NUMERO DI FASCICOLO: 2022-0941
IDENTIFICATIVO DELLA CLASSIFICAZIONE: 3.2.3

Quadro di fiducia

per l’identificazione elettronica svedese

Versione del 4 ottobre 2022

1. Contesto e finalità

Il quadro di fiducia per l'identificazione elettronica svedese mira a stabilire requisiti comuni per gli emittenti di identificazioni elettroniche esaminati e approvati dall'Agenzia svedese per il governo digitale (DIGG). I requisiti sono suddivisi in diversi livelli di protezione, noti come livelli di garanzia, che corrispondono a diversi gradi di sicurezza tecnica e operativa da parte dell'emittente e diversi gradi di verifica che la persona a cui è rilasciato un documento di identificazione elettronica sia effettivamente chi afferma di essere.

I requisiti del presente quadro di fiducia si applicano ai livelli di garanzia da 2 a 4, con il livello 4 corrispondente al livello massimo di protezione.

La conformità è interpretata come segue:

(a) se il livello di garanzia non è specificato, il requisito è soddisfatto a tutti i livelli, mentre

(b) se il livello di garanzia è specificato, la conformità è garantita almeno al livello pertinente.

I requisiti fissati per un livello inferiore a quello pertinente non sono presi in considerazione.

2. Organizzazione e governance

Requisiti operativi generali

K2.1 Gli emittenti di identificazioni elettroniche (e-ID) svedesi che non sono enti pubblici operano come persone giuridiche registrate e sottoscrivono e mantengono l'assicurazione richiesta per l'attività.

K2.2 Gli emittenti di e-ID svedesi devono avere un'attività consolidata, essere pienamente operativi in tutte le parti specificate nel presente documento ed essere esperti nei requisiti giuridici imposti loro in qualità di emittenti di e-ID svedesi.

K2.3 Gli emittenti di e-ID svedesi devono essere in grado di sostenere il rischio di responsabilità per danni e possedere risorse finanziarie sufficienti per condurre le loro operazioni per almeno un anno.

Sicurezza delle informazioni

K2.4 Gli emittenti di e-ID svedesi hanno istituito un sistema di gestione della sicurezza delle informazioni (ISMS) per le parti delle loro attività interessate dal quadro di fiducia, che si basa, se del caso, sulla norma ISO/IEC 27001 o su principi equivalenti per la gestione e il controllo delle attività in materia di sicurezza delle informazioni, tra cui:

(a) tutti i processi amministrativi e tecnici critici per la sicurezza devono essere documentati e basati su una base formale, in cui i ruoli, le responsabilità e i poteri sono chiaramente definiti.

(b) Gli emittenti di e-ID svedesi garantiscono di disporre in ogni momento di risorse umane sufficienti per adempiere ai loro obblighi.

(c) Gli emittenti di e-ID svedesi istituiscono un processo di gestione del rischio che, in modo appropriato, in modo continuo o almeno ogni 12 mesi, analizza le minacce e le vulnerabilità nell'impresa e che, attraverso l'introduzione di misure di sicurezza, bilancia i rischi a livelli accettabili.

(d) Gli emittenti di e-ID svedesi istituiscono un processo di gestione degli incidenti che garantisca sistematicamente la qualità del servizio, le forme di segnalazione successiva e l'adozione di adeguate misure reattive e preventive per attenuare o prevenire i danni derivanti da tali eventi.

(e) Gli emittenti di e-ID svedesi stabiliscono e testano periodicamente un piano di continuità che soddisfi i requisiti di accessibilità dell'impresa attraverso la capacità di ripristinare i processi critici in caso di crisi o incidenti gravi.

(f) Gli emittenti di e-ID svedesi valutano regolarmente il lavoro svolto in materia di sicurezza delle informazioni e introducono misure di miglioramento nel sistema di gestione.

K2.5 Portata e maturità del sistema di gestione:

Livello 4: Il sistema di gestione della sicurezza delle informazioni è conforme alla norma SS-ISO/IEC 27001:2017 o a versioni successive equivalenti o internazionali della norma e, nell'ambito di tale norma, includono tutti i requisiti imposti agli emittenti di e-ID svedesi.

Condizioni di subappalto

K2.6 Un emittente di e-ID svedesi che ha esternalizzato a un'altra parte l'esecuzione di uno o più processi critici per la sicurezza definisce per contratto i processi critici di cui è responsabile il subappaltatore e quali requisiti sono ad essi applicabili e chiarisce il rapporto contrattuale nella dichiarazione dell'emittente.

Tracciabilità, cancellazione e archiviazione dei documenti

K2.7 Gli emittenti di e-ID svedesi conservano:

(a) i documenti relativi alla richiesta, al rilascio, alla ricezione o al blocco delle e-ID;

(b) i contratti, i documenti di politica e le dichiarazioni dell'emittente; e

(c) l'elaborazione della cronologia e di altra documentazione necessaria per dimostrare la conformità ai requisiti imposti agli emittenti di e-ID svedesi e che consenta un follow-up che dimostri l'esistenza e l'efficacia dei processi e dei controlli critici per la sicurezza.

K2.8 Il periodo di conservazione non è inferiore a cinque anni e il materiale può essere prodotto in forma leggibile per tutto il periodo in questione, a meno che un requisito di cancellazione non sia necessario dal punto di vista della privacy e sia supportato dalla legge o da altri regolamenti.

Revisione e follow-up

K2.9 Gli emittenti di e-ID svedesi istituiscono una funzione di revisione interna che riesamina periodicamente le attività di emissione. Il revisore interno è indipendente nell'esercizio delle sue funzioni in modo da garantire un riesame obiettivo e imparziale e dispone delle competenze e dell'esperienza necessarie per l'esercizio delle sue funzioni. Il revisore interno pianifica in modo indipendente lo svolgimento della revisione e lo documenta in un piano di revisione che copre un periodo di tre anni. Gli elementi di revisione sono selezionati sulla base di un'analisi dei rischi e della rilevanza e si basano sulle descrizioni delle operazioni presentate dall'emittente all'Agenzia per il governo digitale.

Livelli 3 e 4: La revisione interna è effettuata sulla base di norme di revisione accettate.

3. Sicurezza fisica, amministrativa e orientata alle persone

K3.1 Le parti centrali dell'operazione sono fisicamente protette contro i danni causati da eventi ambientali, dall'accesso non autorizzato o da altre perturbazioni esterne. Il controllo dell'accesso è applicato in modo tale che l'accesso alle aree sensibili sia limitato al personale autorizzato, che i supporti che contengono informazioni siano conservati e smaltiti in modo sicuro e che l'accesso a tali aree protette sia costantemente monitorato.

K3.2 Prima che una persona assuma uno dei ruoli individuati conformemente al punto K2.4, lettera a), che sono di particolare importanza per la sicurezza, l'emittente di e-ID svedesi ha effettuato controlli dei precedenti al fine di garantire che la persona possa essere considerata affidabile e che disponga delle qualifiche e della formazione necessarie per svolgere in modo sicuro i compiti derivanti dal ruolo.

K3.3 Gli emittenti dispongono di procedure atte a garantire che il solo personale specificamente autorizzato abbia accesso ai dati raccolti e conservati conformemente al punto K2.7.

K3.4 **Livelli 3 e 4:** Gli emittenti garantiscono, lungo tutta la catena del processo di emissione, che la separazione dei compiti sia applicata in modo tale che nessuna persona sia in grado di ottenere un'e-ID a nome di un'altra persona.

4. Sicurezza tecnica

K4.1 Gli emittenti di e-ID svedesi garantiscono che i controlli tecnici in atto siano sufficienti a conseguire il livello di protezione ritenuto necessario in relazione alla natura, alla portata e ad altre circostanze dell'attività, e che tali controlli funzionino e siano efficaci.

K4.2 I mezzi di comunicazione elettronici utilizzati per la trasmissione di dati sensibili sono protetti da intercettazione, manipolazione e riproduzione.

K4.3 Il materiale crittografico sensibile utilizzato per rilasciare e-ID, identificare i titolari e rilasciare certificati di identità è protetto in modo tale che:

(a) l'accesso sia limitato, logicamente e fisicamente, ai ruoli e alle applicazioni strettamente necessari;

(b) il materiale per le chiavi non sia mai memorizzato in testo normale su supporti di memorizzazione persistenti;

(c) il materiale per le chiavi sia protetto dall'uso di un modulo hardware crittografico con meccanismi di sicurezza attivi che contrastino i tentativi sia fisici che logici di compromettere il materiale per le chiavi;

(d) i meccanismi di sicurezza per la protezione del materiale per le chiavi siano trasparenti e basati su norme riconosciute e consolidate; e

(e) **Livelli 3 e 4:** i dati di attivazione per la protezione del materiale per le chiavi siano gestiti attraverso il controllo di più persone.

K4.4 Gli emittenti dispongono di procedure documentate per garantire che il livello di protezione richiesto nell'ambiente informatico pertinente possa essere mantenuto nel tempo e in relazione alle modifiche, comprese valutazioni periodiche delle vulnerabilità e un'adeguata preparazione per far fronte all'evoluzione dei livelli di rischio e agli incidenti che si verificano.

5. Domanda, identificazione e registrazione

Informazioni sulle condizioni

K5.1 Gli emittenti di e-ID svedesi forniscono informazioni sui contratti, i termini e le condizioni, nonché le relative informazioni e le eventuali restrizioni all'uso del servizio, agli utenti connessi, ai fornitori di servizi elettronici e ad altri soggetti che possono fare affidamento sul servizio dell'emittente.

K5.2 L'emittente di e-ID svedesi fa un chiaro riferimento riferimento ai termini e alle condizioni e definisce le procedure in modo che i termini e le condizioni siano forniti al richiedente nel processo di emissione.

K5.3 Gli emittenti di e-ID svedesi forniscono una dichiarazione dell'emittente che comprenda:

(a) l'identità e i dati di contatto dell'emittente;

(b) brevi descrizioni dei servizi e delle soluzioni forniti dall'emittente, compresi i metodi applicati per l'applicazione, l'emissione e il blocco;

(c) le condizioni associate al servizio fornito, compresi gli obblighi dell'utente di proteggere la propria identificazione elettronica, gli obblighi e le responsabilità dell'emittente, le garanzie fornite e la disponibilità promessa;

(d) informazioni sul trattamento dei dati personali e sulle modalità in cui questo viene effettuato; e

(e) disposizioni per modificare i termini o le altre condizioni del servizio fornito, comprese le misure da adottare per interrompere il servizio in modo controllato.

K5.4 **Livelli 3 e 4:** Gli emittenti di e-ID svedesi, su richiesta dell'Agenzia per il governo digitale (DIGG) o di un'altra parte contraente che fa affidamento sui servizi forniti dall'emittente, forniscono informazioni sulle modalità di proprietà e gestione dell'attività.

K5.5 L'emittente di e-ID svedesi che cessa le sue attività segue un piano prestabilito per la cessazione del servizio. Il piano include l'informazione di tutti gli utenti del servizio e del DIGG. L'emittente tiene inoltre a disposizione il materiale archiviato conformemente ai punti K2.7 e K2.8 dopo l'interruzione.

Domanda

K5.6 Un'e-ID svedese può essere rilasciata solo su richiesta del richiedente o tramite un'altra procedura di accettazione equivalente e solo dopo che il richiedente è stato informato delle condizioni in base alle quali viene rilasciata e della responsabilità che gli sarà attribuita.

Tuttavia, il rilascio di un'e-ID che sostituisce o integra un documento di e-ID valido o recentemente bloccato rilasciato in precedenza dallo stesso emittente può avvenire senza alcuna procedura di domanda preliminare.

K5.7 La domanda di e-ID svedese è collegata a un numero d'identità personale o a un numero di coordinamento, nonché alle informazioni altrimenti necessarie all'emittente per fornire tale e-ID.

Determinazione dell'identità del richiedente

K5.8 Gli emittenti di e-ID svedesi devono verificare che le informazioni collegate alla domanda siano complete e corrispondano alle informazioni registrate in un registro ufficiale.

K5.9 Se le informazioni da controllare in un registro ufficiale sono contrassegnate come riservate («identità protetta»), i controlli necessari possono essere effettuati con altri mezzi equivalenti.

K5.10 Identificazione del richiedente durante una visita in presenza:

Gli emittenti di e-ID svedesi possono verificare l'identità del richiedente durante una visita di persona, nello stesso modo si rilascia un documento d'identità standard.

K5.11 Identificazione a distanza del richiedente nella relazioneesistente:

Livello 3: Gli emittenti di e-ID svedesi che hanno già identificato il richiedente in una relazione che comporta transazioni economicamente o giuridicamente significative e in cui il richiedente può essere identificato a distanza con altri mezzi affidabili equivalenti ai requisiti di livello 3 del marchio di qualità e-ID svedese, possono utilizzare questo metodo per stabilire l'identità del richiedente.

Livello 4: Non pertinente.

K5.12 Identificazione tramite e-ID svedese:

Un emittente di e-ID svedesi può identificare il richiedente a distanza mediante un'e-ID svedese valida almeno dello stesso livello di garanzia di quella da rilasciare, se può, senza ostacoli contrattuali, utilizzare tale identificazione come base per il rilascio di una nuova e-ID.

Livello 4: Il periodo di validità dell'e-ID di nuova emissione non deve estendersi oltre il periodo di validità dell'e-ID esistente.

K5.13 Identificazione a distanza del richiedente:

Livello 2: Gli emittenti di e-ID svedesi possono utilizzare registrazioni di immagini affidabili di un documento di identità standard valido e dell'immagine del volto del richiedente come base per stabilire l'identità del richiedente a distanza se il confronto non dà adito a dubbi sulla vera identità del richiedente.

Livello 3: Gli emittenti di e-ID svedesi possono, mediante una lettura sicura di un documento d'identità standard valido contenente dati biometrici memorizzati elettronicamente, stabilire a distanza l'identità del richiedente sulla base di tali dati se i corrispondenti dati biometrici della persona da identificare possono essere raccolti in modo sufficientemente sicuro per poter effettuare un confronto

con un'affidabilità equivalente a quella di una visita di persona, e se il confronto non dà adito a dubbi sulla vera identità del richiedente.

Livello 4: Non pertinente.

Registrazione

K5.14 Gli emittenti di e-ID svedesi, tenendo conto delle norme applicabili in materia di protezione dei dati personali, tengono un registro degli utenti connessi e dei documenti di identificazione elettronica assegnati e mantengono aggiornato tale registro.

6. Rilascio e blocco dell’e-ID

Progettazione dei mezzi tecnici

K6.1 Mezzi tecnici:

Livelli 2 e 3: I mezzi tecnici per l'identificazione elettronica tramite e-ID con il marchio di qualità svedese delle e-ID sono progettati secondo un principio a due fattori, in base al quale una parte consiste in informazioni memorizzate elettronicamente che l'utente deve conservare, e l'altra in ciò che l'utente deve utilizzare per attivare l'e-ID.

Livello 4: I mezzi tecnici per l'identificazione elettronica tramite e-ID con il marchio di qualità svedese delle e-ID sono progettati secondo un principio a due fattori, in base al quale una parte consiste in un modulo di sicurezza personale di cui l'utente è in possesso, e l'altra in ciò che l'utente utilizza per attivare il modulo di sicurezza.

K6.2 Il meccanismo di attivazione e il codice personalizzato sono progettati in modo tale che sia improbabile che terzi violino la protezione, anche con mezzi meccanici.

Livelli 3 e 4: La protezione comprende meccanismi per impedire la copia e la manipolazione del documento di identificazione elettronica.

K6.3 Gli utenti dell'e-ID con il marchio di qualità svedese delle e-ID devono poter scambiare o richiedere un nuovo codice personale, di propria iniziativa, entro il periodo di validità dell'e-ID e in modo gratuito e senza inconvenienti significativi e, attraverso orientamenti o produzione automatica, essere aiutati a mantenere i requisiti di K6.2.

Se l'e-ID è progettato in modo tale che un codice personalizzato non possa essere scambiato, l'utente dovrebbe invece, alle stesse condizioni, essere prontamente in grado di ottenere un nuovo e-ID con un nuovo codice personalizzato che sostituisca il precedente tramite una procedura di blocco.

K6.4 Gli emittenti di e-ID svedesi garantiscono che i dati registrati per l'identificazione elettronica dei titolari rappresentino in modo univoco il richiedente e siano attribuiti alla persona in questione al momento del rilascio del documento di e-ID.

K6.5 Il periodo di validità delle e-ID rilasciate è limitato tenendo conto delle caratteristiche di sicurezza del documento di e-ID e dei rischi di uso improprio. Il periodo massimo di validità dell'e-ID è di cinque anni.

Fornitura del documento di e-ID

K6.6 Fornitura da remoto:

Livello 2: Un emittente di e-ID svedesi fornisce il documento di e-ID in modo da confermare i dati di contatto conservati nel registro ufficiale o le informazioni registrate in relazione alla procedura elettronica conformemente al K5.13 livello 2.

Livello 3: Un emittente di e-ID svedesi che fornisce un'e-ID tramite procedura elettronica conforme a K5.11 livello 3, K5.12 livello 3 o K5.13 livello 3 assicura, in caso di nuova emissione, separatamente e indipendentemente dalla fornitura in termini di sicurezza, che l'utente sia informato che tale documento di e-ID è stato consegnato, o con altre misure garantire un grado equivalente di controllo affinché la persona sia avvisata del rischio di furto di identità in relazione alla fornitura.

Livello 4: Un emittente di e.ID svedese che fornisce un'e-ID tramite una procedura elettronica conforme al livello 4 K5.12 garantisce, in caso di nuova emissione, separatamente e indipendentemente dalla fornitura in termini di sicurezza, che l'utente sia informato che tale documento di e-ID è stato consegnato.

K6.7 Fornitura durante una visita di persona:

Durante una visita di persona e dopo un controllo di identità conformemente al punto K5.10, l'emittente di e-ID svedesi fornisce il documento di identificazione elettronica contro ricevuta firmata e fornisce inoltre la parte che l'utente deve utilizzare per attivare l'e-ID separatamente e indipendentemente dalla fornitura del documento di identificazione elettronica in termini di sicurezza, sulla base dei dati di contatto conservati in un registro ufficiale o di altre informazioni di credibilità equivalente.

Servizio di blocco

K6.8 Gli emittenti di e-ID svedesi forniscono un servizio di blocco con una buona accessibilità per consentire all'utente di bloccare la propria e-ID.

K6.9 Gli emittenti di e-ID svedesi elaborano ed eseguono tempestivamente e in modo sicuro le richieste di blocco e adottano misure per prevenire l'uso improprio sistematico del servizio di blocco o altre azioni intenzionaliche portano al blocco generalizzato dei documenti di identificazione elettronica, garantendo che le e-ID degli utenti siano disponibili quando necessario

7. Verifica delle identità elettroniche dei titolari

K7.1 Gli emittenti di e-ID svedesi garantiscono che, al momento di verificare l'identità del titolare, siano effettuati controlli affidabili sull'autenticità e sulla validità del documento di e-ID.

K7.2 Gli emittenti di e-ID svedesi garantiscono l'attuazione di controlli tecnici di sicurezza in sede di verifica dell'identità elettronica dei titolari, in modo che sia improbabile che terzi possano violare i meccanismi di protezione indovinando, intercettando, riproducendo o manipolando il processo.

8. Rilascio di certificati di identità

Gli emittenti di e-ID svedesi che forniscono un servizio per il rilascio di certificati di identità ai servizi elettronici facenti affidamento rispettano altresì le disposizioni della presente sezione.

K8.1 Gli emittenti di e-ID svedesi garantiscono che il servizio di rilascio dei certificati di identità abbia una buona accessibilità e che il rilascio dei certificati di identità sia preceduto da un'identificazione affidabile conformemente alle disposizioni della sezione 7.

Livello 4: I certificati includono un riferimento al materiale di chiave crittografica verificato dall'emittente come in possesso esclusivo del titolare.

K8.2 I certificati di identità presentati sono validi solo per il tempo necessario a consentire all'utente l'accesso al servizio elettronico richiesto e sono protetti in modo che le informazioni possano essere lette solo dal destinatario previsto e che l'autenticità dei certificati possa essere verificata dai destinatari dei certificati.

K8.3 Gli emittenti di e-ID svedesi, tenendo conto dei rischi di uso improprio del servizio di certificazione, limitano il periodo di tempo entro il quale possono essere rilasciati più certificati di identità consecutivi a un determinato titolare prima che quest'ultimo sia nuovamente identificato conformemente alle disposizioni della sezione 7.