione, costituita da più unità/entità, ciascuna delle quali ha una portata diversa in termini di ciò che è autorizzata a richiedere/trattare, può richiedere e trattare dati per i quali non dispone di motivi legittimi. | Divulgazione di dati (R6)/transazione non autorizzata (R9) |
| TR41 | Un aggressore può interferire con i controlli di integrità e autenticità effettuati dal portafoglio di PID affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR42 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano l'integrità e l'autenticità degli attributi richiesti affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR43 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano tutti gli attributi richiesti appartenenti al medesimo utente affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR44 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano la validità di PID e il loro rilascio da parte di un fornitore di PID affidabile affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR45 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano la validità di un QEAA e il suo rilascio da parte di un prestatore di servizi di fiducia qualificato che sia registrato per il rilascio di QEAA affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR46 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano se i PID sono stati revocati dal fornitore di PID affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR47 | Un aggressore può aggirare o interferire con l'esecuzione di controlli da parte del portafoglio che verificano se il (Q)EAA è stato revocato dal fornitore di (Q)EAA affinché forniscano sempre un esito positivo. | Manipolazione di dati (R7) |
| TR48 | Un aggressore può modificare il contenuto dei dati di backup e recupero che dovrebbero essere soggetti al controllo esclusivo da parte dell'utente. | Manipolazione di dati (R7)/perdita di dati (R8) |
| TR49 | Un aggressore può modificare la cronologia delle transazioni per una determinata istanza di portafoglio a partire dalle registrazioni delle attività. | Manipolazione di dati (R7)/perdita di dati (R8) |
| TR50 | Durante la connessione un aggressore può intercettare la comunicazione dal portafoglio alle parti facenti affidamento sulla certificazione. | Furto di dati (R5)/divulgazione di dati (R6) |
| TR51 | Un aggressore può convincere un utente a condividere dati personali (ad esempio PID, attestati elettronici di attributi, pseudonimi, firme elettroniche, registrazioni e altri dati) con l'aggressore o con un terzo senza che l'utente intendesse farlo. | Furto di dati (R5)/divulgazione di dati (R6) |
| TR52 | Un aggressore può leggere la cronologia delle transazioni per una determinata istanza di portafoglio a partire dalle registrazioni delle attività. | Furto di dati (R5)/divulgazione di dati (R6) |
| TR53 | Un aggressore può esportare o estrarre materiale relativo a chiavi crittografiche al di fuori del WSCD. | Furto di dati (R5)/divulgazione di dati (R6)/transazione non autorizzata (R9) |
| TR54 | Un aggressore può leggere il contenuto dei dati di backup e recupero che dovrebbero essere soggetti al controllo esclusivo da parte dell'utente. | Furto di dati (R5)/divulgazione di dati (R6) |
| TR55 | Un aggressore può aggirare il metodo di autenticazione dell'utente al fine di utilizzare uno pseudonimo generato da un'unità di portafoglio. | Furto di identità (R4) |
| TR56 | Un aggressore può proporre agli utenti un'applicazione che simuli un portafoglio legittimo specifico. | Furto di identità (R4) |
| TR57 | Un aggressore può esportare dati del portafoglio, compresi PID, (Q)EAA o registrazioni. | Furto di identità (R4) |
| TR58 | Un aggressore può esportare materiale di associazione crittografica. | Furto di identità (R4) |
| TR59 | Un aggressore può rilevare le identità attraverso le chiavi crittografiche del portafoglio. | Furto di identità (R4) |
| TR60 | Un aggressore può duplicare l'unità di portafoglio personale di un altro utente sul proprio dispositivo personale e utilizzarla. | Furto di identità (R4)/creazione o uso di un'identità elettronica esistente (R1) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR61 | Le autorità di un altro Stato possono chiedere all'utente di mostrare e/o condividere tutti i dati del portafoglio in una situazione di prossimità, ad esempio quando attraversa la frontiera di tale Stato. | Furto di identità (R4)/sorveglianza (R14) |
| TR62 | Gli utenti non possono trasferire le loro registrazioni delle transazioni dopo un guasto di un dispositivo dell'utente, con conseguente perdita di tracciabilità delle transazioni precedenti sul portafoglio nuovo. | Ripudio (R11) |
| TR63 | Gli utenti non possono recuperare le loro registrazioni delle transazioni dopo un guasto di un dispositivo dell'utente, con conseguente perdita di tracciabilità sul portafoglio nuovo. | Ripudio (R11) |
| TR64 | Le parti facenti affidamento sulla certificazione possono incontrare difficoltà nel dimostrare il consenso per le firme elettroniche a distanza. | Ripudio (R11) |
| TR65 | Un aggressore può subissare di richieste la connessione o le connessioni durante la connessione alle parti facenti affidamento sulla certificazione. | Perturbazione del servizio (R13) |
| TR66 | Un aggressore può subissare un servizio fornitore di stato di connessioni a parti facenti affidamento sulla certificazione. | Perturbazione del servizio (R13) |
| TR67 | Un aggressore può far apparire la presentazione dell'attributo come contestata/negata, nonostante la presentazione dell'attributo attesti la propria validità. | Perturbazione del servizio (R13) |
| TR68 | Un aggressore può revocare PID senza giustificato motivo. | Perturbazione del servizio (R13) |
| TR69 | Un aggressore può revocare PID senza il consenso dell'utente. | Perturbazione del servizio (R13) |
| TR70 | Un aggressore può revocare un (Q)EAA senza giustificato motivo. | Perturbazione del servizio (R13) |
| TR71 | Un aggressore può revocare un (Q)EAA senza il consenso dell'utente. | Perturbazione del servizio (R13) |
| TR72 | Un aggressore può far scattare richieste di identificazione multiple senza che siano riconosciute come richieste orfane intenzionali. | Perturbazione del servizio (R13) |
| TR73 | Un aggressore può inviare più richieste senza alcuna transazione di seguito. | Perturbazione del servizio (R13) |
| TR74 | Un aggressore può consentire a una parte facente affidamento sulla certificazione di richiedere l'identificazione senza un'identificazione (risposta) corrispondente e il pieno controllo. | Perturbazione del servizio (R13) |
| TR75 | Un aggressore può inviare una risposta a una richiesta dopo il *timeout* per la stessa o situazioni analoghe che comportano una perturbazione del servizio. | Perturbazione del servizio (R13) |
| TR76 | Una parte facente affidamento sulla certificazione può inviare più richieste non valide. | Perturbazione del servizio (R13) |
| TR77 | Un aggressore può inviare più richieste non valide a un fornitore del portafoglio. | Perturbazione del servizio (R13) |
| TR78 | Un aggressore può far sì che uno Stato membro non sia in grado di revocare l'inserimento di un fornitore di PID non affidabile nell'elenco di fiducia di fornitori di PID affidabili. | Perturbazione del servizio (R13) |
| TR79 | Un aggressore può impedire la sospensione o la revoca di un portafoglio. | Perturbazione del servizio (R13) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR80 | Un aggressore può bloccare le transazioni effettuate dalle parti facenti affidamento sulla certificazione, dagli utenti e/o dal fornitore di PID. | Perturbazione del servizio (R13) |
| TR81 | Un aggressore può disattivare o rendere indisponibile un WSCD. | Perturbazione del servizio (R13) |
| TR82 | Un aggressore può impedire al fornitore di PID di revocare o sospendere i PID. | Perturbazione del servizio (R13)/ transazione non autorizzata (R9) |
| TR83 | Una parte facente affidamento sulla certificazione può desumere i dati di identità dell'utente oltre i dati condivisi con quest'ultimo. | Sorveglianza (R14) |
| TR84 | Un gruppo di parti facenti affidamento sulla certificazione o di fornitori di PID che mettono in atto pratiche collusive può desumere i dati di identità dell'utente oltre i dati a loro noti. | Sorveglianza (R14) |
| TR85 | Un aggressore può tracciare e rintracciare un utente utilizzando i suoi dati di identificazione personale se non è richiesta l'identificazione dell'utente. | Sorveglianza (R14) |
| TR86 | Un aggressore può combinare una presentazione «falsificata» di combinazioni di (Q)EAA. | Manipolazione di transazioni (R10) |
| TR87 | Un aggressore può attivare/rilevare il portafoglio a distanza (ad esempio nel caso di un'applicazione bancaria che incorpora una richiesta di autenticazione o di attestazione) senza il consenso esplicito o il controllo esclusivo dell'utente, in situazioni in cui l'utente non ne è a conoscenza (ad esempio durante il sonno) o non può vedere la parte facente affidamento sulla certificazione. | Manipolazione di transazioni (R10) |
| TR88 | Gli aggressori possono apportare modifiche ai metadati di una richiesta (nome del servizio, usi ecc.). | Manipolazione di transazioni (R10) |
| TR89 | Gli aggressori possono apportare modifiche alle informazioni di risposta [stato di servizio, numero generato casualmente (*nonce*) ecc.]. | Manipolazione di transazioni (R10) |
| TR90 | Gli aggressori possono apportare modifiche alle informazioni di attributo della richiesta (richieste eccessive ecc.). | Manipolazione di transazioni (R10) |
| TR91 | Una parte facente affidamento sulla certificazione può riprodurre elementi di una sessione precedente in un'altra sessione. | Manipolazione di transazioni (R10) |
| TR92 | Un aggressore può sostituire o modificare i PID durante il loro trasferimento dal fornitore di PID all'unità di portafoglio. | Manipolazione di transazioni (R10) |
| TR93 | Un aggressore può sostituire o modificare i PID durante il loro trasferimento dall'unità di portafoglio alla parte facente affidamento sulla certificazione online. | Manipolazione di transazioni (R10) |
| TR94 | Un aggressore può sostituire o modificare i PID durante il loro trasferimento dall'unità di portafoglio alla parte facente affidamento sulla certificazione offline. | Manipolazione di transazioni (R10) |
| TR95 | Un aggressore può rilasciare PID senza il consenso dell'utente. | Transazione non autorizzata (R9) |
| TR96 | Un aggressore può utilizzare politiche di divulgazione incorporate revocate o non valide, eventualmente senza che le parti facenti affidamento sulla certificazione ne siano a conoscenza. | Transazione non autorizzata (R9) |
| TR97 | Un aggressore può indurre ingannevolmente il portafoglio a verificare firme elettroniche errate. | Transazione non autorizzata (R9) |
| TR98 | Un aggressore può utilizzare il portafoglio al di fuori del controllo dell'utente. | Transazione non autorizzata (R9) |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR99 | Un aggressore può convincere un utente ad autenticare e approvare transazioni con un aggressore o un terzo non autorizzato. | Transazione non autorizzata (R9) |
| TR100 | Un aggressore può far firmare elettronicamente un utente senza presentare il contenuto all'utente o dopo aver presentato contenuti errati. | Transazione non autorizzata (R9) |
| TR101 | Un aggressore può aggirare il controllo di accesso dell'account dell'utente presso il fornitore del portafoglio. | Transazione non autorizzata (R9) |
| TR102 | Un aggressore può assumere l'identità di parti facenti affidamento sulla certificazione durante la connessione con dette parti. | Transazione non autorizzata (R9)/ divulgazione di dati (R6) |
| TR103 | L'utente dietro la parte facente affidamento sulla certificazione nel contesto della connessione del browser può essere diverso dall'utente dietro la parte facente affidamento sulla certificazione nel contesto della connessione del portafoglio. | Transazione non autorizzata (R9)/ divulgazione di dati (R6)/furto di identità (R4) |
| TR104 | Un aggressore può convincere l'utente a revocare il portafoglio dell'utente senza motivo. | Transazione non autorizzata (R9)/ perturbazione del servizio (R13) |
| TR105 | Un aggressore può compiere attacchi MITM. | Transazione non autorizzata (R9)/ divulgazione di dati (R6)/sorveglianza (R14) |
| TR106 | Un aggressore può presentare attributi non validi o revocati da un portafoglio che non si connette regolarmente alla rete. | Effetti su vari rischi |
| TR107 | Un aggressore può rubare informazioni da un utente mediante lo *spoofing* ai danni di un portafoglio. | Effetti su vari rischi |
| TR108 | Un aggressore può assumere l'identità dell'utente riproducendo/imitando una richiesta di dati (ad esempio, autenticazione), che sembrerebbe valida. | Effetti su vari rischi |
| TR109 | Un aggressore può riprodurre una politica di divulgazione incorporata nei confronti di un utente al fine di imitare una richiesta approvata. | Effetti su vari rischi |
| TR110 | Un aggressore può sfruttare la mancanza di informazioni degli utenti del portafoglio, o indebiti ritardi, dopo una violazione o una compromissione della sicurezza. | Effetti su vari rischi |
| TR111 | Un aggressore può modificare un'istanza di portafoglio legittima precedentemente installata al fine di aggiungere componenti malevole. | Effetti su vari rischi |
| TR112 | Un aggressore può modificare un'istanza di portafoglio legittima e proporla agli utenti come legittima. | Effetti su vari rischi |
| TR113 | Un aggressore può sconfiggere il meccanismo di autenticazione dell'utente stesso per aggirare l'autenticazione dell'utente del portafoglio. | Effetti su vari rischi |
| TR114 | Un aggressore può introdurre un codice malevolo o *backdoor* nel codice del portafoglio durante il suo utilizzo sul dispositivo dell'utente. | Effetti su vari rischi |
| TR115 | Un aggressore può introdurre un codice malevolo o *backdoor* nel codice del portafoglio durante il suo sviluppo. | Effetti su vari rischi |
| TR116 | Un aggressore può manomettere la generazione di numeri casuali per ridurne l'entropia in misura sufficiente da consentire attacchi. | Effetti su vari rischi |

| ID<br>*Identificativo* | Descrizione della minaccia<br>*Descrizione della minaccia individuata (*)* | Titolo del rischio<br>*Rischi correlati* |
|---|---|---|
| TR117 | Un aggressore può manomettere i dispositivi dell'utente nella catena di approvvigionamento al fine di includere codici o configurazioni che non soddisfano le condizioni di utilizzo del portafoglio. | Effetti su vari rischi |
| TR118 | Un aggressore può attivare un'unità di portafoglio utilizzando un WSCD oggetto di *spoofing* controllato da aggressori. | Effetti su vari rischi |
| TR119 | Un aggressore può leggere le informazioni inviate alla WSCA e/o al WSCD. | Effetti su vari rischi |
| TR120 | Un aggressore può inviare informazioni arbitrarie al WSCA. | Effetti su vari rischi |
| TR121 | Un aggressore può rubare informazioni intercettando gli scambi tra la WSCA e il WSCD. | Effetti su vari rischi |
| TR122 | Un aggressore può inviare informazioni arbitrarie al WSCD. | Effetti su vari rischi |
| TR123 | Un aggressore può inviare informazioni al WSCD, aggirando la WSCA. | Effetti su vari rischi |
| TR124 | Un aggressore può ricorrere al *phishing* per far sì che gli utenti accedano a un'applicazione web falsa di gestione del portafoglio e di PID. | Effetti su vari rischi |
| TR125 | Un aggressore può sostituire le chiavi del portafoglio con altre chiavi al fine di creare messaggi da utilizzare in un altro attacco. | Effetti su vari rischi |
| TR126 | Un aggressore può modificare o distruggere le chiavi di un portafoglio, rendendo inutilizzabili alcune funzioni del portafoglio stesso. | Effetti su vari rischi |
| TR127 | Un aggressore può controllare un malware per accedere ai dati conservati nel portafoglio. | Effetti su vari rischi |
| TR128 | Un aggressore può accedere agli elementi di prova generati nel portafoglio. | Effetti su vari rischi |
| TR129 | I fornitori di portafogli possono accedere agli oggetti presenti nel portafoglio. | Effetti su vari rischi |
| TR130 | I fornitori di portafogli possono accedere agli elementi di prova generati nel portafoglio. | Effetti su vari rischi |
| TR131 | Un aggressore può rubare un dispositivo di portafoglio sbloccato. | Effetti su vari rischi |
| TR132 | Un aggressore può manipolare il sistema per impedire la registrazione di determinati eventi. | Effetti su vari rischi |
| TR133 | Un aggressore può intercettare la comunicazione tra l'istanza di portafoglio e la WSCA o riprodurre/imitare un utente (ad esempio piratando un meccanismo di autenticazione). | Effetti su vari rischi |

*ALLEGATO II*

**CRITERI PER VALUTARE L'ACCETTABILITÀ DELLE INFORMAZIONI SULLA GARANZIA**

| Nome | Oggetto | Aspetti da considerare |
|---|---|---|
| Sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) | Prodotti delle tecnologie dell'informazione e della comunicazione (TIC) | Informazioni sull'emittente: nessuno (organismi di certificazione accreditati).<br>Informazioni sull'ambito di applicazione:<br>— verifica del profilo di protezione e dell'obiettivo di sicurezza;<br>— verifica del livello di garanzia della valutazione e dei potenziamenti.<br>Informazioni sulla garanzia:<br>— verifica delle restrizioni nella documentazione dell'utente;<br>— per la composizione, può richiedere l'accesso alla relazione tecnica di valutazione. |
| Sistema europeo di certificazione della sicurezza dei servizi cloud (EUCS) (se disponibile) | Servizi cloud | Informazioni sull'emittente: nessuno (organismi di certificazione accreditati).<br>Informazioni sull'ambito di applicazione:<br>— verifica della descrizione del servizio cloud;<br>— verifica del livello di valutazione e dei profili di estensione.<br>Informazioni sulla garanzia:<br>— verifica delle informazioni sulla trasparenza e, se necessario, delle informazioni sulla composizione. |
| Sistemi basati sui criteri comuni gestiti nell'UE, compresi i sistemi del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (*Senior Officials Group — Information Systems Security* — SOG-IS) | Prodotti TIC | Informazioni sull'emittente: nessuno (Stati membri).<br>Informazioni sull'ambito di applicazione:<br>— verifica del profilo di protezione e dell'obiettivo di sicurezza;<br>— verifica del livello di garanzia della valutazione e dei potenziamenti.<br>Informazioni sulla garanzia:<br>— verifica delle restrizioni nella documentazione dell'utente;<br>— per la composizione, può richiedere l'accesso alla relazione tecnica di valutazione. |
| EN 17640:2018 (FITCEM, nonché CSPN, BSZ, LINCE, BSZA) | Prodotti TIC | Informazioni sull'emittente:<br>— verifica del sistema e dei requisiti per gli organismi di certificazione.<br>Informazioni sull'ambito di applicazione:<br>— verifica della descrizione del prodotto;<br>— verifica delle dichiarazioni in materia di sicurezza;<br>— verifica del livello di garanzia.<br>Informazioni sulla garanzia:<br>— verifica delle attività svolte e delle risultanze riportate nella relazione. |
| Sistemi di certificazione di dispositivi per la creazione di firme qualificate conformemente all'articolo 30 del regolamento (UE) n. 910/2014 | Dispositivi per la creazione di firme qualificate | Informazioni sull'emittente:<br>— verifica del sistema e dei requisiti per gli organismi di certificazione.<br>Informazioni sull'ambito di applicazione:<br>— verifica della descrizione del prodotto;<br>— verifica delle dichiarazioni in materia di sicurezza;<br>— verifica del livello di garanzia.<br>Informazioni sulla garanzia:<br>— verifica delle attività svolte. |

| Nome | Oggetto | Aspetti da considerare |
|---|---|---|
| EN ISO/IEC 27001:2022 | SGSI | Informazioni sull'emittente: nessuno (organismi di certificazione accreditati).<br>Informazioni sull'ambito di applicazione:<br>— verifica della descrizione del sistema di gestione;<br>— verifica della dichiarazione di applicabilità.<br>Informazioni sulla garanzia:<br>— verifica delle attività svolte. |
| SOC2 | Organizzazioni | Informazioni sull'emittente:<br>— verifica dello status di contabile pubblico;<br>Informazioni sull'ambito di applicazione:<br>— verifica della dichiarazione di gestione e della descrizione dei controlli;<br>— verifica della dichiarazione di applicabilità.<br>Informazioni sulla garanzia:<br>— verifica delle risultanze contenute nella relazione;<br>— verifica delle lettere ponte (*bridge letters*), se necessario. |
| MDSCert (certificazione della sicurezza dei dispositivi mobili) (GSMA) (se disponibile) | Dispositivi mobili | Informazioni sull'emittente:<br>— verifica dei requisiti per gli organismi di certificazione.<br>Informazioni sull'ambito di applicazione:<br>— verifica del livello di garanzia della sicurezza;<br>— verifica dei requisiti del sistema;<br>Informazioni sulla garanzia:<br>— verifica delle attività e delle risultanze riportate nella relazione. |
| Altri sistemi | Qualsiasi componente | Informazioni sul sistema:<br>— verifica della rilevanza e delle disposizioni del sistema.<br>Informazioni sull'emittente:<br>— verifica dei requisiti per gli organismi di certificazione.<br>Informazioni sull'ambito di applicazione:<br>— verifica dei requisiti del sistema;<br>— verifica dell'obiettivo in materia di sicurezza o di un documento analogo che descriva i requisiti funzionali di sicurezza e di garanzia;<br>— verifica della descrizione del prodotto e dei requisiti funzionali di sicurezza selezionati.<br>Informazioni sulla garanzia:<br>— verifica delle attività e delle risultanze riportate nella relazione. |

*ALLEGATO III*

**REQUISITI FUNZIONALI PER LE SOLUZIONI DI PORTAFOGLIO**

A norma dell'articolo 5 *bis*, paragrafi 4, 5, 8 e 14, del regolamento (UE) n. 910/2014, tra i criteri funzionali che una soluzione di portafoglio certificata e il regime di identificazione elettronica nel contesto del quale detta soluzione è fornita devono soddisfare figurano i requisiti funzionali per le operazioni elencate negli atti seguenti:

1) Regolamento di esecuzione (UE) 2024/2979 della Commissione ([1]) 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;

2) Regolamento di esecuzione (UE) 2024/2982 della Commissione ([2]) 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;

3) Regolamento di esecuzione (UE) 2024/2977 della Commissione ([3]) 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.

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

([2]) 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).

([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).

*ALLEGATO IV*

**METODI E PROCEDURE PER LE ATTIVITÀ DI VALUTAZIONE**

## 1. Audit dell'attuazione di una soluzione di portafoglio

Un'attività di valutazione della conformità deve consistere nella selezione di attività di valutazione specifiche.

I sistemi nazionali di certificazione devono specificare un'attività di valutazione volta ad esaminare le informazioni fornite, che contempli almeno quanto segue:

a) un'analisi delle informazioni fornite a conferma del fatto che sono adatte per una delle architetture specificate nei sistemi nazionali di certificazione;

b) un'analisi della copertura dei rischi e delle minacce di cibersicurezza individuati nel registro dei rischi di cui all'allegato I mediante i controlli di sicurezza descritti.

L'analisi di cui alle lettere da a) a b) si deve basare sulla logica e sulla giustificazione indicate dal fornitore del portafoglio.

## 2. Attività di valutazione relative al dispositivo crittografico sicuro per il portafoglio

1) Le operazioni critiche, compresi i calcoli crittografici, non devono essere pienamente attuate nel dispositivo crittografico sicuro per il portafoglio (WSCD). Tuttavia, la parte attuata nel WSCD, quando opera nell'ambito della soluzione di portafoglio, deve garantire la protezione delle operazioni critiche che esegue nei confronti degli attacchi da parte di aggressori con un potenziale di attacco elevato conformemente al regolamento di esecuzione (UE) 2015/1502 della Commissione ([1]).

2) Il WSCD o parte di esso può rientrare nell'oggetto della certificazione quando è fornito dal titolare del certificato o dal richiedente oppure al di fuori del suo ambito di applicazione quando è integrato in un dispositivo fornito dall'utente finale. Inoltre, i sistemi nazionali di certificazione devono specificare le attività di valutazione per verificare l'idoneità del WSCD nei due casi seguenti:

   a) se l'applicazione crittografica sicura per il portafoglio (WSCA) dipende dal WSCD specifico (ossia se deve essere valutata come prodotto composito sulla base del WSCD), la valutazione della WSCA deve richiedere l'accesso a informazioni supplementari relative alla certificazione del WSCD, compresa, in particolare, la relazione tecnica di valutazione;

   b) se un'architettura presa in considerazione nel sistema utilizza diversi WSCD o se alcune delle operazioni su risorse critiche sono effettuate al di fuori del WSCD, i sistemi nazionali di certificazione devono prevedere attività di valutazione volte a garantire che la soluzione complessiva offra il livello di sicurezza previsto.

3) Come presupposto per la certificazione ai sensi dei sistemi nazionali di certificazione, il WSCD deve essere valutato rispetto ai requisiti per il livello di garanzia elevato di cui al regolamento di esecuzione (UE) 2015/1502.

   Se sono soddisfatte le condizioni di cui all'articolo 3, paragrafo 3, lettera b), la valutazione del WSCD o di parte di esso comprende una valutazione delle vulnerabilità di cui alla norma EN ISO/IEC 15408-3:2022 a livello AVA_VAN.5, come stabilito nell'allegato I del regolamento di esecuzione (UE) 2024/482 della Commissione ([2]), fatto salvo il caso in cui sia debitamente giustificato all'organismo di certificazione che le caratteristiche di sicurezza della WSCA consentono di utilizzare un livello di valutazione inferiore pur mantenendo nel contempo il medesimo livello di garanzia complessivo elevato di cui al regolamento di esecuzione (UE) 2015/1502.

([1]) 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).

([2]) Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Inoltre, nella documentazione relativa a ciascuna specifica architettura, i sistemi nazionali di certificazione devono formulare ipotesi per tale valutazione del WSCD nell'ambito delle quali può essere fornita resistenza nei confronti di aggressori con un potenziale di attacco elevato in linea con il regolamento di esecuzione (UE) 2015/1502 e specificare le attività di valutazione volte a confermare tali ipotesi nonché, in seguito al rilascio del certificato, volte a confermare che tali ipotesi continuano a essere verificate. I sistemi nazionali devono inoltre imporre ai candidati alla certificazione di affinare tali ipotesi per la loro attuazione specifica e di descrivere le misure messe in atto per garantire che le ipotesi siano verificate durante l'intero ciclo di certificazione.

5) In tutti i casi, i sistemi nazionali di certificazione devono comprendere un'attività di valutazione volta a verificare che le informazioni sulla garanzia disponibili per il WSCD siano adeguate ai fini della soluzione di portafoglio, attraverso un'analisi delle informazioni sulla garanzia, quali l'obiettivo di sicurezza per i certificati EUCC, che comprenda le attività seguenti:

   a) verificare che la portata della valutazione sia adeguata, il che per i certificati EUCC significa ad esempio verificare che l'obiettivo in materia di sicurezza dichiari la conformità a uno dei profili di protezione raccomandati nel contesto dell'EUCC;

   b) verificare che le ipotesi relative all'ambiente operativo siano compatibili con la soluzione di portafoglio, il che ad esempio per i certificati EUCC significa che tali ipotesi possono essere riscontrate nell'obiettivo in materia di sicurezza;

   c) verificare che le raccomandazioni contenute negli orientamenti o nella documentazione per l'utente siano compatibili con le condizioni alle quali il WSCD deve essere utilizzato nella soluzione di portafoglio;

   d) verificare che le ipotesi formulate nel contesto del sistema nazionale di certificazione in merito a WSCD siano verificate e contemplate nelle informazioni sulla garanzia.

6) Nei casi in cui alcune delle verifiche non siano pienamente conclusive, i sistemi nazionali di certificazione devono imporre agli organismi di certificazione di specificare i requisiti di compensazione per la WSCA sulla base del WSCD, da includere nella valutazione della WSCA. Laddove ciò non sia possibile, i sistemi nazionali di certificazione devono considerare il WSCD inadatto, il che significa che non deve essere rilasciato un certificato di conformità per la soluzione di portafoglio.

3. **Attività di valutazione relative all'applicazione crittografica sicura per il portafoglio (WSCA)**

1) I sistemi nazionali di certificazione devono esigere che una WSCA, essendo parte di una soluzione di portafoglio, sia valutata rispetto ai requisiti del livello di garanzia come minimo elevato di cui al regolamento di esecuzione (UE) 2015/1502.

2) Tale valutazione deve comprendere una valutazione delle vulnerabilità, come stabilito nella norma EN ISO/IEC 15408-3:2022 a livello di AVA_VAN.5, come stabilito nell'allegato I del regolamento di esecuzione (UE) 2024/482, fatto salvo il caso in cui sia debitamente giustificato all'organismo di certificazione che le caratteristiche di sicurezza della WSCA consentono di utilizzare un livello di valutazione inferiore pur mantenendo nel contempo il medesimo livello di garanzia complessivo elevato di cui al regolamento di esecuzione (UE) 2015/1502.

3) Se la WSCA non è fornita dal fornitore del portafoglio, i sistemi nazionali di certificazione devono formulare ipotesi per tale valutazione della WSCA nell'ambito delle quali può essere fornita resistenza nei confronti di aggressori con un potenziale di attacco elevato in linea con il regolamento di esecuzione (UE) 2015/1502 e specificare le attività di valutazione volte a confermare tali ipotesi nonché, in seguito al rilascio del certificato, volte a confermare che tali ipotesi continuano a essere verificate. I sistemi nazionali devono inoltre imporre ai candidati alla certificazione di affinare tali ipotesi per la loro attuazione specifica e di descrivere le misure messe in atto per garantire che le ipotesi siano verificate durante l'intero ciclo di certificazione.

4) In tutti i casi, i sistemi nazionali di certificazione devono comprendere un'attività di valutazione volta a verificare che le informazioni sulla garanzia disponibili per la WSCA siano adeguate ai fini della soluzione di portafoglio, attraverso un'analisi delle informazioni sulla garanzia, quali l'obiettivo di sicurezza per i certificati EUCC, che comprenda le attività seguenti:

   a) verificare che la portata della valutazione sia adeguata, il che per i certificati EUCC significa ad esempio verificare che l'obiettivo in materia di sicurezza dichiari la conformità a uno dei profili di protezione raccomandati nel contesto dell'EUCC;

   b) verificare che le ipotesi relative all'ambiente operativo siano compatibili con la soluzione di portafoglio, il che ad esempio per i certificati EUCC significa che tali ipotesi possono essere riscontrate nell'obiettivo in materia di sicurezza;

c) verificare che le raccomandazioni contenute negli orientamenti o nella documentazione per l'utente siano compatibili con le condizioni alle quali la WSCA deve essere utilizzata nella soluzione di portafoglio;

d) verificare che le ipotesi formulate nel contesto del sistema nazionale di certificazione in merito alle WSCA siano verificate e contemplate nelle informazioni sulla garanzia.

5) I sistemi nazionali di certificazione devono esigere che la valutazione della WSCA copra tutti i controlli di sicurezza attuati da tale applicazione.

4. **Attività di valutazione relative al dispositivo dell'utente finale**

Poiché il registro dei rischi, di cui all'allegato I del presente regolamento, individua i rischi direttamente correlati alla sicurezza del dispositivo dell'utente finale, i sistemi nazionali di certificazione devono specificare i requisiti di sicurezza per i dispositivi degli utenti finali. Tuttavia, dato che tali dispositivi sono forniti dall'utente finale e non dal fornitore del portafoglio, i suddetti requisiti devono essere coperti da ipotesi.

Per ciascuna ipotesi, la soluzione di portafoglio deve prevedere un meccanismo atto a verificare, per ciascuna unità di portafoglio, che il dispositivo dell'utente finale sottostante soddisfi l'ipotesi in questione. Tali meccanismi sono considerati controlli di sicurezza e sono oggetto di attività di valutazione volte a dimostrarne l'idoneità e l'efficacia corrispondente al livello di garanzia adeguato.

Di seguito sono riportati due esempi:

a) un dispositivo dell'utente finale può comprendere un WSCD certificato, che deve essere dimostrato. Di norma, ciò avviene utilizzando un meccanismo crittografico per verificare la presenza nel WSCD certificato di un segreto crittografico disponibile soltanto nel WSCD certificato. In tal caso, il segreto crittografico dovrebbe essere considerato una risorsa critica ed essere coperto dalla certificazione del WSCD e/o della WSCA;

b) un requisito tipico per i dispositivi degli utenti finali prevede che i dispositivi debbano ricevere aggiornamenti di sicurezza. Dato che tale requisito è correlato all'istanza di portafoglio, il meccanismo utilizzato per verificare la disponibilità di aggiornamenti di sicurezza deve essere coperto soltanto da attività di valutazione a un livello di garanzia adatto all'istanza di portafoglio, in particolare dato che è probabile che sia integrato nell'istanza di portafoglio.

5. **Attività di valutazione relative all'istanza di portafoglio**

1) Nella valutazione dell'istanza di portafoglio devono essere prese in considerazione le due sfide principali seguenti:

a) è probabile che l'istanza di portafoglio esista in una serie di varianti della stessa applicazione di base, con ciascuna variante specializzata per una categoria specifica di dispositivi degli utenti finali;

b) è probabile che le diverse varianti dell'istanza di portafoglio necessiteranno di aggiornamenti frequenti per seguire lo sviluppo della piattaforma di sicurezza sottostante, ad esempio quando vengono individuate vulnerabilità che richiedono modifiche delle applicazioni.

2) Nella valutazione dell'istanza di portafoglio si deve tenere conto di tali sfide specifiche. Una delle conseguenze immediate consiste nel fatto che il quadro dei criteri comuni potrebbe non essere adeguato in tutti i casi. Pertanto, ove necessario, occorre prendere in considerazione metodologie di valutazione alternative. I sistemi nazionali di certificazione devono prendere in considerazione l'utilizzo della metodologia di cui alla norma EN 17640:2018 in relazione a quanto segue:

a) nell'ambito del sistema stesso;

b) attraverso sistemi nazionali basati sulla metodologia;

c) attraverso sistemi nazionali basati su principi analoghi ma creati prima dello sviluppo della metodologia di cui alla norma EN 17640:2018.

3) Inoltre, dato che vi può essere un valore aggiunto limitato nello svolgere una valutazione dedicata integrale di ciascuna variante, i sistemi nazionali di certificazione devono prendere in considerazione l'opportunità di specificare criteri che consentono di svolgere un campionamento al fine di evitare la ripetizione di attività di valutazione identiche e di concentrarsi su attività specifiche di una determinata variante. I sistemi nazionali di certificazione impongono a tutti gli organismi di certificazione di giustificare il ricorso al campionamento.

4) I sistemi nazionali di certificazione devono prevedere aggiornamenti dell'istanza di portafoglio nel contesto del processo complessivo di gestione delle modifiche specificato per la soluzione di portafoglio. Essi devono altresì stabilire norme in merito alle procedure che il fornitore del portafoglio deve seguire per ogni aggiornamento (ad esempio analizzare l'impatto delle modifiche sui controlli di sicurezza) e in merito alle attività di valutazione che devono essere svolte dall'organismo di certificazione riguardanti gli aggiornamenti a determinate condizioni (ad esempio valutare l'efficacia operativa di un controllo di sicurezza modificato). Il processo di gestione delle modifiche è uno dei processi la cui efficacia operativa deve essere verificata annualmente a norma dell'articolo 18, paragrafo 3.

6. **Attività di valutazione relative ai servizi e ai processi utilizzati per la fornitura e il funzionamento della soluzione di portafoglio**

1) Per la valutazione dei servizi e dei processi che svolgono un ruolo nella fornitura e nell'esercizio della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, il gruppo di valutazione deve raccogliere elementi di prova svolgendo attività di valutazione, tra le quali possono figurare attività di audit, ispezione, verifica e convalida.

2) L'organismo di certificazione deve confermare che gli elementi di prova sono sufficienti e adeguati a fornire garanzie sufficienti del fatto che i servizi e i processi soddisfano i requisiti di certificazione, confermando quanto segue:

   a) l'esattezza delle informazioni presentate nella descrizione dei processi e dei servizi;

   b) l'idoneità della progettazione e dei controlli dei processi e dei servizi a soddisfare i criteri di valutazione;

   c) l'efficacia operativa dell'attuazione di tali controlli per un periodo specificato prima della valutazione.

3) L'esattezza della descrizione e l'efficacia operativa di un'attuazione dei controlli possono essere considerate obiettivi della verifica, ai sensi della norma ISO/IEC 17000:2020, delle corrispondenti dichiarazioni del fornitore del portafoglio (ossia la conferma dell'equità di eventi già verificatisi o di risultati già ottenuti), mentre l'idoneità della progettazione e dei controlli dei servizi e dei processi a soddisfare i criteri di valutazione può essere considerata un obiettivo di convalida, ai sensi della norma ISO/IEC 17000:2020, della corrispondente dichiarazione del fornitore del portafoglio (ossia la conferma della plausibilità di un uso futuro auspicato o di un risultato previsto).

4) Considerando che una soluzione di portafoglio non può operare prima di essere certificata, l'efficacia operativa non può essere confermata sulla base del funzionamento effettivo della soluzione. Di conseguenza ciò deve essere confermato utilizzando gli elementi di prova raccolti durante le prove o i progetti pilota.

5) Possono già esistere sistemi nazionali di certificazione per servizi e processi specifici, ad esempio per l'*onboarding* degli utenti. L'uso di tali sistemi è preso in considerazione dai sistemi nazionali di certificazione, se del caso.

7. **Attività di valutazione relative ai servizi TIC utilizzati per la fornitura e il funzionamento della soluzione di portafoglio**

1) Talune architetture di portafoglio possono basarsi su servizi TIC dedicati, compresi i servizi cloud per la fornitura e il funzionamento di una soluzione di portafoglio, e tali servizi possono ospitare dati sensibili così come operazioni sensibili. In tal caso, i sistemi nazionali di certificazione devono specificare i requisiti di sicurezza per tali servizi TIC.

2) Esistono già numerosi sistemi di certificazione per i servizi TIC, i servizi cloud e altre fonti di informazioni sulla garanzia, comprese quelle che figurano nell'allegato II. I sistemi nazionali di certificazione si basano, se disponibili e applicabili, su tali meccanismi esistenti, attraverso uno dei meccanismi seguenti:

   a) imporre l'uso di uno specifico sistema o di una selezione di sistemi, specificando le condizioni alle quali i servizi TIC o cloud devono essere valutati utilizzando tali sistemi;

   b) lasciare la scelta della valutazione al fornitore del portafoglio e utilizzare l'attività di analisi della dipendenza per esaminare l'adeguatezza delle informazioni sulla garanzia ottenute attraverso tali valutazioni.

3) In entrambi i casi, i sistemi nazionali di certificazione devono specificare le attività di valutazione supplementari necessarie per analizzare o integrare le informazioni ottenute attraverso tali sistemi.

*ALLEGATO V*

**ELENCO DELLE INFORMAZIONI PUBBLICAMENTE DISPONIBILI IN MERITO AI PORTAFOGLI**

1. Tra le informazioni che devono essere rese pubbliche a norma dell'articolo 8, paragrafo 5, devono figurare almeno le seguenti:

   a) qualsiasi limitazione all'uso della soluzione di portafoglio;

   b) orientamenti e raccomandazioni da parte del fornitore del portafoglio volti a fornire assistenza agli utenti finali nella configurazione, nell'installazione, nella diffusione, nel funzionamento e nella manutenzione in sicurezza dei portafogli;

   c) il periodo durante il quale agli utenti finali sarà offerta assistenza di sicurezza, in particolare per quanto concerne la disponibilità di aggiornamenti connessi alla cibersicurezza;

   d) informazioni di contatto del fabbricante o fornitore e metodi accettati per ricevere informazioni sulle vulnerabilità dagli utenti finali e dai ricercatori nel settore della sicurezza;

   e) un riferimento ad archivi online che elencano le vulnerabilità divulgate pubblicamente relative ai portafogli e a qualsiasi suggerimento pertinente in materia di cibersicurezza.

2. Le informazioni di cui al paragrafo 1 devono essere rese disponibili in modo chiaro, completo e facilmente accessibile, in uno spazio accessibile al pubblico, a chiunque intenda utilizzare una soluzione di portafoglio.

*ALLEGATO VI*

**METODOLOGIA PER VALUTARE L'ACCETTABILITÀ DELLE INFORMAZIONI SULLA GARANZIA**

1. **Valutazione della disponibilità della documentazione sulla garanzia**

I valutatori devono elencare la documentazione sulla garanzia disponibile per ciascun componente pertinente della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita. Successivamente i valutatori devono valutare la pertinenza complessiva di ciascun documento sulla garanzia ai fini del riesame della dipendenza.

Nel contesto dell'analisi sono presi in considerazione gli aspetti seguenti:

1) per quanto riguarda la documentazione stessa sulla garanzia:

   a) il tipo di documentazione sulla garanzia, con tutti i dettagli richiesti

      (esempi di tali documenti sono i certificati di conformità ai sensi della norma EN ISO/IEC 27001:2022 o di tipo 1 o di tipo 2 per i rapporti ISAE);

   b) il periodo coperto o il periodo di validità [tale periodo può essere integrato da una lettera ponte (un documento volto a coprire un periodo di tempo compreso tra la data di chiusura del periodo di riferimento del rapporto ISAE corrente e la pubblicazione di un nuovo rapporto ISAE) o da una dichiarazione analoga];
   c) il quadro applicabile (ad esempio la norma esistente);

   d) se la documentazione sulla garanzia comprende una mappatura dei requisiti del sistema;

2) per quanto riguarda la competenza professionale e l'imparzialità dell'emittente della relazione in materia di garanzia:

   a) il nome dell'organismo di certificazione e, se disponibile, il nome del valutatore capo;

   b) gli elementi di prova della competenza dell'organismo di certificazione e del valutatore (ad esempio accreditamento, certificazione personale ecc.);

   c) gli elementi di prova dell'imparzialità dell'organismo di certificazione e del valutatore (ad esempio accreditamento ecc.).

2. **Valutazione della garanzia relativa ai singoli requisiti**

I valutatori devono verificare che la documentazione sulla garanzia disponibile per la soluzione di portafoglio e il regime di identificazione elettronica nel contesto del quale detta soluzione è fornita sia adeguata al fine di stabilire se la soluzione di portafoglio soddisfa le aspettative relative ai requisiti individuali del sistema di certificazione.

La valutazione deve essere effettuata per ciascun componente pertinente della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita, formulando un'ipotesi sui controlli di sicurezza della soluzione di portafoglio.

Per ciascuna di tali ipotesi, il gruppo di valutazione stabilisce se la garanzia fornita nella documentazione sulla garanzia disponibile sia adeguata o meno.

La determinazione dell'adeguatezza della garanzia si basa sugli elementi seguenti:

1) le informazioni richieste sono disponibili, con il livello di garanzia atteso, nella documentazione sulla garanzia;

2) le informazioni disponibili nella documentazione sulla garanzia non riguardano l'intero ambito di applicazione del requisito, ma i controlli supplementari o compensativi (ossia i controlli interni che riducono il rischio di carenze di controllo esistenti o potenziali) attuati nella soluzione di portafoglio o nel regime di identificazione elettronica nel contesto del quale detta soluzione è fornita consentono ai valutatori di stabilire che le informazioni sono adeguate;

3) le informazioni disponibili nella documentazione sulla garanzia non offrono il livello di garanzia atteso, ma i controlli attuati per valutare e monitorare il fornitore del portafoglio consentono ai valutatori di stabilire che le informazioni sono adeguate;

4) se la documentazione sulla garanzia menziona non conformità in materia di progettazione o attuazione dei controlli utilizzati per soddisfare un'ipotesi, le azioni correttive proposte e attuate dal fornitore del portafoglio e riesaminate dai suoi valutatori devono essere adeguate a garantire che l'ipotesi sia effettivamente soddisfatta.

*ALLEGATO VII*

**CONTENUTO DEL CERTIFICATO DI CONFORMITÀ**

1. Un identificativo unico assegnato dall'organismo di certificazione che rilascia il certificato di conformità.

2. Informazioni relative alla soluzione di portafoglio certificata e ai regimi di identificazione elettronica nel contesto dei quali detta soluzione è fornita, così come in merito al titolare del certificato di conformità, comprese le informazioni seguenti:
   a) nome della soluzione di portafoglio;
   b) nome dei regimi di identificazione elettronica nel contesto dei quali la soluzione di portafoglio è fornita;
   c) versione della soluzione di portafoglio che è stata valutata;
   d) nome, indirizzo e informazioni di contatto del titolare del certificato di conformità;
   e) collegamento al sito web del titolare del certificato di conformità contenente le informazioni che devono essere rese pubbliche

3. Informazioni relative alla valutazione e certificazione della soluzione di portafoglio e dei regimi di identificazione elettronica nel contesto dei quali detta soluzione è fornita, comprese le informazioni seguenti:
   a) nome, indirizzo e informazioni di contatto dell'organismo di certificazione che ha rilasciato il certificato di conformità;
   b) se diverso dall'organismo di certificazione, il nome dell'organismo di valutazione della conformità che ha effettuato la valutazione, unitamente alle informazioni concernenti il suo accreditamento;
   c) nome del titolare del sistema;
   d) riferimenti al regolamento (UE) n. 910/2014 e al presente regolamento;
   e) un riferimento alla relazione di certificazione associata al certificato di conformità;
   f) un riferimento alla relazione di valutazione della certificazione associata al certificato di conformità;
   g) un riferimento alle norme utilizzate ai fini della valutazione, comprese le loro versioni;
   h) la data di rilascio del certificato di conformità;
   i) il periodo di validità del certificato di conformità.

*ALLEGATO VIII*

**CONTENUTO DELLA RELAZIONE PUBBLICA DI CERTIFICAZIONE E DELLA RELAZIONE DI VALUTAZIONE DELLA CERTIFICAZIONE**

1. La relazione pubblica di certificazione deve contenere quanto meno gli elementi seguenti:

   a) una sintesi;

   b) l'identificazione della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita;

   c) una descrizione della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale detta soluzione è fornita;

   d) le informazioni di sicurezza da rendere pubblicamente disponibili, come descritto nell'allegato V, o un rimando a tali informazioni;

   e) una sintesi del piano preliminare di audit e convalida;

   f) una sintesi del riesame e della decisione relativa alla certificazione.

2. La relazione di valutazione della certificazione deve contenere quanto meno:

   a) una descrizione della progettazione della soluzione di portafoglio, del sistema di identificazione e del processo di *onboarding*, unitamente alla valutazione dei rischi e al piano di convalida specifico;

   b) una descrizione del modo in cui la soluzione di portafoglio soddisfa i requisiti del livello di garanzia elevato e del modo in cui ciò è dimostrato dai risultati della valutazione della certificazione della soluzione di portafoglio effettuata conformemente al presente regolamento;

   c) una descrizione del risultato della valutazione della conformità della soluzione di portafoglio e del regime di identificazione elettronica nel contesto del quale le unità di portafoglio corrispondenti sono fornite, in particolare la conformità rispetto agli aspetti seguenti:

      — requisiti di cui all'articolo 5 *bis*, paragrafi 4, 5 e 8 del regolamento (UE) n. 910/2014;

      — il requisito relativo alla separazione logica di cui all'articolo 5 *bis*, paragrafo 14, del regolamento (UE) n. 910/2014;

      — se applicabili, le norme e le specifiche tecniche di cui articolo 5 *bis*, paragrafo 24, del regolamento (UE) n. 910/2014, descrivendo nel contempo il modo in cui tali requisiti sono correlati ai requisiti normativi corrispondenti specificati dai sistemi nazionali di certificazione;

   d) una sintesi del risultato delle prestazioni del piano di convalida, comprese tutte le non conformità individuate.

*ALLEGATO IX*

**CALENDARIO PER LE VALUTAZIONI DI SORVEGLIANZA OBBLIGATORIE**

1. L'articolo 18 specifica i requisiti per il ciclo di certificazione, in particolare lo svolgimento di attività di valutazione periodiche. Tali attività comprendono come minimo le seguenti:

   a) una valutazione completa dell'oggetto della valutazione della conformità nella valutazione iniziale e in ogni valutazione di ricertificazione, compresa una caratteristica di aggiornamento di qualsiasi componente del prodotto;

   b) una valutazione delle vulnerabilità nella valutazione iniziale e in ogni valutazione di ricertificazione, e almeno ogni due anni nelle valutazioni di sorveglianza, che comprenda almeno le modifiche nell'oggetto della valutazione della conformità e le modifiche nel panorama delle minacce dall'ultima valutazione delle vulnerabilità;

   c) attività supplementari quali i test di penetrazione in caso di aumento del livello di rischio o di insorgenza di minacce nuove;

   d) una valutazione dell'efficacia operativa dei processi di manutenzione almeno ogni anno nelle valutazioni di sorveglianza e di ricertificazione, che comprenda come minimo i processi di controllo, aggiornamento e gestione delle vulnerabilità delle versioni;

   e) a seguito di un riesame e di una decisione relativa alla certificazione aventi esito positivo, il rilascio di un certificato di conformità dopo la valutazione iniziale e dopo ogni valutazione di ricertificazione.

2. Nella tabella 1 è riportato un calendario di riferimento basato su un ciclo quadriennale, nel contesto del quale:

   a) l'anno 1 inizia con il primo rilascio del certificato di conformità; nonché

   b) tutte le attività di valutazione devono essere svolte entro 12 mesi dalla valutazione dell'anno precedente.

3. Il calendario di cui alla tabella 1 costituisce una raccomandazione volta a garantire una ricertificazione tempestiva e ad evitare perturbazioni nella fornitura della soluzione di portafoglio. Altri calendari possono essere possibili nella misura in cui la validità del certificato di conformità non superi i cinque anni, come stabilito all'articolo 5 *quater*, paragrafo 4, del regolamento (UE) n. 910/2014.

4. Oltre alle valutazioni periodiche, può essere avviata una valutazione speciale su richiesta dell'organismo di certificazione o del titolare del certificato di conformità, a seguito di una modifica significativa dell'oggetto della certificazione o del panorama delle minacce.

5. Qualsiasi valutazione, comprese le valutazioni di sorveglianza e le valutazioni speciali, potrebbe portare al rilascio di un certificato di conformità nuovo, in particolare in caso di modifiche significative dell'oggetto della certificazione, ma avente la stessa data di scadenza del certificato di conformità originale.

*Tabella 1*

**Un ciclo di valutazione completo quadriennale**

| Tempo | Tipo di val. | Attività |
|---|---|---|
| Anno 0 | Iniziale | — Valutazione completa dell'oggetto della certificazione, compresa la valutazione delle vulnerabilità<br>— compresa una caratteristica per effettuare aggiornamenti relativi a ciascun componente software;<br>— valutazione dei processi di manutenzione, esclusa la loro efficacia operativa;<br>— rilascio del certificato di conformità e avvio del ciclo quadriennale. |
| Anno 1 | Sorveglianza | — Valutazione dell'efficacia operativa dei processi di manutenzione:<br>— come minimo verifica, aggiornamento, gestione delle vulnerabilità delle versioni;<br>— valutazione delle modifiche che incidono sulla sicurezza del prodotto. |

| Tempo | Tipo di val. | Attività |
|---|---|---|
| Anno 2 | Sorveglianza | — Valutazione delle vulnerabilità della soluzione completa;<br>— valutazione dell'efficacia operativa dei processi di manutenzione:<br>— come minimo controllo, aggiornamento, gestione delle vulnerabilità delle versioni;<br>— valutazione delle modifiche che incidono sulla sicurezza del prodotto. |
| Anno 3 | Sorveglianza | — Valutazione dell'efficacia operativa dei processi di manutenzione:<br>— come minimo verifica, aggiornamento, gestione delle vulnerabilità delle versioni;<br>— valutazione delle modifiche che incidono sulla sicurezza del prodotto. |
| Anno 4 | Ricertificazione | 1) Valutazione completa dell'oggetto della certificazione, compresa la valutazione delle vulnerabilità<br>2) valutazione semplificata per caratteristiche/processi che non sono cambiati;<br>3) compresa una caratteristica per effettuare aggiornamenti relativi a ciascun componente software;<br>4) valutazione dei processi di manutenzione, compresa la loro efficacia operativa;<br>5) rilascio di un certificato di conformità nuovo. |