Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Berna, 20 giugno 2025

Progetto di ordinanza sull'ld-e

Rapporto esplicativo per l'avvio della procedura di consultazione

Compendio

L'ordinanza concernente la legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (ordinanza sull'Id-e; OIdE) precisa in particolare le procedure e le competenze per l'emissione e l'utilizzo dell'e-ID. Definisce inoltre l'infrastruttura di fiducia statale, che consente ad autorità e attori privati di emettere e verificare in modo sicuro mezzi di autenticazione elettronici. L'obiettivo dell'ordinanza è di creare una base chiara e sicura per utilizzare l'e-ID e altri mezzi di autenticazione elettronici.

Situazione iniziale

Dopo l'esito negativo della votazione popolare del 7 marzo 2021 sulla legge federale sui servizi d'identificazione elettronica, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia di sviluppare, insieme alla Cancelleria federale e al Dipartimento federale delle finanze, un mezzo d'identificazione elettronico statale sicuro. Il 13 giugno 2022 il Consiglio nazionale e il Consiglio degli Stati hanno accolto sei mozioni che chiedevano la creazione di un mezzo d'identificazione elettronico statale. Il 22 novembre 2023 il Consiglio federale ha adottato l'avamprogetto della legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (LIdE) con lo scopo di introdurre un mezzo d'identificazione elettronico statale gratuito e facoltativo che permettesse di provare la propria identità per via elettronica in modo semplice e sicuro. L'e-ID sarà emesso dalla Confederazione e garantirà la maggiore protezione possibile dei dati personali, in particolare tramite la minimizzazione dei dati. Ai fini dell'autodeterminazione digitale, l'emissione e l'utilizzo dell'e-ID sono facoltativi. Ai titolari sarà inoltre garantito il controllo dei loro dati. Oltre all'e-ID è in corso la digitalizzazione di altri mezzi di autenticazione. La Confederazione mette a disposizione la necessaria infrastruttura di fiducia, compresi il portafoglio elettronico (wallet), l'applicazione per la verifica dei mezzi di autenticazione elettronici, il registro di base e il registro di fiducia. Tale infrastruttura potrà essere utilizzata pure da privati che intendono emettere e verificare mezzi di autenticazione elettronici. Nella votazione finale del 20 dicembre 2024 il Parlamento ha approvato a larga maggioranza la LIdE (Consiglio nazionale: 170 favorevoli, 25 contrari, 1 astensione; Consiglio degli Stati: 43 favorevoli, 1 contrario, 0 astensioni). Il 7 maggio è formalmente riuscito il referendum sulla LIdE; la votazione si terrà il 28 settembre 2025.

Se il Popolo respinge il referendum, la LIdE entrerà in vigore al più presto a metà 2026. Fino ad allora, il Consiglio federale deve poter adottare anche le disposizioni di esecuzione. Tuttavia, ciò è possibile soltanto se la

procedura di consultazione viene aperta prima della votazione sul referendum.

Contenuto del progetto

La LIdE intende permettere, in futuro, agli abitanti della Svizzera e agli Svizzeri all'estero di identificarsi in forma elettronica in modo semplice, sicuro e rapido. L'avamprogetto d'ordinanza concretizza l'attuazione di tale legge e disciplina in particolare l'infrastruttura di fiducia, l'e-ID e gli aspetti tecnici e organizzativi connessi ai mezzi di autenticazione elettronici. L'infrastruttura di fiducia è pensata per tutti i mezzi di autenticazione elettronici e comprende il registro di base, che contiene gli identificativi, il registro di fiducia, necessario per controllare tali identificativi, nonché applicazioni per conservare e verificare i mezzi di autenticazione elettronici. Il progetto in consultazione disciplina l'iscrizione, l'utilizzo e la cancellazione di informazioni concernenti i mezzi di autenticazione elettronici da parte di persone fisiche e giuridiche.

L'e-ID è richiesto online e l'Ufficio federale di polizia è responsabile della sua emissione. L'identità può essere verificata online o in presenza presso i centri cantonali di registrazione o, nel caso degli Svizzeri all'estero, presso la rappresentanza consolare svizzera competente. Per la verifica dell'identità online occorre fotografare il documento d'identità e registrare l'immagine del viso sotto forma di sequenze video; la verifica si svolge in modo automatizzato. Le sequenze video vengono confrontate con l'immagine del viso registrata nei sistemi d'informazione di cui all'articolo 17 capoverso 2 LIdE (p. es. nel sistema d'informazione sui documenti d'identità). Se i dati corrispondono, il richiedente riceve l'e-ID direttamente sul suo dispositivo. I Cantoni e le rappresentanze consolari svizzere all'estero che verificano l'identità in presenza potrebbero adottare procedure differenti.

Importanti informazioni tecniche concernenti, ad esempio, il formato e gli standard dei mezzi di autenticazione elettronici sono pubblicati come raccomandazioni, ma possono essere dichiarati in parte vincolanti.

Indice

Rapporto esplicativo

1 Punti essenziali del progetto

La LIdE mette a disposizione degli abitanti della Svizzera e degli Svizzeri all'estero un mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici di elevata qualità in modo rapido e sicuro. Il presente progetto di ordinanza concretizza l'attuazione della LIdE. Disciplina in particolare l'infrastruttura di fiducia e l'e-ID nonché l'attuazione degli aspetti tecnici e organizzativi connessi con l'utilizzo di mezzi di autenticazione elettronici in generale.

1.1 Infrastruttura di fiducia

La LIdE prevede che le componenti essenziali dell'infrastruttura di fiducia non siano destinate unicamente all'e-ID, ma in linea di massima a tutti i mezzi di autenticazione elettronici compatibili. Essa disciplina:

- il registro di base, in cui gli emittenti di mezzi di autenticazione elettronici possono iscrivere i dati richiesti, ad esempio i loro identificativi;

- il registro di fiducia, ovvero il sistema che permette di confermare gli identificativi iscritti nel registro di base;

- l'applicazione per conservare e presentare mezzi di autenticazione elettronici e il sistema per le copie di sicurezza; e

- l'applicazione per verificare i mezzi di autenticazione elettronici.

In generale, il progetto di ordinanza precisa le procedure di iscrizione, utilizzo e cancellazione dei dati nell'infrastruttura di fiducia, applicabili a tutte le persone fisiche e giuridiche che intendono emettere e utilizzare mezzi di autenticazione elettronici.

1.2 Procedura di richiesta e di emissione dell'e-ID

Il progetto di ordinanza concretizza la richiesta, la verifica dell'identità, l'emissione e la revoca dell'e-ID emesso dalla Confederazione. L'e-ID viene richiesto online e l'identità può essere verificata online o in presenza presso i centri cantonali di registrazione o, nel caso degli Svizzeri all'estero registrati al consolato, presso la rappresentanza consolare svizzera competente. L'Ufficio federale di polizia (fedpol) è competente per emettere l'e-ID.

In una prima fase, il richiedente installa l'applicazione per conservare e presentare mezzi di autenticazione elettronici della Confederazione (portafoglio elettronico statale, wallet della Confederazione) sul suo dispositivo (p. es. sullo smartphone). In una seconda fase, fotografa il suo documento d'identità ufficiale (carta d'identità, passaporto, carta di soggiorno per stranieri) e registra l'immagine del viso sotto forma di sequenze video. I dati vengono trasmessi per verifica tramite l'applicazione del servizio statale.

In linea di massima la verifica viene effettuata in modo automatizzato. Se i dati trasmessi corrispondono a quelli iscritti nei registri ufficiali, l'e-ID sarà disponibile immediatamente sul dispositivo del richiedente. L'e-ID può essere emesso contemporaneamente in più applicazioni su uno o più dispositivi. Questa procedura dovrebbe richiedere solo pochi minuti. Tuttavia, è possibile che, quando verrà introdotto l'e-ID, i tempi di attesa saranno più lunghi (lista d'attesa). Il sistema per l'emissione verrà gradualmente ampliato garantendone la qualità.

L'identità può essere fatta verificare in presenza presso un centro cantonale di registrazione o una rappresentanza consolare. La procedura di verifica può variare perché è di competenza dei Cantoni e della Confederazione (per le rappresentanze della Svizzera all'estero).

1.3 Informazioni tecniche

Per garantire un utilizzo sicuro dell'e-ID sono precisati i requisiti tecnici dell'e-ID. Il Dipartimento federale di giustizia e polizia (DFGP) disciplina il formato tecnico e gli attributi per la trasmissione dei dati, i requisiti dell'interfaccia con il sistema d'informazione per l'emissione e la revoca dell'e-ID nonché gli standard e i protocolli per la comunicazione dei dati nell'ambito dell'emissione dell'e-ID.

Le informazioni tecniche seguenti sono pubblicate principalmente come raccomandazioni (art. 33 e 34): il formato dei mezzi di autenticazione elettronici, gli standard e i protocolli per la procedura di comunicazione dei dati nell'ambito dell'emissione e della presentazione dei mezzi di autenticazione elettronici. Il DFGP può prevedere che le raccomandazioni o parti di esse siano dichiarate vincolanti (art. 35).

2 Diritto comparato, rapporto con il diritto europeo

L'Unione europea (UE) ha avviato una serie di riforme nell'ambito dell'identità digitale. Il Consiglio federale ritiene necessario tenere conto di questi sviluppi nelle riflessioni condotte in proposito a livello nazionale. Il 3 giugno 2021, la Commissione europea ha adottato una proposta che modifica il regolamento (UE) 910/2014 (regolamento eIDAS) e introduce un quadro giuridico per un'identità digitale europea. In base al nuovo regolamento, è previsto che nei 24 mesi successivi all'entrata in vigore delle nuove disposizioni, gli Stati membri mettano a disposizione dei cittadini portafogli elettronici che collegano la loro identità elettronica nazionale ai mezzi di autenticazione di altri attributi personali (p.es. licenza di condurre, diplomi, conto bancario). Questi portafogli possono essere emessi dalle autorità o da privati riconosciuti dagli Stati membri.

Il 30 aprile 2024 il Consiglio europeo ha adottato la proposta di modifica del regolamento eIDAS. Il quadro definito dalla Commissione europea si fonda sui principi dell'identità autogestita (Self-Sovereign Identity, SSI), ma non fornisce indicazioni di carattere tecnico sulle esatte modalità di attuazione di tali principi. Tra il 12 agosto 2024

e il 9 settembre 2024[1] così come tra il 29 novembre 2024 e il 2 gennaio 2025, la Commissione europea ha avviato la consultazione su cinque progetti relativi a regolamenti di esecuzione recanti modalità di applicazione del regolamento eIDAS. I regolamenti di esecuzione disciplinano in particolare standard tecnici, questioni procedurali e formati, al fine di garantire l'interoperabilità, l'affidabilità e la certezza del diritto negli Stati membri dell'UE. Si concentrano in particolare sugli incidenti legati alla sicurezza in relazione ai portafogli elettronici, all'utilizzo transfrontaliero dei mezzi d'identificazione elettronici nonché alla compilazione e alla gestione di un elenco di emittenti, verificatori e portafogli elettronici.

Rispetto all'UE, la Svizzera persegue un approccio meno regolamentato che lascia maggiore spazio all'innovazione e rinuncia a procedure di autorizzazione formali e costose nonché alla tenuta di elenchi. La Svizzera non è giuridicamente tenuta a recepire il regolamento eIDAS, le relative modifiche e i regolamenti di esecuzione. Tuttavia, visti gli stretti rapporti commerciali e sociali che intrattiene con la maggior parte degli Stati membri dell'UE, ha interesse a introdurre un sistema di identità elettronica interoperabile con quello dell'UE. La LIdE prevede che il Consiglio federale possa concludere trattati internazionali per il riconoscimento dell'e-ID svizzero all'estero e il riconoscimento di e-ID stranieri in Svizzera (art. 32 LIdE). La presente ordinanza tiene conto degli sviluppi nell'UE e non va interpretata in modo tale da pregiudicare la compatibilità con l'identificazione elettronica prevista dal diritto europeo.

3 Commento ai singoli articoli

Ingresso

La presente ordinanza si fonda su vari articoli della LIdE. Gli articoli 2 capoverso 5 lettera a, 3 capoverso 7, 4, 8 capoversi 2 e 3, 9 capoverso 2, 17 capoverso 1, 18 capoversi 5 e 6, 20, 21, 28 capoverso 4, 30, 31 capoverso 5, 33 e 35 capoverso 2 LIdE non però sono citati singolarmente nell'ingresso.

Capitolo 1: Oggetto

Art. 1

Nel complesso l'ordinanza si prefigge di garantire la gestione ineccepibile e sicura dell'infrastruttura di fiducia e dell'e-ID in quanto mezzo di autenticazione elettronico, salvaguardando in tal modo la sicurezza (in particolare l'affidabilità del sistema) e l'inclusione. Ciò viene garantito mediante condizioni tecniche e regole procedurali. L'accento è posto sulla sicurezza per impedire gli abusi o la manipolazione nonché instaurare e conservare la fiducia nel sistema.

[1] Regolamenti di esecuzione (UE) della Commissione (2024/2977, 2024/2979, 2024/2980, 2024/2981, 2024/2982) adottati il 4 dic. 2024.

L'ordinanza stabilisce le regole di base per allestire e gestire i registri, le applicazioni per conservare e presentare mezzi di autenticazione elettronici (portafoglio elettronico statale[2]), nonché l'applicazione per verificare i mezzi di autenticazione elettronici (check app della Confederazione) (lett. a). Disciplina l'intero processo relativo all'identità elettronica (e-ID) che comprende la richiesta di emissione, la verifica dell'identità del richiedente, l'effettiva emissione nonché le condizioni per la revoca dell'e-ID (lett. b). Inoltre, precisa le modalità di conservazione dei dati personali e determina come e quando questi devono essere cancellati. Ciò riguarda in particolare i dati relativi alla procedura di emissione di un e-ID o di altri mezzi di autenticazione elettronici (lett. c).

Capitolo 2: Infrastruttura di fiducia

L'infrastruttura di fiducia, con i relativi servizi, costituisce un'applicazione specializzata dell'Ufficio federale di giustizia (UFG). L'UFG funge da mandante nei confronti dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e assume la responsabilità globale.

Sezione 1: Portale per il trattamento dei dati dei registri

Art. 2 Scopo e gestione

Un portale elettronico è messo a disposizione degli emittenti e dei verificatori di mezzi autenticazione elettronici per permettere loro di iscrivere dati nel registro di base e nel registro di fiducia. Questo portale, come altre piattaforme di registrazione, serve a raccogliere i dati necessari per l'iscrizione nei registri. L'UFG è competente per il portale.

L'iscrizione avviene mediante il portale elettronico messo a disposizione dal Dipartimento federale delle finanze sul quale vi è un'applicazione dedicata che permette a emittenti e verificatori di svolgere tutte le loro attività e di pagare gli emolumenti. A medio termine si intende realizzare il principio Once Only mediante l'integrazione in altri portali o il collegamento con pacchetti di dati esistenti.

Art. 3 Dati iscritti all'atto della registrazione

Cpv. 1

Ai fini della registrazione, gli emittenti e i verificatori di mezzi di autenticazione elettronici registrano i seguenti dati:

- per le persone fisiche: nome(i) e cognome(i);
- per le persone giuridiche o le società di persone:

[2] Il portafoglio elettronico porta il nome protetto: «swiyu».

- ditta, sede e numero d'identificazione delle imprese (IDI) secondo la legge federale del 18 giugno 2010[3] sul numero d'identificazione delle imprese;
- indirizzo;
- indirizzo di posta elettronica;
- numero di telefono;
- informazioni di pagamento.

A medio termine occorre valutare se il registro IDI può fornire direttamente i dati. Durante la consultazione occorre valutare da quando tale interfaccia potrebbe essere realizzata. Si esamina inoltre la possibilità di un confronto con il Registro federale degli edifici e delle abitazioni, affinché possano essere riprese automaticamente anche informazioni come la sede di una persona giuridica o di una società di persone. Secondo l'articolo 15*a* dell'ordinanza del 9 giugno 2017[4] sul Registro federale degli edifici e delle abitazioni, l'UFG segnala i dati errati all'Ufficio federale di statistica.

Cpv. 2

L'indirizzo, il numero di telefono, l'indirizzo di posta elettronica o altri dati di contatto non sono iscritti nei registri ma sono conservati presso l'UFIT. Tali dati non sono pubblicamente accessibili e servono soltanto per iscrivere e gestire rispettivamente i dati di base e la relazione commerciale nel sistema. La raccolta di informazioni di pagamento è necessaria perché emittenti e verificatori devono versare un emolumento per i dati che iscrivono nel registro di base e per i dati di cui chiedono l'iscrizione nel registro di fiducia (art. 38). Per evitare gravosi processi di controllo, eventuali cancellazioni dai registri e procedure di incasso, sono previsti esclusivamente pagamenti istantanei (p. es. tramite carte di credito).

Sezione 2: Registro di base

Art. 4 Contenuto

Dopo essersi registrato sul portale, l'emittente o il verificatore di mezzi di autenticazione elettronici ha accesso al registro di base, nel quale può iscrivere, mediante un'interfaccia tecnica, dati che servono a garantire l'autenticità e l'integrità dei mezzi di autenticazione elettronici che emette. Questi dati comprendono chiavi crittografiche pubbliche e indicazioni sui mezzi di autenticazione elettronici revocati. L'emittente ottiene pure un accesso protetto al registro di base per poter gestire i suoi mezzi di autenticazione revocati. Oltre agli emittenti, anche i verificatori possono iscrivere dati nel registro di base. All'atto dell'iscrizione dei suoi dati, l'emittente o il verificatore riceve un parametro

[3] RS **431.03**

[4] RS **431.841**

anonimo identificabile (identificativo). Il rispettivo identificativo è generato mediante un'interazione tecnica con l'UFIT. L'emittente o il verificatore è responsabile della gestione dei dati che iscrive. L'identificativo non permette di risalire all'identità dell'emittente o del verificatore.

I contenuti del registro di base sono pubblicamente accessibili mediante un'interfaccia che non richiede registrazione. È necessario consultare i dati per verificare la validità crittografica dei mezzi di autenticazione elettronici. I dati iscritti nel registro di base da un emittente o da un verificatore sono protetti dal trattamento da parte di terzi, di modo che soltanto l'emittente o il verificatore può trattarli e l'autenticità di tali dati è garantita in ogni momento.

Art. 5 Modifica e cancellazione dei dati da parte dell'emittente o del verificatore

L'emittente o il verificatore di mezzi di autenticazione elettronici dispone liberamente delle informazioni che iscrive nel registro di base. Mediante il portale può modificare o cancellare in ogni momento i dati che ha iscritto. In caso di cancellazione sono eliminati l'identificativo che gli è stato attribuito, la sua chiave crittografica e i dati sulla revoca di singoli mezzi di autenticazione. Pertanto, la validità dei mezzi di autenticazione già emessi non può più essere verificata perché le informazioni necessarie a tal fine non sono più disponibili.

L'emittente o il verificatore deve provare di essere il legittimo possessore dell'iscrizione, in particolare mediante l'identificativo o la necessaria chiave crittografica privata. Generalmente, questa tappa della verifica si svolge in modo automatizzato. Se la prova non può più essere fornita, ad esempio perché la chiave crittografica privata è andata persa, occorre rendere plausibile la legittima possessione dell'iscrizione in altro modo, ad esempio mediante i dati raccolti e verificati durante il processo di iscrizione nel registro di fiducia o mediante altri dati che permettono un'identificazione affidabile, se l'emittente o il verificatore non è registrato nel registro di fiducia. La disposizione è formulata in modo neutro sotto il profilo tecnologico per permettere altri tipi di prove tecniche in base all'evoluzione tecnica.

Invece di cancellare l'iscrizione, l'emittente o il verificatore di mezzi di autenticazione elettronici può disattivarlo, di modo che i mezzi di autenticazione già emessi rimangano verificabili. Possono così ad esempio essere verificati mezzi di autenticazione elettronici che conservano la loro validità malgrado siano stati emessi da un'organizzazione non più attiva. Se intende disporre successivamente di un identificativo attivo, l'emittente o il verificatore deve registrarsi di nuovo e iscrivere i dati nel registro di base.

Art. 6 Cancellazione dei dati non necessari

Cpv. 1 e 2

Se constata che un emittente o un verificatore iscrive nel registro di base dati che non sono necessari per le finalità di cui all'articolo 2 capoverso 1 LIdE, l'UFG incarica l'UFIT di cancellare tali dati o l'intera iscrizione. Tuttavia, prima che i dati siano cancellati, informa l'emittente o il verificatore interessato, sempre che ciò sia possibile con un

onere adeguato. Se i dati iscritti costituiscono una ciberminaccia o il loro contenuto è illecito, l'intera iscrizione è cancellata senza informare dapprima l'emittente o il verificatore interessato.

Cpv. 3

In occasione della consultazione del registro di base possono essere generati dati, segnatamente indirizzi IP e altri dati analoghi a seconda del protocollo utilizzato (art. 2 cpv. 5 lett. a LIdE). Tali dati possono essere registrati soltanto per mantenere la sicurezza delle informazioni e dei servizi, per assicurare la manutenzione tecnica dell'infrastruttura o per controllare il rispetto dei regolamenti di utilizzazione (art. 57*l* lett. b n. 1–3 della legge del 21 marzo 1997[5] sull'organizzazione del Governo e dell'Amministrazione). Lo scopo della registrazione è di garantire l'utilizzo e il funzionamento sicuri dell'infrastruttura di fiducia nonché l'utilizzo sicuro dell'e-ID e di altri mezzi di autenticazione elettronici. A tal fine occorre conservare i dati per 90 giorni al massimo; al più tardi dopo 90 giorni tali dati devono essere distrutti.

Art. 7 Conservazione di dati modificati o cancellati

I dati del registro di base che sono stati modificati o cancellati sono conservati per dieci anni dall'UFIT o da un altro servizio della Confederazione per garantire la tracciabilità dei dati contenuti nei registri. La tracciabilità di tali dati è di importanza centrale per garantire l'integrità, l'autenticità e il valore probatorio dei dati. In particolare, nelle vertenze giudiziarie si deve poter provare in quale momento sono stati pubblicati determinati dati. Di conseguenza, la conservazione dei dati dopo una modifica dell'iscrizione nel registro di base è determinante per la certezza del diritto. Il termine di dieci anni corrisponde al termine generale di conservazione nelle relazioni d'affari. Questi dati non sono pubblicamente accessibili.

La Confederazione conserva questi dati anche dopo la scadenza dei dieci anni, nella misura in cui ciò sia necessario per garantire un utilizzo sicuro dei mezzi di autenticazione elettronici. In questo caso può cancellare dal registro di base singoli dati o l'intera iscrizione. Questo termine è necessario per poter verificare retroattivamente la tracciabilità, il successivo identificativo di un emittente o di un verificatore precedentemente iscritto nel registro di base, nonché per un utilizzo sicuro e affidabile dei mezzi di autenticazione elettronici.

[5] RS **172.010**

Sezione 3: Registro di fiducia

Art. 8 Contenuto

Cpv. 1

L'UFIT mette a disposizione un sistema pubblicamente accessibile che contiene dati per la verifica dell'identità di emittenti e verificatori e per l'utilizzo sicuro di mezzi di autenticazione elettronici (registro di fiducia). Il registro di fiducia permette di consultare informazioni verificate dalla Confederazione sull'identità dei partecipanti collegati al sistema. Ad esempio, il legame tra l'identificativo e la chiave pubblica viene confermato e comunicato a fedpol. L'applicazione per la presentazione e la conservazione dei mezzi di autenticazione elettronici, in caso di transazione (richiesta di emissione o di verifica), in linea di massima mostra informazioni provenienti dal registro di fiducia. I partecipanti collegati al sistema possono decidere liberamente in ogni momento se consultare il registro di fiducia.

Se si consulta un identificativo confermato nel registro di fiducia, vengono mostrati l'identificativo iscritto nel registro di base e il nome o la ditta dell'emittente o del verificatore, insieme all'indicazione, se si tratta di un'autorità o di un servizio pubblico. Se l'emittente o il verificatore iscritto è una persona giuridica, sono visibili anche l'IDI nonché eventualmente ulteriori iscrizioni in altri registri, come ad esempio il registro di commercio. Il registro di fiducia contiene anche eventuali informazioni sui mezzi di autenticazione elettronici che possono essere emessi o verificati da autorità o servizi che adempiono compiti pubblici (art. 13)

Per la verifica crittografica dei mezzi di autenticazione elettronici o l'allestimento di canali di comunicazione tecnicamente sicuri, il registro di fiducia non è necessario ma mira a consolidare la fiducia di un attore nei confronti del suo interlocutore, ad esempio se tra loro non vi è alcuna relazione, se uno dei due desidera informazioni supplementari o se è necessaria una conferma dell'esattezza delle informazioni condivise. Per questo motivo nel registro di fiducia sono contenute le informazioni sull'identità di un attore verificate dalla Confederazione.

Il registro di fiducia offre quindi trasparenza, in modo che sia chiaro per tutti chi, ad esempio, richiede più dati del necessario durante la verifica di un mezzo di autenticazione elettronico. Se non è iscritto nel registro di fiducia, un emittente o un verificatore non viene identificato dalla Confederazione e quindi la sua identità non è confermata. I dati del registro di fiducia sono pubblicamente accessibili. Per consultare i dati pubblici non occorre registrarsi.

Cpv. 2

Oltre alla verifica degli identificativi, in caso di sospetto di utilizzo inappropriato dell'infrastruttura di fiducia o di un mezzo di autenticazione elettronico o se i formati, gli standard e i protocolli di cui all'articolo 35 non sono adempiuti, il registro di fiducia offre agli utenti una menzione di tale sospetto. La menzione serve per utilizzare in modo sicuro i mezzi di autenticazione elettronici e aiuta gli utenti dei portafogli elettronici a utilizzare le check app in modo sicuro.

L'obiettivo è rafforzare la fiducia nel traffico elettronico di dati e fornire agli utenti del sistema indicatori efficaci per un utilizzo sicuro. Oltre a verificare l'identità degli emittenti e dei verificatori, i partecipanti collegati al sistema devono poter avere la necessaria fiducia quando quotidianamente presentano e verificano i mezzi di autenticazione elettronici.

Art. 9 Richiesta di iscrizione nel registro di fiducia

Cpv. 1
Per poter richiedere l'iscrizione dei suoi dati nel registro di fiducia, un'autorità oppure un emittente o un verificatore privato deve essere iscritto nel registro di base. Il richiedente deve fornire la necessaria prova tecnica della sua iscrizione nel registro di base. La prova da fornire viene verificata tramite il portale con una procedura automatizzata.

Cpv. 2

Secondo l'articolo 3 capoverso 3 LIdE, un'autorità o un servizio che adempie compiti pubblici può presentare richiesta di conferma del suo identificativo. Oltre a fornire la prova tecnica di cui al capoverso 1, con la richiesta devono essere indicati l'IDI e i dati di contatto della persona responsabile dell'identificativo.

Cpv. 3 e 4

Secondo l'articolo 3 capoverso 4 LIdE, un emittente o verificatore privato (persona fisica o giuridica) può chiedere che il suo identificativo iscritto nel registro di base sia confermato dall'UFIT e iscritto nel registro di fiducia.

La richiesta di una persona fisica o giuridica è diversa dalla richiesta di un'autorità o di un servizio che adempie compiti pubblici. Una persona fisica deve disporre di un e-ID ed esibirlo. Una persona giuridica, oltre a fornire la prova tecnica di cui al capoverso 1, deve corredare la richiesta con una firma elettronica qualificata della persona o delle persone con diritto di firma ai sensi della legge del 18 marzo 2016[6] sulla firma elettronica (FiEle) nonché fornire le informazioni seguenti:

[6] RS **943.03**

- il numero IDI;
- i dati di contatto della persona giuridica;
- i dati di contatto della(e) persona(e) responsabile(i) dell'identificativo; e
- in caso di assenza di un'iscrizione nel registro svizzero di commercio, giustificativi come una copia del contratto di società o lo statuto, un estratto attuale autenticato del registro di commercio estero o un documento equivalente.

Art. 10 Verifica della richiesta

Cpv. 1 e 2

L'UFG verifica se la richiesta è completa e se le informazioni fornite sono corrette. Dopo aver verificato la richiesta e l'identità del richiedente ed essersi assicurato che il richiedente possa agire in nome della persona giuridica o della società di persone, l'UFG trasmette all'UFIT il risultato di tale verifica. L'UFIT conferma quindi le informazioni di cui all'articolo 8 capoverso 1, iscrive la conferma nel registro di fiducia e la rende accessibile.

Cpv. 3

Se nell'ambito della verifica di una richiesta l'UFG constata che è incompleta o erronea, ne informa il richiedente. Nel contempo gli concede un termine di 30 giorni per inoltrare i dati mancanti o correggere gli errori. Questa regola serve a rendere più efficiente la gestione e a garantire che il richiedente abbia abbastanza tempo per rimediare a eventuali lacune.

Se la richiesta non è completata o rettificata di conseguenza entro tale termine, la procedura di verifica è sospesa. Ciò significa che l'elaborazione della richiesta non è portata avanti e non viene effettuata alcuna iscrizione nel registro di fiducia.

Art. 11 Aggiornamento

Cpv. 1
Le modifiche necessitano di una nuova richiesta di iscrizione nel registro di fiducia e la loro correttezza e completezza deve essere verificata dall'UFG. L'emittente o il verificatore segnala tramite il portale (art. 2) ogni modifica delle sue informazioni di cui all'articolo 8 capoverso 1 lettere b-d. Tra queste rientrano in particolare il nome della persona fisica o giuridica iscritta nel registro di fiducia; eventuali informazioni sulle iscrizioni della persona giuridica in altri registri, come il registro di commercio, il registro d'identificazione delle imprese (registro IDI), il codice LEI (Legal Entity Identifier). La segnalazione si concentra sui dati pubblicati nel registro di fiducia che sono necessari per la conferma dell'identificativo. Non è necessario segnalare eventuali modifiche di altri dati raccolti nell'ambito della richiesta di iscrizione e non pubblicati nel registro di fiducia.

Se un'emittente o un verificatore iscritto nel registro di fiducia può fornire la prova tecnica del possesso dell'identificativo originariamente confermato, è possibile aggiungere, senza verifica del contenuto, altri identificativi, oltre a quello già confermato. In questo caso non sono dovuti emolumenti aggiuntivi.

Cpv. 2 e 6

Se l'iscrizione risale a più di cinque anni prima, l'UFG chiede all'emittente o al verificatore se le sue informazioni sono ancora attuali. Questa richiesta d'informazioni non equivale a un'ingiunzione di inoltrare le informazioni attuali per una nuova verifica da parte dell'UFG (cpv. 3). Tuttavia, il risultato della richiesta può portare a una procedura d'ingiunzione.

Viene avviata una procedura di ingiunzione se l'UFG ha motivo di ritenere che l'iscrizione non è più attuale e che l'emittente o il verificatore registrato non ha segnalato alcuna modifica delle informazioni secondo il capoverso 1. In questo caso, l'UFG ingiunge per scritto all'emittente o al verificatore di rettificare i dati necessari entro 30 giorni. L'ingiunzione deve essere scritta e di norma viene effettuata elettronicamente, deve essere brevemente motivata e devono essere elencate le azioni necessarie. L'emittente o il verificatore deve poter capire cosa deve fare e quali sono i motivi dell'ingiunzione.

L'UFG verifica i dati o i giustificativi presentati e trasmette all'UFIT il risultato della sua verifica affinché aggiorni la conferma. Se le condizioni per un aggiornamento sono adempiute, l'UFIT lo iscrive nel registro di fiducia.

Ai termini di conservazione dei dati cancellati dal registro di fiducia si applicano le disposizioni di cui all'articolo 7 capoverso 1.

Art. 12 Cancellazione su richiesta dell'emittente o del verificatore

Cpv. 1

Un'emittente o un verificatore può richiedere in qualsiasi momento la cancellazione della sua iscrizione dal registro di fiducia. Se viene richiesta la cancellazione, l'iscrizione viene rimossa. Se la cancellazione riguarda solo l'iscrizione nel registro di fiducia, l'emittente o il verificatore conserva il proprio identificativo iscritto nel registro di base. In questo caso, in caso di utilizzo di mezzi di autenticazione elettronici l'identità dell'emittente o del verificatore non può più essere confermata dall'UFIT. Per il titolare del mezzo di autenticazione elettronico non è più confermato che l'emittente o il verificatore è effettivamente chi dice di essere. Al posto della cancellazione può quindi chiedere che nel registro di fiducia sia confermato pubblicamente che un determinato identificativo gli era stato precedentemente assegnato ed era confermato fino alla disattivazione.

Come per la richiesta di cancellare un'iscrizione dal registro di base, l'emittente o il verificatore iscritto nel registro di fiducia deve dimostrare di essere il legittimo posses-

sore dell'iscrizione, in particolare mediante l'identificativo o la chiave crittografica privata necessaria (cfr. art. 5). Inoltre, l'UFG verifica se l'autorità, il servizio o il richiedente dispone del documento di identità necessario.

Cpv. 2

Se un emittente o un verificatore è oggetto da parte dell'UFG di un'ingiunzione secondo l'articolo 11 capoverso 3 di fornire giustificativi per l'aggiornamento della sua iscrizione e non vi dà seguito tempestivamente, l'UFG provvede affinché l'UFIT cancelli la conferma dell'identificativo dal registro di fiducia.

Cpv. 3

Il termine di conservazione per l'identificativo confermato cancellato dal registro di fiducia è retto dall'articolo 7 capoverso 1. Il termine di conservazione vale anche per eventuali modifiche dei dati del registro di fiducia (mutazioni verificate di iscrizioni nel registro di fiducia). Di conseguenza, di norma si applica un periodo di conservazione di dieci anni e, nella misura in cui ciò sia necessario per garantire l'utilizzo sicuro dei mezzi di autenticazione elettronici, la Confederazione può conservare i dati anche oltre tale termine decennale.

Art. 13 Iscrizione di altri dati da parte delle autorità

Oltre all'identificativo confermato e alla menzione di un sospetto di utilizzo inappropriato dell'infrastruttura di fiducia o di un mezzo di autenticazione elettronico secondo l'articolo 18, il registro di fiducia mette a disposizione degli utenti anche informazioni fornite da un'autorità o da un servizio che adempie compiti pubblici. Ciò include in particolare i dati che consentono di stabilire quali autorità o servizi pubblici sono autorizzati a rilasciare e verificare un determinato tipo di mezzo di autenticazione elettronico. L'autorità o il servizio che fornisce tali informazioni è responsabile della loro correttezza.

Le autorità o i servizi che adempiono compiti pubblici devono essere registrati nel registro di base per poter iscrivere autonomamente dati supplementari nel registro di fiducia. Su richiesta, l'UFG concede loro un accesso dedicato al sistema. Essi possono anche pubblicare autonomamente informazioni sui tipi di mezzi di autenticazione di cui sono responsabili. Queste includono, ad esempio, schemi tecnici che stabiliscono da quali campi di dati è composto un mezzo di autenticazione. Inoltre, è possibile definire quali attori, identificati in base ai loro identificativi, sono considerati emittenti e verificatori legittimi, indicando almeno gli identificativi delle autorità o dei servizi in questione e la denominazione del rispettivo mezzo di autenticazione elettronico.

Sezione 4: Applicazioni digitali

Art. 14 Requisiti dell'applicazione per la conservazione e la presentazione di mezzi di autenticazione elettronici

Cpv. 1

L'UFIT mette a disposizione un'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici (portafoglio elettronico statale). Deve provvedere affinché tale applicazione sia accessibile ai disabili (art. 28 cpv. 2 LIdE). Per garantire il corretto funzionamento dell'applicazione, l'utente deve utilizzare un dispositivo che soddisfi determinati requisiti basati sugli standard attualmente diffusi nel settore riguardo allo sviluppo di applicazioni mobili. Tra le altre cose occorre che il sistema operativo installato sul dispositivo sia ampiamente diffuso, sia ancora supportato dal fornitore del sistema e continui a ricevere aggiornamenti di sicurezza.

Cpv. 2

Se l'emittente o il verificatore non è iscritto nel registro di base o nel registro di fiducia (lett. a) e non utilizza l'applicazione messa a disposizione dalla Confederazione per la verifica dei mezzi di autenticazione elettronici (lett. b), all'utente potrebbe non essere chiaro con chi sta interagendo. La mancanza di registrazione aumenta i rischi per la protezione dei dati, poiché non è possibile identificare in modo univoco le parti coinvolte. Senza questa trasparenza, è difficile verificare se gli attori sono affidabili. Inoltre, non è possibile registrare informazioni di sicurezza, il che può potenzialmente portare ad abusi, all'accesso non autorizzato a dati personali o ad altre lacune di sicurezza.

In quanto provvedimento tecnico e organizzativo da adottare per garantire la protezione e la sicurezza dei dati nell'ambito dello scambio elettronico dei dati (art. 33 lett. e LIdE), prima di un possibile trasferimento di dati l'applicazione dell'utente segnala quindi che un emittente o un verificatore non è iscritto nel registro di base o nel registro di fiducia. Se un verificatore utilizza l'applicazione della Confederazione, invece, tale segnalazione non viene effettuata e all'utente viene comunicato che il verificatore utilizza l'applicazione ufficiale per la verifica dei mezzi di autenticazione elettronici secondo l'articolo 9 LIdE. In questo caso, l'impostazione predefinita dell'applicazione, conforme alla protezione dei dati, garantisce all'utente la trasmissione sicura dei dati.

Art. 15 Sistema per le copie di sicurezza

Dopo lo smarrimento o l'acquisto di un nuovo dispositivo (p. es. uno smartphone), in genere è normale ripristinare le applicazioni installate e i dati memorizzati a partire da un backup. In tal modo, si possono rapidamente ritrovare le funzionalità del vecchio sistema. Una possibilità analoga è offerta ai titolari del portafoglio elettronico statale. Ripristinare i mezzi di autenticazione elettronici non è possibile se, come nel caso dell'e-ID, è necessario un legame tramite processore crittografico al dispositivo mobile del titolare. Di conseguenza, tali mezzi di autenticazione elettronici devono nuovamente essere richiesti all'emittente.

Cpv. 1

La funzione di base dell'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici permette al titolare di generare e crittografare una copia di

sicurezza del contenuto (in particolare dei mezzi di autenticazione elettronici) del portafoglio elettronico. Il titolare può decidere liberamente dove conservare tale copia di sicurezza. Dopo aver cambiato dispositivo (smartphone, computer ecc.), i mezzi di autenticazione elettronici memorizzati possono essere ripristinati manualmente.

Il trasferimento e il ripristino di queste copie di sicurezza sono influenzati in modo decisivo dalle funzioni messe a disposizione dal sistema operativo del dispositivo. Inoltre, i titolari devono ricordare una password (p. es. crittografia con wordlist) necessaria per decrittare le copie di sicurezza. Se la password viene dimenticata o smarrita, non è possibile ripristinare i dati. Le password non sono note alla Confederazione.

Cpv. 2

L'UFIT mette a disposizione un sistema informatico in cui i titolari possono conservare le copie di sicurezza create sui loro dispositivi (art. 8 cpv. 2 LIdE). Il sistema non è accessibile a terzi. L'utilizzo del sistema per le copie di sicurezza è facoltativo ed è consentito solo agli utenti del portafoglio elettronico statale. Solo i titolari possono accedere al contenuto delle loro copie di sicurezza. In caso di inattività prolungata, se le copie di sicurezza non vengono aggiornate o scaricate, dopo tre anni i dati vengono cancellati.

Va tenuto presente che, dopo il caricamento dei dati da un backup, i mezzi di autenticazione non possono più essere validamente utilizzati se, come nel caso dell'e-ID, è previsto un legame con il titolare tramite un processore crittografico (cfr. art. 18 cpv. 2 LIdE). In questo caso, la prova del legame con il titolare è vincolata al dispositivo originariamente utilizzato al momento dell'emissione. In caso di smarrimento o sostituzione di tale dispositivo, è quindi necessaria una nuova emissione per poter utilizzare i pertinenti mezzi di autenticazione.

Art. 16 Verifica di altri mezzi di autenticazione elettronici mediante l'applicazione di cui all'articolo 9 LIdE

Cpv. 1 e 2

La presente disposizione attua la norma di delega prevista all'articolo 9 capoverso 2 LIdE per la verifica di altri mezzi di autenticazione elettronici con la check app della Confederazione. Oltre a verificare l'e-ID conformemente al capoverso 1, la check app della Confederazione serve a verificare la validità di altri mezzi di autenticazione elettronici. Lo scopo è di promuovere l'utilizzo dell'infrastruttura di fiducia e la diffusione dei mezzi di autenticazione elettronici.

L'utilizzo della check app della Confederazione per verificare i mezzi di autenticazione elettronici è facoltativo. I verificatori possono decidere liberamente se utilizzare l'applicazione della Confederazione o se ricorrere a una soluzione analoga.

Le autorità o i servizi che adempiono compiti pubblici, nonché gli emittenti privati possono chiedere all'UFG che i loro mezzi di autenticazione elettronici siano verificabili con la check app della Confederazione. La condizione è che i mezzi di autenticazione

adempiano i requisiti tecnici (formati, standard e protocolli) e che l'emittente sia iscritto nel registro di fiducia.

Cpv. 3

Affinché un mezzo di autenticazione elettronico possa essere verificato mediante la check app della Confederazione, oltre alle condizioni di cui al capoverso 2, deve essere garantito che non vi si oppongano interessi pubblici, in particolare per quanto riguarda la sicurezza o la protezione dei dati. È inoltre necessario che il mezzo di autenticazione elettronico sia ampiamente diffuso nella pratica e generalmente accettato.

La check app della Confederazione è prevista principalmente per la verifica dell'e-ID. La sua estensione ad altri mezzi di autenticazione elettronici necessita di un onere tecnico e organizzativo supplementare nonché di corrispondenti risorse. Per garantire che tali estensioni siano utili per gli interessi pubblici e restino proporzionate all'onere, con l'applicazione della Confederazione devono poter essere verificati mezzi di autenticazione di rilevanza sociale superiore.

Cpv. 4

Se desidera che la check app della Confederazione possa verificare i suoi mezzi di autenticazione elettronici, un emittente deve presentare una richiesta all'UFG. L'adeguamento della check app della Confederazione è gratuito. Se un mezzo di autenticazione elettronico dell'emittente adempie tutte le condizioni per essere integrato nella check app della Confederazione, l'UFG decide di estendere l'applicazione e informa l'UFIT di adottare i provvedimenti necessari.

Sezione 5: Utilizzo inappropriato dell'infrastruttura di fiducia e dei mezzi di autenticazione elettronici

Art. 17 Procedura di verifica

Cpv. 1 e 2

Se viene a conoscenza di un utilizzo inappropriato dell'infrastruttura di fiducia o di un mezzo di autenticazione elettronico, ad esempio da parte di un titolare di un mezzo di autenticazione elettronico, di un emittente o di un verificatore, l'UFG esegue una procedura di verifica che serve a proteggere e salvaguardare l'integrità del sistema in cui vengono utilizzati i mezzi di autenticazione elettronici. La possibilità di compiere una segnalazione di cui dispongono gli utenti collegati al sistema garantisce che le lacune di sicurezza possano essere rapidamente individuate e affrontate riducendo al minimo i rischi per la sicurezza e la protezione dei dati. Il progetto di ordinanza precisa quando sussiste un utilizzo inappropriato:

a. Un requisito importante per un utilizzo sicuro dei mezzi di autenticazione elettronici è che l'emittente o il verificatore utilizzi i suoi dati ufficiali. Non vengono ad esempio utilizzati dati ufficiali quando una persona iscritta nel registro di fiducia

utilizza un'identità che non corrisponde alla sua identità effettiva o se nelle relazioni d'affari si presenta come un'altra persona. Quest'ultimo caso vale anche per un emittente o un verificatore iscritto esclusivamente nel registro di base.

L'identità ufficiale delle persone fisiche, analogamente al contenuto dell'e-ID di cui all'articolo 15 capoverso 3 LIdE, può includere anche dati aggiuntivi, come il cognome d'affinità, il nome ricevuto in un ordine religioso, il nome d'arte o il nome dell'unione domestica registrata nonché la menzione di segni particolari. In determinati casi, tali informazioni possono essere utili o addirittura necessarie per le transazioni commerciali. Possono quindi costituire parte dell'identità se sono indicate anche nella carta d'identità, in un altro documento d'identità o nella carta di legittimazione del titolare e sono state utilizzate nella procedura di richiesta secondo l'articolo 9. Quest'ultimo caso riguarda anche le persone giuridiche la cui identità può essere nota in particolare per un determinato prodotto di marca o un determinato servizio.

b. Un mezzo di autenticazione non deve avere contenuti illeciti o servire a uno scopo illecito.

c. Se un mezzo di autenticazione elettronico contiene dati personali degni di particolare protezione, come ad esempio dati relativi alla salute o informazioni sulle convinzioni religiose, il titolare di tale mezzo di autenticazione deve esserne informato per iscritto. Questa informazione deve chiarire che i dati contenuti sono particolarmente sensibili e sono quindi oggetto di una maggiore protezione. In questo modo si garantisce che l'interessato sia consapevole della sensibilità dei suoi dati e, se del caso, possa dare il suo consenso al trattamento. La comunicazione scritta serve quindi a informare il titolare dell'importanza e della protezione di questi dati prima di una specifica elaborazione. Il portafoglio elettronico della Confederazione supporta un formato di dati che consente agli emittenti di segnalare le informazioni sensibili direttamente nell'applicazione. Quando viene richiesto un determinato campo di dati, gli utenti ne sono esplicitamente avvertiti prima della trasmissione.

d. Per utilizzare in modo sicuro i mezzi di autenticazione elettronici, la loro verifica deve rispettare i principi fondamentali della protezione dei dati. Ciò significa in particolare che la raccolta di dati personali non deve essere sproporzionata. I dati possono quindi essere raccolti solo per uno scopo chiaramente definito e comprensibile per la persona interessata. Non è quindi ammesso utilizzare i dati per scopi diversi da quelli definiti in precedenza. Non appena i dati non sono più necessari per lo scopo perseguito, devono essere distrutti o anonimizzati. Questa procedura protegge la sfera privata delle persone interessate e garantisce che il trattamento dei loro dati sia sempre conforme alle norme sulla protezione dei dati.

Cpv. 3 e 4

Per verificare un sospetto, l'UFG può adottare diverse misure. Ad esempio, può verificare i dati raccolti tramite il portale per il trattamento dei dati dei registri di cui all'articolo 2, nonché i dati provenienti dal registro di base e dal registro di fiducia. Inoltre, può ad esempio, ricevere informazioni tecniche sui dati trasmessi o richiederle successivamente per garantire che i dati siano stati elaborati in modo corretto e sicuro. Può anche indagare sull'origine del mezzo di autenticazione elettronico per individuare eventuali lacune di sicurezza o irregolarità. Ha inoltre la possibilità di contattare direttamente il titolare del mezzo di autenticazione in questione e il suo emittente o verificatore. In questo ambito, l'UFG può chiarire i fatti richiedendo ulteriori informazioni sulla transazione in questione.

L'UFG può verificare un utilizzo inappropriato soltanto se viene utilizzato un identificativo univoco. In caso di sospetto di gravi violazioni della protezione dei dati, l'UFG informa l'Incaricato federale della protezione dei dati e della trasparenza o il servizio cantonale competente del relativo utilizzo inappropriato.

Art. 18 Menzione dell'utilizzo inappropriato

Se, dopo una verifica secondo l'articolo 17 capoverso 3, constata un utilizzo inappropriato dell'infrastruttura di fiducia o dei mezzi di autenticazione elettronici, l'UFG comunica il risultato della verifica all'UFIT. Quest'ultimo registra il risultato nel registro di fiducia e lo rende visibile al massimo per sei mesi. L'UFG informa immediatamente l'emittente o il verificatore interessato purché ciò sia possibile con un onere adeguato. L'iscrizione serve a garantire trasparenza e fiducia e a permettere agli utenti di decidere in modo informato se desiderano utilizzare il mezzo di autenticazione elettronico in un determinato contesto. Ciò contribuisce ad aumentare la sicurezza complessiva del sistema riguardante i mezzi di autenticazione elettronici e a garantire la correttezza delle informazioni contenute nel registro di fiducia. La visibilità di una menzione nel registro di fiducia cessa al più tardi alla scadenza del termine di cui al capoverso 3.

La visibilità di una menzione può essere prolungata. Dopo la scadenza del termine o se riceve nuove segnalazioni, l'UFG verifica se continua a esservi un utilizzo inappropriato. Se tale è il caso, l'iscrizione resta visibile per un ulteriore periodo di tempo per continuare a garantire un utilizzo sicuro dei mezzi di autenticazione elettronici. Nei casi manifesti questo prolungamento garantisce che gli utenti dispongano di informazioni aggiornate sull'utilizzo inappropriato dell'infrastruttura di fiducia o del mezzo di autenticazione elettronico e possano quindi prendere decisioni informate senza che sia necessaria una segnalazione. La trasparenza e il rapporto di fiducia contribuiscono a garantire il costante rispetto dei requisiti legali necessari per mantenere la fiducia nell'infrastruttura di fiducia e nell'utilizzo dei mezzi di autenticazione elettronici.

Vi è un palese e continuo utilizzo inappropriato, ad esempio se un emittente o un verificatore si finge una persona che non è, se un emittente emette mezzi di autenticazione elettronici con contenuti illeciti o per scopi illeciti, o se un emittente o un verificatore è stato identificato come programma automatizzato (bot). Se il prolungamento è dovuto

a motivi palesi, l'UFG può prevedere che l'iscrizione sia pubblicata a tempo indeterminato.

Art. 19 Cancellazione della menzione

L'UFIT cancella la menzione dal registro di fiducia dopo la scadenza della durata stabilita. I dati collegati alla menzione così come le informazioni iscritte dall'UFIT nel quadro della procedura di verifica, sono conservati dieci anni dalla Confederazione e non sono pubblicamente accessibili. La Confederazione può conservare l'iscrizione cancellata anche dopo i dieci anni se ciò è necessario per l'utilizzo sicuro dell'infrastruttura di fiducia o dei mezzi di autenticazione elettronici.

Capitolo 3: Id-e

Sezione 1: Richiesta

Art. 20 Condizioni generali

Cpv. 1

Chi desidera ottenere un e-ID deve utilizzare un dispositivo che garantisca il legame secondo l'articolo 18 capoverso 2 LIdE e deve installare sul suo dispositivo un'applicazione secondo l'articolo 8 capoverso 1 LIdE o un'altra applicazione secondo l'articolo 18 capoversi 4 o 5 LIdE nella quale sarà emesso l'e-ID. Il proprietario del dispositivo può conservare il suo e-ID e quello di un terzo, ad esempio di un minore o di una persona sotto curatela di cui è rappresentante legale.

L'articolo 18 capoverso 4 LIdE amplia le possibilità di garantire anche altre soluzioni per garantire il legame con il titolare. La disposizione è volutamente formulata in modo neutro dal punto di vista tecnologico al fine di consentire diverse soluzioni. In linea di principio, tuttavia, sono necessarie una garanzia automatizzata e una prova tecnica per dimostrare, ad esempio, che la coppia di chiavi crittografiche utilizzata per il legame con il titolare proviene da un processore crittografico hardware dedicato.

Cpv. 2 e 3

La richiesta deve essere presentata dal futuro titolare dell'e-ID. Se è minorenne o sotto curatela generale, l'interessato deve presentare il consenso del suo rappresentante legale. Quest'ultimo può dare il proprio consenso direttamente nel processo online con il proprio e-ID se ne possiede uno. In caso contrario, deve consegnare il consenso firmato alla persona minorenne o sotto curatela, oppure accompagnarla presso un centro di registrazione, un ufficio della migrazione o una rappresentanza svizzera all'estero per verificare la sua identità. Per il richiedente minorenne, in caso di autorità parentale congiunta, è sufficiente il consenso di uno dei genitori.

Art. 21 Requisiti riguardo all'immagine del viso

La verifica dell'identità mediante riconoscimento facciale automatizzato può essere effettuata solo se nei sistemi d'informazione di cui all'articolo 17 capoverso 2 LIdE vi è una fotografia del richiedente. Inoltre, tale fotografia deve essere di qualità sufficiente e conforme agli standard della Convenzione del 7 dicembre 1944[7] relativa all'aviazione civile internazionale. Infine, deve essere salvata e poter essere consultata in formato elettronico.

Art. 22 Presentazione della richiesta

Il richiedente deve inoltrare la richiesta tramite l'applicazione per la conservazione e la presentazione di mezzi di autenticazione elettronici secondo l'articolo 8 LIdE (portafoglio elettronico statale).

Art. 23 Verifica dell'identità tramite l'applicazione di cui all'articolo 8 LIdE

Cpv. 1

Il richiedente può far verificare la sua identità tramite l'applicazione per la conservazione e la presentazione di mezzi di autenticazione elettronici se la sua identità è stata verificata in presenza almeno una volta, vale a dire al momento della prima emissione dell'e-ID o nell'ambito del rilascio di un documento d'identità di cui all'articolo 14 lettera a LIdE (carta d'identità, passaporto, carta di soggiorno per stranieri o carta di legittimazione).

Se il richiedente è in possesso di una carta di legittimazione valida secondo l'articolo 17 capoverso 1 dell'ordinanza del 7 dicembre 2007[8] sullo Stato ospite (OSOsp) in combinato disposto con l'articolo 71*a* capoverso 1 dell'ordinanza sull'ammissione, il soggiorno e l'attività lucrativa (OASA), la verifica dell'identità in presenza viene effettuata presso un ufficio dei passaporti o un ufficio della migrazione designato dal Dipartimento federale degli affari esteri (DFAE).

Cpv. 2

Per far verificare la sua identità online, il richiedente scansiona la zona di lettura ottica (MRZ) o il chip del suo documento d'identità ufficiale (carta d'identità, passaporto o carta di soggiorno per stranieri), quindi riprende il suo volto (Liveness-Check). Il risultato della scansione e/o della lettura del chip, nonché la sua immagine del viso (sotto

[7] RS **0.748.0**

[8] RS **192.121**

forma di sequenze video) sono poi trasmessi tramite l'applicazione a fedpol, che esaminerà direttamente la richiesta.

Cpv. 3

Per verificare i dati trasmessi dal richiedente, fedpol utilizza una parte del sistema d'informazione per l'emissione e la revoca dell'e-ID di cui all'articolo 26 capoverso 1 LIdE. Questo sistema consente di confrontare automaticamente le informazioni trasmesse, in particolare l'immagine del viso, con quelle contenute nei sistemi d'informazione a cui fedpol ha accesso in virtù dell'articolo 26 capoverso 3 LIdE. Fedpol può intervenire nel processo di confronto delle immagini del viso a fini del controllo della qualità.

Art. 24 Verifica dell'identità in presenza

Il richiedente che, al posto della verifica dell'identità tramite l'applicazione per conservare e presentare mezzi di autenticazione elettronici, auspica una verifica dell'identità in presenza, deve fissare un appuntamento a tal fine. Per i servizi forniti in presenza possono essere riscossi emolumenti

Il servizio cantonale competente o la rappresentanza consolare svizzera all'estero verifica l'identità del richiedente sulla base del documento d'identità da lui presentato, del suo viso e delle informazioni contenute nei sistemi d'informazione di cui all'articolo 17 capoverso 2 LIdE. Il confronto dell'immagine del viso può essere eseguito automaticamente. A tal fine può essere utilizzata la stazione di registrazione dei dati biometrici (verifica automatizzata). In questo caso, il richiedente deve essere informato che la sua identità è verificata mediante la stazione di registrazione. Questo dispositivo fornisce una valutazione che aiuta a decidere, ma la decisione finale spetta comunque al collaboratore specializzato. Durante la verifica dell'identità in presenza, nel sistema non viene registrato né conservato alcun dato. Il risultato della verifica è trasmesso in via elettronica a fedpol mediante il sistema d'informazione per l'emissione e la revoca dell'e-ID.

Chi desidera ottenere un e-ID può richiederlo insieme a una carta d'identità o un passaporto secondo l'articolo 14 lettera a numero 1 LIdE (variante *Documenti+*). In caso di richiesta di emissione congiunta, la verifica dell'identità del richiedente viene effettuata nell'ambito dell'emissione di uno dei documenti d'identità di cui all'articolo 14 lettera a numero 1 LIdE. La possibilità di richiedere un e-ID insieme al passaporto e/o alla carta d'identità costituisce un servizio supplementare. Poiché la verifica dell'identità è appena stata effettuata, in questo caso non è prevista alcuna verifica supplementare per convalidare l'emissione dell'e-ID. Una volta completata la procedura di verifica dell'identità, l'emissione dell'e-ID può essere effettuata prima della ricezione del documento d'identità.

Gli Svizzeri all'estero secondo la legge del 26 settembre 2014[9] sugli Svizzeri all'estero (LSEst) possono far verificare la loro identità presso la competente rappresentanza consolare svizzera.

Art. 25 Decisione automatizzata

Quando installa l'applicazione, il richiedente è informato in merito al trattamento automatizzato dei suoi dati personali, conformemente all'articolo 21 della legge del 25 settembre 2020[10] sulla protezione dei dati (LPD). Per proseguire la procedura, il richiedente deve espressamente consentire al fatto che la decisione è presa in modo automatizzato. Su richiesta del servizio di supporto tecnico di fedpol o per ragioni di controllo della qualità, la decisione automatizzata può essere verificata da un collaboratore specializzato incaricato della verifica dell'identità.

L'articolo 21 capoverso 1 LPD prevede che il titolare del trattamento informa la persona interessata di ogni decisione basata esclusivamente su un trattamento di dati personali automatizzato che abbia per lei effetti giuridici o conseguenze significative (decisione individuale automatizzata). Secondo l'articolo 21 capoverso 2 LPD, il titolare del trattamento dà su richiesta alla persona interessata la possibilità di esprimere un parere.

Art. 26 Richiesta dell'Id-e all'estero

Se l'applicazione di cui all'articolo 8 capoverso 1 LIdE o l'applicazione di cui all'articolo 18 capoverso 4 o 5 LIdE non può essere installata all'estero, in particolare a causa di un blocco geografico, l'e-ID non può essere richiesto.

Sezione 2: Emissione e revoca

L'e-ID statale sotto forma di mezzo d'identificazione elettronico per le persone fisiche è emesso esclusivamente da fedpol tramite l'infrastruttura di fiducia statale. L'e-ID consente di provare la propria identità nel mondo virtuale, il che è necessario per determinate operazioni online, ad esempio la richiesta di un estratto del casellario giudiziale o l'ottenimento da un fornitore certificato di una firma elettronica con la quale firmare in modo giuridicamente valido. L'e-ID è paragonabile alla carta d'identità o al passaporto nel mondo fisico, ma non li sostituisce. Tutti i cittadini devono poter decidere liberamente se utilizzare un e-ID, una carta d'identità fisica o un passaporto.

Nella maggior parte dei casi, fedpol potrà eseguire i compiti necessari per l'emissione dell'e-ID in modo automatizzato. In caso di dubbi da parte di fedpol o di incertezze del

[9] RS **195.1**

[10] SR **235.1**

sistema automatico, fedpol può intervenire e riesaminare i dati generati durante il riconoscimento facciale. Fedpol decide quando la decisione automatizzata deve essere riesaminata da un'istanza di controllo.

Art. 27 Emissione

Cpv. 1

Con la stessa richiesta è possibile ottenere l'e-ID in diverse applicazioni, su uno o più dispositivi (in un massimo di dieci portafogli elettronici). L'emissione simultanea si prefigge di prevenire un utilizzo abusivo dell'e-ID.

Cpv. 2

I seguenti dati relativi alla procedura di emissione sono registrati nel sistema d'informazione per l'emissione e la revoca dell'e-ID:

a. i valori delle verifiche automatiche dell'identità tramite l'applicazione di cui all'articolo 8 LIdE;

b. il numero d'identificazione della persona che compie la verifica e le decisioni che ha preso;

c. il nome, il cognome e il numero e-ID del rappresentante legale;

d. le informazioni sul legame tra l'e-ID e il titolare;

e. i numeri delle versioni delle parti o dell'intero sistema d'informazione per l'emissione e la revoca dell'e-ID;

f. la data di inizio e di fine della procedura di emissione;

g. il parametro tecnico sull'e-ID (p. es. codice risultante dall'hash crittografico o valore hash).

Questi dati, compresi i dati biometrici di cui all'articolo 17 capoverso 4 LIdE, necessari per le inchieste concernenti il conseguimento fraudolento o l'utilizzo inappropriato di un e-ID e conservati unicamente a tal fine sono distrutti cinque anni dopo la scadenza dell'e-ID conformemente all'articolo 27 capoverso 1 lettera b LIdE.

Cpv. 3

L'ordinanza dipartimentale disciplinerà in particolare il formato tecnico e gli attributi per la trasmissione dei dati, i requisiti dell'interfaccia con il sistema d'informazione per

l’emissione e la revoca degli e-ID nonché gli standard e i protocolli per la comunicazione dei dati nell’ambito dell’emissione dell’e-ID. Attualmente lo sviluppo dei requisiti, documentati su GitHub, è ancora in corso.

Art. 28 Durata di validità

Cpv. 1 e 2

La durata di validità dell’e-ID è basata sulla data di emissione: l’e-ID è valido dal momento dell’emissione da parte di fedpol. Se per la stessa richiesta sono emessi più e-ID, fa fede la data di emissione del primo e-ID.

Se insieme all’e-ID la persona richiede anche uno dei documenti di cui all’articolo 14 lettera a numero 1 LIdE, la durata di validità dell’e-ID è calcolata a partire dalla data di emissione dell’e-ID e non da quella di emissione del documento in questione.

L’e-ID è valido al massimo quanto il documento presentato in occasione della richiesta.

Cpv. 3

Per motivi di sicurezza dell’informazione, il DFGP può fissare una durata di validità inferiore. La durata di validità dell’e-ID non deve eccedere quella del documento utilizzato in occasione della procedura di emissione.

Art. 29 Richiesta di revoca

Cpv. 1

Fedpol può revocare l’e-ID su richiesta del titolare o del rappresentante legale di un minorenne o di una persona sotto curatela generale. Un minorenne o una persona sotto curatela generale può chiedere la revoca del suo e-ID senza dover ottenere l’autorizzazione del suo rappresentante legale.

Cpv. 2 e 3

Per ogni richiesta di revoca presso fedpol, il titolare dell’e-ID o il rappresentante legale di un minorenne o di una persona sotto curatela generale deve dimostrare la propria identità con un documento d’identità valido o, se è (ancora) in possesso dell’e-ID, con quest’ultimo.

Se la revoca dell’e-ID è chiesta da un rappresentante legale, quest’ultimo deve pure provare l’identità del minorenne o della persona sotto curatela generale nonché il suo diritto di rappresentanza.

Cpv. 4

In caso di perdita del dispositivo, il titolare o il rappresentante legale può segnalare la perdita alla competente autorità di polizia o alla rappresentanza consolare. Essa informa fedpol, che revoca immediatamente l'e-ID.

Art. 30 Procedura in caso di sospetto di conseguimento fraudolento o utilizzo abusivo o di rischio per la sicurezza

Se vi è il sospetto di conseguimento fraudolento o utilizzo abusivo dell'e-ID o se la sicurezza dell'e-ID è a rischio, fedpol può eseguire una procedura di verifica. Può in particolare far nuovamente verificare l'identità del titolare, analizzare i dati biometrici raccolti nella procedura di emissione e sentire il titolare, le persone interessate o terzi.

Fedpol può revocare d'ufficio un e-ID. La revoca è automatica e verbalizzata. È menzionata nel registro di base. Consultando l'elenco delle revoche, il verificatore potrà constatare che l'e-ID in questione non è più valido.

Art. 31 Gestione del sistema d'informazione per l'emissione e la revoca degli Id-e

Cpv. 1 e 2

Fedpol consulta ogni giorno in maniera automatizzata i sistemi di informazione di cui all'articolo 26 capoverso 3 LIdE. Il DFGP disciplina le interfacce e il funzionamento del sistema d'informazione per l'emissione e la revoca degli e-ID.

Capitolo 4: Accesso alle applicazioni da parte dei disabili

Art. 32

L'UFIT deve garantire che l'applicazione per la presentazione e la conservazione dei mezzi di autenticazione elettronici nonché l'applicazione per la loro verifica siano accessibili anche ai disabili. Anche fedpol deve adottare le misure necessarie affinché sia garantito l'accesso alle applicazioni utilizzate nella procedura di ottenimento dell'e-ID o per la sua revoca, quindi ad esempio alle interfacce utente per l'inserimento dei dati nonché a singole parti della procedura di emissione. L'UFIT e fedpol devono in particolare garantire l'accesso alle applicazioni in caso di aggiornamenti importanti dei sistemi, i cosiddetti «release». Queste misure contribuiscono a promuovere l'inclusione digitale e a garantire l'accesso a servizi importanti per tutte le persone.

Capitolo 5: Formato dei mezzi di autenticazione elettronici nonché standard e protocolli per la procedura di comunicazione dei dati

Art. 33 Pubblicazione dei formati e degli standard e protocolli

Cpv. 1

Questa normativa si prefigge di creare una base affidabile e interoperabile per utilizzare in modo sicuro i mezzi di autenticazione elettronici e per verificarli in modo affidabile.

I mezzi di autenticazione elettronici in questo ambito possono ad esempio essere documenti digitali, certificati o altre forme di mezzi di autenticazione trasmessi in un formato elettronico a prova di falsificazione. Al fine di garantire che tali mezzi di autenticazione siano giuridicamente certi e chiaramente comprensibili in contesti diversi, che si tratti della comunicazione con le autorità, della trasmissione di certificati o della verifica, è necessario stabilire condizioni quadro tecniche standardizzate. Ciò include in particolare la definizione di formati, come i formati dei documenti o i formati strutturati dei dati, nonché di standard e protocolli che garantiscono la trasmissione sicura di tali dati. Gli standard e i protocolli comprendono principalmente le raccomandazioni tecniche e organizzative volte a garantire l'integrità e l'autenticità dei mezzi di autenticazione elettronici nonché l'interoperabilità tra gli attori collegati al sistema.

L'UFG è responsabile della creazione e della manutenzione del quadro sicuro e interoperabile che consente di utilizzare i mezzi di autenticazione elettronici nell'infrastruttura di fiducia.

Cpv. 2

L'UFG deve pubblicare i formati, gli standard e i protocolli sotto forma di raccomandazioni (best practice) sulla pagina web della Confederazione. Può anche rinviare a siti web che gestisce, come in particolare GitHub. Le best practice contengono spiegazioni dettagliate su come creare, controllare e utilizzare i mezzi di autenticazione elettronici in modo sicuro ed efficiente. La pubblicazione sotto forma di best practice garantisce che tutti gli attori possano seguire gli stessi standard senza limitare gli sviluppi o le innovazioni individuali. Le best practice mirano quindi a promuovere un sistema sicuro e interoperabile per utilizzare e verificare i mezzi di autenticazione elettronici, rafforzare la fiducia nell'infrastruttura digitale e consentirne un uso ampio e semplice.

Art. 34 Adeguamento delle raccomandazioni

Cpv. 1 e 2

La pubblicazione di raccomandazioni secondo l'articolo 33 (best practice) garantisce che i formati e gli standard possano essere costantemente adattati dall'UFG agli sviluppi tecnici e ai requisiti legali. Ciò consente anche agli attori privati di beneficiare delle ultime innovazioni tecnologiche e giuridiche e di mantenere aggiornati i propri sistemi.

Per adeguare le best practice l'UFG può ricorrere a esperti interni ed esterni, nonché a comitati tecnici specializzati e a organizzazioni di standardizzazione.

Cpv. 3

Anche le modifiche delle best practice devono essere pubblicate. Per la pubblicazione vale quanto previsto nell'articolo 33 capoverso 2.

Art. 35 Formati, standard e protocolli vincolanti

Cpv. 1

Il DFGP può dichiarare vincolanti, in un'ordinanza dipartimentale, formati specifici per mezzi di autenticazione elettronici nonché standard e protocolli per la pubblicazione dei dati per i partecipanti al sistema dell'infrastruttura di fiducia, in particolare gli emittenti e i verificatori di mezzi di autenticazione elettronici nonché i fornitori di applicazioni secondo l'articolo 18 capoversi 4 e 5 LIdE. È il caso, ad esempio, se gli attuali formati e standard non garantiscono la necessaria interoperabilità tra diversi sistemi e attori. Se l'interoperabilità manca, i dati non possono essere scambiati in modo efficiente e senza errori tra i servizi interessati. I formati, gli standard e i protocolli vincolanti valgono in ogni caso anche per l'applicazione della Confederazione per la conservazione e la presentazione di mezzi di autenticazione elettronici secondo l'articolo 8 capoverso 1 LIdE.

Un'altra ragione per dichiarare vincolanti formati, standard e protocolli è la necessità di sostituire versioni obsolete con nuove versioni più sicure ed efficienti. Inoltre, una tale dichiarazione serve a far progredire un eventuale processo di standardizzazione e ad accelerare la messa in atto dei progressi tecnici. Senza una normativa vincolante, l'utilizzo di troppe soluzioni diverse potrebbe frammentare il sistema e lederne l'efficacia.

Cpv. 2

Prima di dichiarare vincolante un formato, uno standard o un protocollo, il DFGP consulta tutti gli attori e i gruppi di interesse rilevanti. Si garantisce così che le norme proposte possano essere attuate nella pratica e siano accettate dalle parti interessate. L'obiettivo di questa consultazione è di verificare la praticabilità delle modifiche previste e di identificare tempestivamente potenziali sfide.

Queste consultazioni offrono anche una possibilità per promuovere un processo di standardizzazione e un'unificazione congiunti e consolidati nell'ecosistema svizzero. Il coinvolgimento delle cerchie interessate garantisce un'ampia accettazione e un'attuazione per quanto possibile agevole. Inoltre, promuove l'uso consolidato e uniforme degli standard.

Cpv. 3

Se il DFGP dichiara vincolante un formato, uno standard o un protocollo, la normativa entra in vigore al più presto tre mesi dopo tale dichiarazione. Questo termine consente alle parti interessate di prepararsi alle nuove regole e quindi di adattare i loro sistemi e processi per soddisfare i requisiti.

Tuttavia, a seconda della portata e della complessità delle modifiche, il DFGP può anche prevedere un termine più lungo se il carattere vincolante richiede un intervento importante sui sistemi o le infrastrutture esistenti. Può ad esempio essere necessario un termine transitorio di più mesi o addirittura anni per consentire un adattamento e un'implementazione completi. Soprattutto quando vengono introdotte nuove tecnologie o formati più sicuri, è importante dare agli attori interessati il tempo necessario per aggiornare i sistemi esistenti e garantire che restino continuamente compatibili. Questi termini di transizione flessibili permettono di eseguire il processo di transizione senza inutili disagi o ritardi.

In casi urgenti di minaccia immediata del funzionamento dei mezzi di autenticazione elettronici o dell'infrastruttura di fiducia, l'UFIT può effettuare immediatamente le modifiche necessarie. A tal fine si basa sulla legge federale del 18 dicembre 2020[11] sulla sicurezza delle informazioni (LSIn). Tali misure urgenti sono particolarmente importanti in caso di minacce, vulnerabilità e lacune nella sicurezza che potrebbero mettere in discussione l'integrità o la confidenzialità dei dati. In questi casi, può essere necessario agire rapidamente per evitare danni gravi o lacune nella sicurezza ma non è necessario dichiarare vincolanti determinati formati, standard o protocolli.

Art. 36 Menzione del mancato rispetto di formati, standard e protocolli nel registro di fiducia

Indipendentemente dal sospetto di utilizzo inappropriato dell'infrastruttura di fiducia o di mezzi di autenticazione elettronici, può essere apportata una menzione nel registro di fiducia, se l'UFG constata che i formati, gli standard o i protocolli non sono rispettati. In un caso simile l'UFG può eseguire una procedura di verifica per valutare la conformità tecnica e giuridica. Se viene constatato un inadempimento, nel registro di fiducia viene inserita una menzione per gli emittenti e i verificatori conformemente all'articolo 18 e la cancellazione secondo l'articolo 19. Altrettanto vale per i fornitori di portafogli elettronici di terzi secondo l'articolo 18 capoversi 4 e 5 LIdE.

Capitolo 6: Emolumenti

Art. 37 Emolumenti concernenti il registro

Con l'entrata in vigore della LIdE, sotto i profili tecnico e operativo sarà possibile fornire rapidamente agli abitanti della Svizzera e agli Svizzeri all'estero un e-ID e altri mezzi di autenticazione elettronici di elevata qualità (p. es. estratto del casellario giudiziale, licenza di condurre digitale, in ambito sanitario o nel contesto dei diritti politici).

I costi complessivi per l'infrastruttura di fiducia sono stimati a circa 20,8 milioni di franchi all'anno, dei quali circa il 50 per cento consiste in costi d'esercizio per l'infrastruttura di fiducia. I costi d'esercizio comprendono i costi per l'iscrizione nel registro di base, i costi per la verifica delle richieste di iscrizione e di aggiornamento dei dati nel registro di

[11] RS **128**

fiducia e i rimanenti costi per la gestione dell'infrastruttura di fiducia. Poiché per quanto riguarda l'utilizzo dell'infrastruttura si devono formulare ipotesi, dopo la messa in esercizio l'importo degli emolumenti sarà regolarmente verificato.

Gli emolumenti dipendono dai costi annuali dell'infrastruttura di fiducia, che sono costituiti dalle uscite del servizio specializzato e-ID dell'UFG e dell'UFIT, ossia i costi diretti per il personale del servizio specializzato, i costi generali, i costi dei posti di lavoro, le spese per beni e servizi e le spese d'esercizio dell'UFIT, i costi delle licenze e gli ammortamenti.

Costi annuali dell'infrastruttura di fiducia di cui è tenuto conto nel calcolo degli emolumenti:	
Costi diretti del personale	CHF 3,96 mio.
Costi generali (art. 4 cpv. 2 lett. c OgeEm) (20 %)	CHF 0,79 mio.
Costi dei posti di lavoro (art. 4 cpv. 2 lett. b OgeEm (22 posti di lavoro); importo secondo tabella AFF 2025	CHF 0,31 mio.
Spese per beni e servizi e spese d'esercizio dell'UFIT	CHF 3,0 mio.
Costi delle licenze	CHF 0,1 mio.
Ammortamenti contabili sugli impianti (infrastruttura di fiducia)	CHF 2,67 mio.
Totale	**CHF 10,83 mio.**

Da questi costi occorre distinguere rimanenti costi pari a 9,93 milioni di franchi di cui non è tenuto conto nel calcolo degli emolumenti, in considerazione dell'interesse pubblico all'esercizio dell'infrastruttura di fiducia. La Confederazione ha interesse a sviluppare e gestire un sistema informatico e di comunicazione moderno a vantaggio della popolazione e dell'economia.

Cpv. 1

Si stima che **un terzo** dei costi dell'infrastruttura di fiducia coperti dagli emolumenti sia destinato al registro di base, il che corrisponde a 3,61 milioni di franchi. A beneficiare in primo luogo dell'infrastruttura di fiducia e dell'utilizzo di mezzi di autenticazione elettronici come l'e-ID sono in particolare le autorità. Sono previsti anche ulteriori impieghi dell'infrastruttura, in particolare per la licenza di condurre digitale, nel settore sanitario e nel contesto dei diritti politici. Ciò riguarda sia le autorità federali sia i servizi cantonali. In primo luogo, sono quindi le autorità ad approfittare dell'infrastruttura di fiducia e dell'utilizzo di mezzi di autenticazione elettronici come l'e-ID. Viste queste premesse si prevede che circa il 60 per cento dei costi totali per il registro di base, ovvero circa 2,17 milioni di franchi, sarà generato dall'esercizio connesso con l'utilizzo da parte delle autorità. Tuttavia, secondo la LIdE per le autorità non sono riscossi emolumenti ma la

loro quota di costi deve essere presa in considerazione nel calcolo degli emolumenti. Il restante 40 per cento dei costi (1,44 mio. fr.) è a carico dell'economia privata. Per tale utilizzo viene calcolato un emolumento che risulta dai rimanenti costi di 1,44 milioni di franchi per il registro di base e dal numero di iscrizioni previste.

Nel fissare l'emolumento, per quanto possibile, si tiene conto dei possibili sviluppi futuri e di un orizzonte temporale più lungo per la pianificazione. Sulla base di tale orizzonte temporale, si prevede che le iscrizioni annuali nel registro di base corrisponderanno in media al 20 per cento delle nuove iscrizioni complessive nel registro di commercio cantonale[12]. Tale previsione si basa su un'attenta stima delle iscrizioni, che tiene conto sia del gruppo target più ampio sia della natura volontaria dell'iscrizione. Sono prese in considerazione soltanto le nuove iscrizioni perché gli emittenti e i verificatori gestiscono autonomamente le proprie iscrizioni nel registro di base, ossia effettuano autonomamente modifiche e altri adeguamenti. Tuttavia, l'utilizzo del registro di base non è riservato soltanto alle imprese già iscritte nel registro di commercio ma anche ad altre imprese finora non iscritte e a singole persone. Malgrado questo ampliamento del gruppo target, l'effettivo utilizzo del registro risulta piuttosto moderato: la media del 20 per cento rispecchia quindi una stima prudente dell'effettiva partecipazione.

Pertanto, dai costi totali rimanenti, pari a 1,44 milioni di franchi, e dalle previste iscrizioni nel registro di base risulta un emolumento di 150 franchi.

Cpv. 2

Secondo l'articolo 31 LIdE la riscossione di un emolumento è prevista quando gli emittenti e i verificatori chiedono di iscrivere i loro dati nel registro di fiducia. Diversamente dall'iscrizione nel registro di base, per confermare l'identificativo di un emittente o di un verificatore privato nel registro di fiducia occorre verificare la richiesta secondo l'articolo 10 o verificare che i dati nel registro di fiducia siano aggiornati secondo l'articolo 11 capoverso 4. L'emolumento per la verifica di una richiesta è quindi calcolato forfettariamente in base all'onere previsto e **ammonta a 350 franchi** per richiesta verificata.

Art. 38 Emolumenti per la verifica dell'identità in presenza

Cpv. 1

Gli emolumenti per la verifica dell'identità in presenza nella procedura di emissione dell'e-ID sono stabiliti dai Cantoni nell'ambito delle presenti condizioni quadro:

a. se viene emesso solo l'e-ID: 29 franchi per la verifica dell'identità;

b. se viene emesso l'e-ID combinato con il rilascio di una carta d'identità, di un passaporto o di entrambi i documenti: un emolumento massimo di 15 franchi per

[12] La media delle nuove iscrizioni si basa sulle tabelle comparative dei rapporti annuali cantonali fornite dall'Ufficio federale del registro di commercio conformemente all'articolo 5*a* dell'ordinanza sul registro di commercio (cfr. Statistica del registro di commercio).

la verifica dell'identità, in aggiunta all'emolumento da pagare per il rilascio di tali documenti.

Questa normativa sugli emolumenti fornisce una chiara struttura degli emolumenti relativi alle diverse varianti di emissione dell'e-ID e al contempo impedisce che, per l'e-ID, i Cantoni chiedano un importo superiore ai costi della verifica dell'identità in presenza.

Cpv. 2

Le rappresentanze consolari possono riscuotere un emolumento di massimo 28 franchi per la verifica dell'identità in presenza, secondo l'articolo 14 capoverso 3 dell'ordinanza del 7 ottobre 2015[13] sugli emolumenti del DFAE.

Capitolo 7: Disposizioni finali

Art. 39 Modifica di altri atti normativi

Il progetto propone di modificare altri atti normativi. Questi adeguamenti mirano in particolare a favorire l'utilizzo dell'e-ID sia nel mondo virtuale che in quello reale. L'e-ID deve sempre essere accettato come prova dell'identità, in particolare dalle autorità, indipendentemente dal fatto che l'identificazione sia effettuata online o in presenza. L'e-ID non sostituisce i documenti d'identità fisici, ma deve poter essere presentato come alternativa. Grazie all'applicazione per la verifica dei mezzi di autenticazione elettronici, le autorità possono ad esempio verificare facilmente un e-ID in caso di contatto diretto con una persona. Dovranno accettare l'e-ID anche nell'ambito di una procedura in cui non occorre una copia di un documento d'identità (art. 24 LIdE).

Art. 40 Entrata in vigore

L'articolo 35 capoverso 2 lettera b LIdE prevede la possibilità di predisporre successivamente il sistema per le copie di sicurezza (art. 15). Tale sistema vuole consentire al titolare di conservare le copie di sicurezza dei suoi mezzi di autenticazione elettronici. Esso dovrà essere predisposto entro due anni dall'entrata in vigore della presente ordinanza. Anche l'adeguamento dell'applicazione per la verifica dei mezzi di autenticazione elettronici di cui all'articolo 16 (check app della Confederazione) e per la verifica in presenza secondo l'articolo 24 dovrà essere messo in atto entro due anni dall'entrata in vigore della presente ordinanza.

[13] RS **191.11**

4 Commenti all'Allegato 1 (modifica di altri atti normativi)

Con l'introduzione della LIdE e della relativa ordinanza, il titolare di un e-ID potrà identificarsi presentando l'e-ID oppure, come finora, con un documento d'identità fisico. In particolare, per garantire l'utilizzo dell'e-ID, è necessario modificare diverse ordinanze del Consiglio federale.

Va fatto notare che anche alcune ordinanze del DFGP dovranno essere modificate a livello dell'unità amministrativa interessata.

4.1 Ordinanza SIMIC del 12 aprile 2006[14]

Art. 9 lett. b n. 9

Tutti i cittadini stranieri residenti in Svizzera sono registrati in SIMIC (Sistema d'informazione centrale sulla migrazione) con dati personali univoci. Tutte le funzioni e le attività svolte durante il soggiorno in Svizzera, dall'entrata all'uscita, sono registrate in SIMIC. Più di 30 000 collaboratori degli uffici della migrazione federali, cantonali e comunali nonché diversi uffici di collocamento lavorano con questa applicazione.

I dati del settore degli stranieri sono ora resi accessibili tramite una procedura di richiamo anche al Servizio competente in materia di identità statale di fedpol (fedpol SID) per l'adempimento dei compiti secondo la LIdE.

Art. 10 lett. b n. 9

I dati del settore dell'asilo sono ora resi accessibili tramite una procedura di richiamo anche a fedpol SID per l'adempimento dei compiti secondo la LIdE.

Art. 18 cpv. 4 lett. g

La Segreteria di Stato della migrazione (SEM) distrugge i dati personali non degni di archiviazione contenuti nel SIMIC in base alla regola seguente: i dati biometrici destinati alla carta di soggiorno per stranieri sono distrutti 20 anni dopo la loro registrazione.

Allegato 1

Il catalogo dei dati SIMIC, rappresentato sotto forma di tabella, comprende ora anche fedpol SID.

[14] RS **142.513**

4.2 Ordinanza del 20 settembre 2002[15] sui documenti d'identità (ODI)

Art. 28 lett. l

All'articolo 28, che definisce gli scopi dell'elaborazione dei dati, deve essere aggiunta una nuova lettera l secondo la quale il sistema d'informazione per documenti d'identità (ISA) serve in particolare per la verifica dell'identità secondo l'articolo 17 LIdE quando viene emesso un e-ID.

ISA raccoglie i dati per l'allestimento delle carte d'identità e dei passaporti svizzeri e li mette a disposizione dei servizi responsabili della produzione dei documenti. La cerchia di utenti in seno alle autorità federali, agli uffici cantonali dei passaporti e alle rappresentanze svizzere all'estero comprende varie centinaia di persone.

All. 1 (art. 30 cpv. 1)

L'accesso a ISA da parte delle autorità interessate e l'estensione dei loro diritti sono disciplinati nell'allegato 1. Al Servizio competente in materia di identità statale (fedpol SID) saranno attribuiti gli stessi diritti di elaborare o consultare i dati registrati in ISA come al servizio di polizia competente della Confederazione (fedpol Pol; cfr. art. 12 cpv. 2 lett. d e f, nonché cpv. 3 LDI), esclusi firma, impronte digitali e stato del documento. fedpol SID riceverà inoltre le iscrizioni inerenti al blocco nonché i dati sulla denuncia o sulla revoca della perdita.

4.3 Ordinanza del 19 ottobre 2016[16] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

Art. 11 cpv. 5

L'indirizzo postale privato di privati e rappresentanti di organizzazioni finora poteva essere trattato solo nei sistemi IAM (art. 9 lett. b OIAM). Ora, invece, anche l'indirizzo postale privato delle persone di cui all'articolo 8 OIAM (ma non delle persone di cui all'art. 9 lett. a OIAM) può essere trattato nei pertinenti sistemi IAM, nei servizi di elenchi e nell'archivio centralizzato delle identità di cui all'articolo 13 OIAM e quindi le rispettive voci sono contrassegnate con due asterischi (**). Tali dati possono essere comunicati soltanto a sistemi d'informazione dell'Amministrazione federale centrale. Il rispetto di questa limitazione deve essere garantito dai rispettivi sistemi IAM. A seconda che un sistema d'informazione a valle appartenga o no all'Amministrazione federale centrale, l'indirizzo postale privato deve essere inserito nell'elenco di cui all'articolo 15 capoverso 2 OIAM. Non è consentito, ad esempio, comunicare l'indirizzo postale privato a un gestore esterno secondo l'articolo 17 OIAM.

[15] RS **143.11**

[16] RS **172.010.59**

La limitazione concerne unicamente le voci contrassegnate con due asterischi e si applica soltanto ai dati di persone di cui all'articolo 8. Non si applica invece all'indirizzo postale privato di persone di cui all'articolo 9 lettera b OIAM, che può già ora essere trattato e in certi casi comunicato anche a gestori esterni.

Art. 19 cpv. 1

L'e-ID è un mezzo d'identificazione elettronico che permette di provare la propria identità. Non può invece essere utilizzato per ricevere un'autorizzazione di accesso.

Art. 19 cpv. 3

Quando viene presentato, l'e-ID viene trasmesso al verificatore sotto forma di pacchetto di dati conformemente all'articolo 7 capoverso 1 LIdE.

All. lett. g

Con l'introduzione dell'e-ID, anche le relative informazioni supplementari (numero e-ID, emittente e data di emissione) devono poter essere trattate in un sistema IAM. Tali informazioni devono poter essere salvate anche nei corrispondenti archivi per gli audit.

Il trattamento di altri attributi dell'e-ID è già disciplinato in altre lettere dell'allegato.

4.4 Ordinanza del 19 ottobre 2022[17] sul casellario giudiziale (OCaGi)

Art. 52 cpv. 2

L'articolo 52 capoversi 2 e 3 OCaGi disciplina i requisiti relativi alla prova dell'identità di cui all'articolo 54 capoverso 3 LCaGi: in linea di massima sono accettati secondo l'articolo 52 capoverso 2 OCaGi solo i documenti d'identità ufficiali, ovvero passaporto, carta d'identità e carta di soggiorno per stranieri. Nella procedura di richiesta in linea si accetta anche l'e-ID secondo la LIdE del 20 dicembre 2024.

4.5 Ordinanza del 27 ottobre 1976[18] sull'ammissione alla circolazione (OAC)

Art. 11 cpv. 3 e 4

Utilizzo dell'e-ID per la domanda di rilascio di una licenza
All'elenco dei documenti d'identità di cui all'articolo 11 capoverso 3 OAC occorre aggiungere l'e-ID. L'utilizzo dell'e-ID permette di digitalizzare ulteriormente la presentazione della domanda per il rilascio di una licenza per allievo conducente, di una licenza di condurre o del permesso per il trasporto professionale di persone,

[17] RS **331**

[18] RS **741.51**

purché i Cantoni ne facciano uso e creino possibilità per usufruirne. Poiché l'identità viene già verificata al momento del rilascio di un e-ID secondo la LIdE (online da fedpol [art. 17 cpv. 1 lett. a LIdE] o in presenza presso un'autorità o un ufficio designato [art. 17 cpv. 1 lett. b LIdE]), in questo caso presentarsi personalmente sarebbe superfluo. Affinché le autorità possano trattare le domande pervenute anche per via elettronica, la persona incaricata di ricevere la domanda deve poter certificare l'identità in una forma elettronica adeguata a tal fine. Pertanto, si propone di completare l'articolo 11 capoverso 4 e l'allegato 4 OAC.

4.6 Ordinanza del 30 novembre 2018[19] concernente il sistema d'informazione sull'ammissione alla circolazione (OSIAC)

Allegati 1 e 2

Indirizzo e-mail e numeri di telefono
Indicare indirizzi e-mail o numeri di telefono (di cellulare o di rete fissa) è importante nella comunicazione tra le autorità e i cittadini nel contesto digitale e consente di alleggerire l'onere amministrativo per entrambe le parti. Tali indicazioni sono necessarie per il processo di rilascio della licenza digitale per allievo conducente e, in futuro, lo saranno anche per altri documenti e mezzi di autenticazione elettronici.

Secondo l'articolo 14 OAC[20], le autorità d'ammissione trasmettono al sottosistema SIAC Persone le generalità del richiedente. Di conseguenza nella domanda per il rilascio di una licenza per allievo conducente, di una licenza di condurre o del permesso per il trasporto professionale di persone secondo l'allegato 4 OAC occorre inserire l'indirizzo e-mail e il numero di telefono cellulare.

Affinché gli attributi possano essere riportati nel sistema d'informazione sull'ammissione alla circolazione (SIAC), il termine generico «numeri di telefono» e l'«indirizzo e-mail» devono essere ripresi negli allegati 1 numero 22 e 2 numeri 112, 212, 222, 223 e 232 **OSIAC**.

Numero AVS
Il numero AVS è un identificativo univoco assegnato alle persone che risiedono in Svizzera (o ai fini dell'assicurazione sociale o a coloro che esercitano un'attività lucrativa). Si rivela quindi utile per ottimizzare i processi amministrativi. Dalla revisione della legge sull'AVS, molte autorità cantonali utilizzano già il numero AVS come identificativo univoco. Ciò consente di garantire l'esattezza dei dati secondo il diritto in materia di protezione dei dati e riduce l'onere amministrativo, in modo da sgravare le autorità d'esecuzione. Si possono così evitare in ampia misura i costi degli errori di identificazione di nomi e gli inconvenienti per gli interessati.

[19] RS **741.58**
[20] RS **741.51**

Pertanto, occorre aggiungere il numero AVS negli allegati 1 numero 21 e 2 numeri 111 e 211 OSIAC[21].

Numeri di identificazione commerciali (IDI, numero RIS, numero di partner commerciale)
Il termine generico «numeri di identificazione commerciali» comprende identificativi univoci per persone giuridiche, che a seguito delle modifiche sull'e-ID devono essere integrati per semplici motivi di completezza.

- Per le persone giuridiche, il numero d'identificazione delle imprese (IDI) e il numero RIS del Registro delle imprese e degli stabilimenti sono l'equivalente del numero AVS e fungono quindi da identificativi univoci. L'Ufficio federale della dogana e della sicurezza dei confini (UDSC) prevede di utilizzare il numero IDI e il numero RIS nel quadro della fatturazione della tassa sul traffico pesante commisurata alle prestazioni (TTPCP)[22] e di acquisirli dal SIAC per un'esecuzione efficace[23]. L'utilizzo del numero IDI e del numero RIS può migliorare ulteriormente la qualità dei dati, come nel caso del numero AVS.

- Il numero di partner commerciale permette di identificare il partner commerciale in modo univoco nel quadro della fatturazione e semplifica il trattamento dei dati di base.

Il termine generico «numeri di identificazione commerciali» deve quindi essere ripreso negli allegati 1 numero 21 e 2 numeri 212, 221, 222, 231, 232 e 241 OSIAC.

Lingua di corrispondenza
Il termine «lingua» non è chiaro; nell'allegato 1 numero 22 OSIAC deve quindi essere precisato e sostituito con «lingua di corrispondenza».

4.7 Ordinanza del 15 novembre 2017[24] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT)

Art. 20a cpv. 1, frase introduttiva e lett. b-d, cpv. 2 lett. a, frase introduttiva e n. 3 nonché cpv. 4 e 5

Per i servizi di telefonia mobile, la verifica dell'identità della persona fisica è obbligatoria. La relativa procedura non è disciplinata. È possibile identificare una persona fisica in presenza, tramite video oppure online. Nell'ultimo caso occorre rispettare gli standard di sicurezza e qualità definiti nella circolare della FINMA 2016/7 «Video identificazione e identificazione online». Per garantire un'identificazione sicura, il mezzo

[21] SR **741.58**
[22] RS **641.81**
[23] Conformemente all'articolo 89*d* lettera f della legge federale sulla circolazione stradale (LCStr; RS ***741.01***)
[24] RS **780.11**

d'identificazione deve essere valido il giorno del rilevamento, vale a dire nel momento in cui è presentato al fornitore o al rivenditore o è utilizzato online[25].

L'articolo 20*a* OSCPT è modificato per tenere conto dell'e-ID emesso da fedpol per le persone fisiche e introdotto con la LIdE. L'elenco dei documenti di cui al capoverso 1 è completato aggiungendo l'e-ID (lett. d).

L'e-ID consiste in un pacchetto di dati che servono per provare la propria identità online (art. 13 LIdE). Pertanto, nella frase introduttiva, la nozione «documenti» è sostituita con il termine più generale «mezzi d'identificazione». Al capoverso 2, «documento» è sostituito con «mezzo d'identificazione», più adeguato per tenere conto dell'e-ID. Il capoverso 3 resta invariato.

Il *capoverso 4, primo periodo* rimane invariato. In questo caso il termine «documento» può essere mantenuto perché fa riferimento ai documenti di cui al capoverso 1 lettere a–c e non all'e-ID. È aggiunto un *secondo periodo* per tenere conto delle informazioni specifiche necessarie in caso di utilizzo di un e-ID, ovvero soltanto i dati di cui al capoverso 2 e la fotografia, al posto di una copia del documento d'identità fisico. L'e-ID, infatti, contiene informazioni che il passaporto, la carta d'identità o la carta di soggiorno per stranieri non contengono, in particolare il numero AVS (art. 15 cpv. 1 lett. i LIdE). Sarebbe sproporzionato e contrario all'articolo 6 LPD chiedere a chi decide di identificarsi con un e-ID di fornire queste informazioni visto che non sarebbe tenuto a farlo se decidesse di identificarsi con un documento d'identità fisico.

Inoltre, occorre registrare i dati necessari per la verifica dell'autenticità e dell'integrità, come una firma elettronica (art. 5 cpv. 2 LIdE). Il fornitore o il rivenditore non è obbligato a verificare in modo dettagliato l'autenticità del documento d'identità, ma è soltanto tenuto ad accettare documenti d'identità la cui autenticità risulta plausibile[26]. Pertanto, deve essere effettuato unicamente un controllo sommario. Per quanto riguarda l'e-ID, senza un controllo sarebbe possibile far registrare dati errati o presentare la fotografia di un'altra persona presso un fornitore o un rivenditore poco scrupoloso. Inoltre, la produzione di questi dati di verifica sarà verosimilmente rapida, cosicché la loro raccolta e trasmissione non richiederà più tempo che per un documento d'identità fisico.

Nel capoverso 5, aggiunto per una migliore leggibilità, la disposizione di cui all'articolo 20*a* capoverso 4, secondo periodo OSCPT è ripresa e adeguata all'e-ID. Per migliorare la leggibilità è stato introdotto un capoverso 5. Poiché riguarda i dati raccolti, il rimando ai relativi capoversi è stato adeguato aggiungendo il capoverso 4. Il termine entro cui il rivenditore deve trasmettere i dati ai fornitori di servizi di telecomunicazione rimane invariato a tre giorni.

---

[25] Cfr. rapporto esplicativo del 15.11.2023 concernente la revisione parziale di ordinanze esecutive della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**LSCPT**), ad art. 20*a*, pag. 20 e seguenti.

[26] Cfr. il rapporto esplicativo summenzionato, ad art. 20a, pag. 20 e seguenti.

4.8 Ordinanza del 29 agosto 2012[27] sulle poste (OPO)

Art. 35e cpv. 2 lett. c e cpv. 3

Gli utenti del sistema di recapito ibrido, in particolare gli emittenti e i destinatari, devono identificarsi e autenticarsi presso la Posta (cpv. 1). Secondo la lettera c, per l'identificazione delle persone può essere utilizzato l'e-ID. In questo modo viene precisato che nel quadro del servizio universale si aggiunge l'e-ID come prova elettronica dell'identità. La Commissione federale delle poste non deve quindi determinare quali prove elettroniche dell'identità possono essere utilizzate per l'identificazione degli utenti (cpv. 3).

4.9 Ordinanza del 9 marzo 200728 sui servizi di telecomunicazione (OST)

Art. 41 cpv. 5 lett. b

Con la LIdE si crea la base per emettere mezzi d'identificazione elettronici che permettono alle singole persone di identificarsi in ambito digitale mediante dati confermati a livello statale. In questo modo si crea la base per un e-ID con cui le persone possono provare la propria identità. Ora per accedere ai servizi a valore aggiunto bloccati ai minorenni è possibile provare la propria identità con un e-ID.

4.10 Ordinanza del 6 ottobre 1997[29] concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT)

Art. 4 cpv. 1ter e art. 4 cpv. 1ter lett. a

Con la LIdE si crea la base per emettere mezzi d'identificazione elettronici che permettono alle singole persone di identificarsi in ambito digitale mediante dati confermati a livello statale. In questo modo si crea la base per un e-ID con cui le persone possono provare la propria identità. Nell'ambito dell'attribuzione di elementi d'indirizzo, la prova dell'identità del richiedente può anche essere fornita con un e-ID.

4.11 Ordinanza del 5 novembre 2014[30] sui domini Internet (ODIn)

Art. 24 cpv. 3 lett. a

---

27 RS **783.01**

28 RS **784.101.1**

29 RS **784.104**

30 RS **784.104.2**

Con la LIdE si crea la base per emettere mezzi d'identificazione elettronici che permettono alle singole persone di identificarsi in ambito digitale mediante dati confermati a livello statale. In questo modo si crea la base per un e-ID con cui le persone possono provare la propria identità. Nell'ambito dell'attribuzione di nomi di dominio, la prova dell'identità del richiedente e del rispetto delle condizioni di attribuzione può anche essere fornita con un e-ID.

4.12 Ordinanza del 4 dicembre 2000[31] sulla medicina della procreazione (OMP)

Art. 21 cpv. 2

In linea di principio, il richiedente può provare la sua identità mediante una copia di un documento d'identità (passaporto, carta d'identità o documento d'identità equivalente) oppure con un e-ID secondo la LIdE. La possibilità di trasmettere una copia di un documento d'identità online ha già dato buoni risultati in relazione alla richiesta di un estratto del casellario giudiziale. L'introduzione dell'e-ID rende inoltre possibile una variante digitale della prova dell'identità che non richiede la presentazione di una copia del documento d'identità.

4.13 Ordinanza del 22 marzo 2017[32] sulla cartella informatizzata del paziente (OCIP)

L'emittente dello strumento d'identificazione necessario per accedere alla cartella informatizzata del paziente (CIP) deve verificare l'identità del richiedente. In futuro, l'identità potrà essere provata anche mediante l'e-ID.

Con l'adozione della LIdE, la legge federale del 19 giugno 2015[33] sulla cartella informatizzata del paziente (LCIP) viene modificata in modo che soltanto gli emittenti privati di strumenti d'identificazione devono essere certificati da un organismo riconosciuto (art. 11 lett. c LCIP). I Cantoni in quanto emittenti di strumenti d'identificazione[34], invece, non sono certificati. Tuttavia, gli strumenti d'identificazione emessi dai Cantoni devono soddisfare gli stessi requisiti di quelli emessi da privati. I Cantoni sono responsabili per il rispetto di tali requisiti.

Gli strumenti d'identificazione emessi dai Cantoni, così come quelli emessi da privati, devono essere utilizzati dai professionisti della salute e dai pazienti per autenticarsi nel sistema della CIP. In futuro, deve poter essere impiegato anche il sistema gestito dalla CaF che sulla base dell'e-ID consente l'autenticazione di persone fisiche (AGOV).

---

31 RS **810.112.2**

32 RS **816.11**

33 RS **816.1**

34 I Cantoni di Ginevra e Vaud rilasciano già strumenti d'identificazione per accedere alla CIP.

Art. 9 cpv. 2 lett. e

Agli strumenti con i quali i professionisti della salute possono autenticarsi per accedere alla CIP si aggiungono gli strumenti d'identificazione emessi dai Cantoni. L'autenticazione può essere effettuata anche tramite AGOV.

Art. 16

Agli strumenti con i quali i pazienti possono confermare il consenso per la costituzione di una CIP si aggiungono gli strumenti d'identificazione emessi dai Cantoni (*lett. b*). Il consenso può essere confermato anche tramite AGOV (*lett. c*).

Art. 17 cpv. 1 lett. c

Agli strumenti con i quali i pazienti possono autenticarsi per accedere alla CIP si aggiungono gli strumenti d'identificazione emessi dai Cantoni. L'autenticazione può essere effettuata anche tramite AGOV.

Art. 24 cpv. 1

La persona che richiede uno strumento d'identificazione per accedere alla CIP potrà provare la sua identità all'emittente di strumenti d'identificazione esibendo l'e-ID.

Art. 27a Strumenti d'identificazione emessi dai Cantoni

Siccome dovranno essere certificati soltanto gli emittenti privati di strumenti d'identificazione (art. 11 lett. c LCIP), occorre disciplinare chi è responsabile di garantire che siano utilizzati unicamente strumenti d'identificazione sicuri per autenticarsi e accedere alla CIP. Il *capoverso 1* attribuisce questa responsabilità ai Cantoni in quanto emittenti. I Cantoni devono assicurare che gli strumenti d'identificazione da essi rilasciati rispettino i requisiti di cui agli articoli 23–27 OCIP e le condizioni di cui all'articolo 31 capoversi 2 e 3. I requisiti sono disciplinati nell'allegato 8 dell'ordinanza del DFI del 22 marzo 2017[35] sulla cartella informatizzata del paziente (OCIP-DFI).

I Cantoni comunicano all'Ufficio federale della sanità pubblica (UFSP) gli strumenti d'identificazione da essi rilasciati (*cpv. 2*). Secondo il capoverso 3, quest'ultimo provvede affinché tali strumenti d'identificazione vengano pubblicati, analogamente ai certificati degli emittenti privati di strumenti d'identificazione secondo l'articolo 33 capoverso 2.

La clausola di salvaguardia concernente gli strumenti d'identificazione rilasciati da emittenti certificati (art. 37 cpv. 1 lett. b) si applica anche agli strumenti d'identificazione

[35] RS **816.111**

emessi dai Cantoni (cpv. 4). L'UFSP può richiedere ai Cantoni i documenti necessari per valutare le circostanze.

Art. 28 cpv. 2

Soltanto gli emittenti privati di strumenti d'identificazione devono essere certificati. Anche l'accreditamento vale quindi soltanto per gli organismi che certificano tali emittenti privati. Il *capoverso 2* è modificato di conseguenza.

Art. 31, rubrica e cpv. 1

Soltanto gli emittenti privati di strumenti d'identificazione devono essere certificati. I Cantoni sono responsabili per gli strumenti d'identificazione che emettono. La *rubrica* e *il capoverso 1* sono modificati di conseguenza.

Art. 32 cpv. 3

L'organismo di certificazione rilascia il certificato soltanto agli emittenti privati di strumenti d'identificazione che soddisfano i rispettivi requisiti. Gli emittenti cantonali di strumenti d'identificazione, invece, non vengono certificati e non ricevono quindi alcun certificato. Il *capoverso 3* è modificato di conseguenza.

Art. 36 cpv. 1

Soltanto gli emittenti privati di strumenti d'identificazione devono comunicare all'organismo di certificazione ogni sostanziale adeguamento tecnico od organizzativo. Questo obbligo non si applica agli emittenti cantonali di strumenti d'identificazione, perché per questi ultimi sono responsabili i Cantoni. Il *capoverso 1* è modificato di conseguenza.

4.14 Ordinanza del 23 novembre 2016[36] sulla firma elettronica (OFiEle)

Art. 5 cpv. 1bis

I prestatori di servizi di certificazione devono accertare l'identità precisa delle persone che chiedono il rilascio di un certificato regolamentato (art. 9 cpv. 1 FiEle). Di norma i richiedenti devono presentarsi personalmente presso un prestatore di servizi di certificazione riconosciuto (art. 5 cpv. 1 OFiEle). L'obbligo di presentarsi personalmente decade se l'identità è provata mediante un e-ID. Questo nuovo capoverso precisa ulteriormente le procedure riguardanti l'identificazione tramite e-ID.

[36] RS **943.032**

Art. 6 cpv. 1

L'obbligo di una persona che chiede il rilascio di un certificato regolamentato per un'unità IDI che non è una persona fisica di esibire un passaporto, una carta d'identità svizzera o una carta d'identità riconosciuta per l'entrata in Svizzera è precisato indicando che può essere utilizzato anche un'e-ID secondo la LIdE.

4.15 Ordinanza dell'11 novembre 2015[37] sul riciclaggio di denaro (ORD)

Art. 17 cpv. 3 lett. b e 3bis

L'articolo 17 capoverso 3 ORD disciplina le procedure che i commercianti di cui all'articolo 2 capoverso 1 lettera b ORD devono applicare per identificare la controparte secondo le prescrizioni in materia di riciclaggio di denaro.

Per l'identificazione della controparte, nella prassi sono accettati soltanto documenti validi. La verifica è svolta da un ufficio di revisione interno o esterno. Alla lettera b deve quindi essere aggiunto «ed è valido» per tenere conto della prassi vigente e far sì che il testo dell'ordinanza corrisponda al nuovo capoverso 3bis lettera b.

Per maggiore chiarezza, nel nuovo articolo 17 capoverso 3bis ORD è precisato che l'identificazione della controparte può essere effettuata anche mediante l'e-ID secondo la LIdE.

L'utilizzo dell'e-ID ai fini dell'identificazione delle controparti da parte degli intermediari finanziari (art. 2 cpv. 1 lett. a LRD) è disciplinato nelle prescrizioni dell'Autorità federale di vigilanza sui mercati finanziari FINMA. L'utilizzo dell'e-ID per identificare le controparti di saggiatori del commercio e delle loro società del gruppo che commerciano metalli preziosi bancari a titolo professionale (art. 42bis LCMP) e sono considerate intermediari finanziari (art. 2 cpv. 2 lett. g LRD) è disciplinato nell'ordinanza UDSC sul riciclaggio di denaro (ORD-UDSC) (cfr. art. 17 cpv. 1 lett. d LRD e art. 42ter cpv. 4 LCMP).

Inoltre, a prescindere dall'articolo 17 capoverso 3bis ORD, l'e-ID può essere utilizzato per verificare l'identità dei clienti da cui il titolare di una patente di fonditore o di acquirente accetta materie da fondere (art. 168*a* cpv. 2 in combinato disposto con l'art. 172*e* cpv. 1 OCMP nonché direttive e istruzioni ancora da emanare).

[37] RS **955.01**

5 Ripercussioni

5.1 Ripercussioni per la Confederazione

Con il presente progetto d'ordinanza non si attendono ripercussioni finanziarie o sull'effettivo del personale che vanno oltre il fabbisogno di risorse già previsto nel quadro del programma e-ID per l'implementazione, la gestione e l'ulteriore sviluppo dell'infrastruttura di fiducia, l'emissione dell'e-ID e i progetti pilota concernenti l'e-ID per il periodo 2023–2028.

5.2 Ripercussioni per i Cantoni e i Comuni

L'e-ID può essere richiesto ed emesso online e l'identità può essere fatta verificare in presenza presso un centro di registrazione. Le persone interessate possono quindi prendere appuntamento per far verificare unicamente l'identità dell'e-ID (variante semplice), ad esempio per evitare di salvare dati biometrici supplementari, o recarsi presso l'autorità per richiedere l'e-ID insieme al rilascio di documenti fisici (variante *Documenti+*).

Sulla base di esperienze internazionali e stime di massima, si prevede che solo l'1 per cento di tutti i potenziali utenti dell'e-ID opterà per la variante semplice. Per la variante *Documenti+* si stima che, in particolare a causa delle tasse supplementari, soltanto il 5 per cento delle persone che si presentano all'autorità per rinnovare i documenti deciderà di richiedere direttamente anche l'e-ID, ossia circa 40 000 casi all'anno per gli uffici dei passaporti. Per motivi di procedura possono usufruire della variante *Documenti+* soltanto i richiedenti di una carta d'identità svizzera o un passaporto svizzero.

5.3 Ripercussioni sull'economia

In Svizzera la trasformazione digitale procede a grandi passi. Un numero crescente di transazioni può essere effettuato online; presentarsi di persona è sempre meno necessario. Ci si attende sempre più che sia possibile svolgere per via elettronica diverse operazioni, preferibilmente su uno smartphone. La LIdE e le presenti disposizioni d'esecuzione costituiscono la base per utilizzare mezzi di autenticazione elettronici nelle transazioni online. Si creano le condizioni per un ecosistema che consente di emettere, utilizzare e presentare in modo sicuro diversi mezzi di autenticazione elettronici. Si tratta di un insieme di norme e standard, procedure, principi ed elementi infrastrutturali che instaurano la fiducia nelle procedure digitali, ne garantiscono la conformità, e sono accettati e utilizzati da un vasto pubblico. Con l'e-ID, le autorità e le imprese possono utilizzare gli stessi formati per numerosi servizi online. Per gli utenti di tali servizi si riduce il numero delle diverse procedure di autenticazione, il che contribuisce anche a minimizzare i dati e a proteggere la sfera privata. Definendo standard e riducendo gli ostacoli all'utilizzo di servizi online, si creano grandi opportunità di innovazione per l'economia e i servizi pubblici.

5.4 Ripercussioni sulla società

I mezzi d'identificazione elettronici riconosciuti contribuiscono a proteggere l'identità dei loro titolari in una società ampiamente interconnessa rendendo molto più difficile usurpare l'identità di una persona e utilizzarla in maniera potenzialmente problematica. Nelle applicazioni della Confederazione per la conservazione, la presentazione e la verifica di mezzi d'identificazione elettronici, si dà agli utenti la possibilità di verificare l'identità degli emittenti e dei verificatori dei mezzi di autenticazione elettronici. Le applicazioni dovrebbero essere più intuitive possibile, in modo che i mezzi di autenticazione elettronici siano di facile accesso e semplici da usare per tutti i cittadini.

Per promuovere la resilienza digitale e la sovranità digitale, si segue il principio dell'identità autogestita. Essa consente di conservare i dati in maniera decentralizzata presso i singoli utenti. Lo scambio di dati tra le parti interessate dalla transazione si svolge direttamente tramite un servizio centrale.

6 Aspetti giuridici

6.1 Sicurezza delle informazioni

L'utilizzazione abusiva delle informazioni così come le perturbazioni dell'infrastruttura di fiducia e del sistema d'informazione per l'emissione e la revoca degli e-ID possono pregiudicare considerevolmente gli interessi della Svizzera e i diritti delle persone nonché compromettere il compito legale di assicurare il funzionamento dell'infrastruttura di fiducia e del sistema d'informazione. Per garantire nel miglior modo possibile la sicurezza delle informazioni si applicano la legge federale del 18 dicembre 2020[38] sulla sicurezza delle informazioni (LSIn) e la relativa ordinanza (OSIn[39]).

L'UFG e l'UFIT per l'infrastruttura di fiducia e fedpol per il sistema d'informazione per l'emissione e la revoca degli e-ID sono tenuti a provvedere affinché le violazioni della sicurezza delle informazioni siano individuate tempestivamente, le loro cause accertate e le eventuali ripercussioni ridotte al minimo. A tal fine, tali autorità adottano le misure necessarie (p. es. analizzando regolarmente i file log) allo scopo di individuare incidenti legati alla sicurezza o lacune in materia di sicurezza. In caso di incidenti di questo tipo, l'UFIT per l'infrastruttura di fiducia e fedpol per il sistema d'informazione adottano le misure immediate necessarie per ridurre al minimo eventuali ripercussioni sulla sicurezza delle informazioni. Nell'ambito dell'infrastruttura di fiducia e dell'e-ID, simili incidenti o lacune si verificano in particolare nel caso in cui la confidenzialità, l'integrità o la disponibilità dei mezzi di autenticazione elettronici, dell'infrastruttura di fiducia o del sistema d'informazione sono compromesse o pregiudicate, vi è il rischio

[38] RS **128**

[39] RS **128.1**

di gravi perturbazioni o se ne sono verificate oppure nel sistema vi sono punti deboli o errori che rappresentano un'importante ciberminaccia.

Nel presente progetto di ordinanza non è necessario disciplinare nel dettaglio la gestione delle minacce alla sicurezza delle informazioni, perché la LSIn e la OSIn prevedono già le pertinenti basi giuridiche per affrontare tali minacce. Come per la LPD, anche in questo caso si fa riferimento al diritto vigente. Ciò significa che le normative vigenti nelle pertinenti leggi sono già sufficienti per garantire un trattamento sicuro dei rischi per la sicurezza delle informazioni.

6.2 Protezione dei dati

Le disposizioni del diritto in materia di protezione dei dati (LPD e relative ordinanze) si applicano a tutti. Le persone fisiche, gli emittenti e i verificatori del settore privato sono sottoposti alle disposizioni per i privati; la Confederazione (fedpol e altre autorità) nonché gli emittenti e i verificatori del settore pubblico sottostanno alle disposizioni per gli organi federali. Nel presente progetto di ordinanza non si rimanda alle pertinenti disposizioni della LPD per evitare ripetizioni e non complicare l'interpretazione. La LIdE precisa già come viene messa in atto la protezione dei dati nell'ambito dell'e-ID. Le disposizioni d'esecuzione concretizzano il contesto istituito nella LIdE per il trattamento, la conservazione e la cancellazione di dati.

L'UFIT mette a disposizione del pubblico un registro di base che permette ai verificatori di assicurarsi che i mezzi di autenticazione non siano stati modificati successivamente e che provengono dall'emittente iscritto nel registro di base. Quest'ultimo contiene le chiavi crittografiche richieste per verificare l'autenticità e l'integrità dei mezzi di autenticazione, gli identificativi degli emittenti e dei verificatori nonché dati relativi alla revoca di tali mezzi. I dati concernenti la revoca dei mezzi di autenticazione elettronici non consentono di risalire né all'identità del titolare né al contenuto del mezzo di autenticazione elettronico.

I dati richiesti per l'iscrizione nel registro di base sono frutto di un'autodichiarazione. Le modifiche apportate al registro sono salvate quotidianamente e conservate per dieci anni. In occasione della consultazione del registro vengono generati dati, segnatamente indirizzi IP, che possono essere conservati al massimo 90 giorni per garantire la sicurezza e assicurare la manutenzione dell'infrastruttura. Il salvataggio di dati al momento della presentazione e della verifica dei mezzi di autenticazione elettronici richiede il consenso del titolare, che può essere revocato in qualsiasi momento. Tutti gli altri dati sono distrutti 90 giorni dopo la loro registrazione nel sistema.

L'UFIT mette a disposizione un registro di fiducia pubblicamente accessibile che contiene informazioni verificate sull'identità di emittenti e verificatori allo scopo di garantire un utilizzo sicuro dei mezzi di autenticazione elettronici. L'iscrizione nel registro viene effettuata soltanto su richiesta e previo consenso esplicito della persona interessata. Tra gli altri dati verificati possono esserci informazioni del registro di commercio o attestati. Durante il processo vengono rilevati altri dati personali, come dati di contatto delle persone con diritto di firma, che però non sono pubblicamente accessibili.

L’UFIT mette a disposizione un’applicazione per verificare i mezzi di autenticazione elettronici. È quindi possibile verificare la validità delle chiavi crittografiche di un mezzo di autenticazione, in particolare dell’e-ID. La Confederazione in quanto emittente non ha accesso al contenuto dei mezzi di autenticazione elettronici o ai dati sul loro utilizzo. Gli utenti possono registrare diversi mezzi di autenticazione nell’applicazione e salvare i dati personali in maniera decentralizzata. La Confederazione in quanto emittente dell’applicazione non ha accesso ai contenuti dei mezzi di autenticazione elettronici. Anche le copie di sicurezza salvate su un sistema gestito dalla Confederazione rimangono illeggibili grazie alla crittografia lato utente. Per garantire l’autenticità dei portafogli elettronici vengono utilizzati identificativi tecnici trattati principalmente dall’emittente dell’e-ID.

Il portafoglio elettronico permette agli utenti di salvare i dati dei mezzi di autenticazione criptandoli in un sistema per le copie di sicurezza. All’accesso la persona deve autenticarsi in modo univoco. Anche se questi dati sono crittografati e la Confederazione non vi può accedere, il salvataggio costituisce un trattamento di dati personali o di dati degni di particolare protezione. Lo scopo del trattamento è unicamente di mettere a disposizione un servizio per salvaguardare i mezzi di autenticazione ed evitare perdite di dati.

L’e-ID contiene dati personali come il cognome ufficiale, i nomi, la data di nascita, il sesso, il luogo d’origine, il luogo di nascita, la cittadinanza, l’immagine del viso e il numero AVS. Può contenere anche informazioni sul documento d’identità utilizzato per la sua emissione. Nel sistema d’informazione per l’emissione e la revoca dell’e-ID sono registrati anche dati concernenti l’emissione e la revoca nonché dati relativi al rappresentante legale di minorenni o di persone sotto curatela. Per la verifica dell’identità si procede con una breve registrazione dell’immagine del viso sotto forma di sequenze video, che serve unicamente per individuare un’eventuale usurpazione dell’identità.

Il sistema d’informazione per l’emissione e la revoca dell’e-ID conserva i dati importanti per 20 anni a decorrere dalla data di emissione, i dati relativi alla procedura di emissione (incl. i dati biometrici) per cinque anni dalla data di scadenza dell’e-ID e tutti gli altri dati per 90 giorni. Il salvataggio dell’e-ID avviene in maniera decentralizzata sullo smartphone del titolare. Fedpol, in quanto emittente dell’e-ID, non riceve informazioni relative all’utilizzo di quest’ultimo. Il titolare decide autonomamente quali dati comunicare quando presenta l’e-ID. I verificatori sono tenuti per legge a proteggere i dati personali.

Alla luce del previsto trattamento dei dati personali nel quadro dei sistemi per le copie di sicurezza, dell’emissione dell’e-ID e dell’infrastruttura di fiducia, i diritti fondamentali delle persone interessate possono essere lesi. A tale proposito viene effettuata una valutazione d’impatto approfondita sulla protezione dei dati per stimare globalmente il rischio per i diritti fondamentali.