Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2018
www.dirittofederale.admin.ch
La versione elettronica firmata
è quella determinante

18.049

Messaggio concernente la legge sui servizi d'identificazione elettronica

del 1° giugno 2018

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di legge sui servizi d'identificazione elettronica.

Nel contempo vi proponiamo di togliere dal ruolo il seguente intervento parlamentare:

2018	M	17.3083	Digitalizzazione. Un'identità elettronica per ridurre la burocrazia a livello nazionale (N 8.3.2017, Gruppo liberale radicale; N 20.9.2017, S 28.02.2018)

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

1° giugno 2018

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Alain Berset
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

La digitalizzazione della società compie enormi passi avanti. La possibilità di identificarsi in Internet in modo sicuro e semplice svolge un ruolo decisivo nel quadro dell'accettazione e dell'ulteriore diffusione di applicazioni digitali in rete. La legge sui servizi di identificazione elettronica (Legge sull'ID, LSIE), oggetto del presente messaggio, introduce la base legale per il rilascio di mezzi di identificazione elettronica che permettono al singolo di identificarsi nello spazio digitale mediante dati attestati dallo Stato.

La LSIE intende promuovere comunicazioni elettroniche sicure tra privati e con le autorità. A tal fine, il disegno prevede una suddivisione dei compiti tra settore pubblico e settore privato. Lo Stato continuerà ad adempiere il suo compito principale che consiste nel verificare e confermare ufficialmente l'identità di una persona, ma, considerata la dinamica del cambiamento tecnologico, non sarebbe tuttavia in grado di sviluppare e produrre i supporti tecnici richiesti per una tale identificazione. Il settore privato, più vicino agli utenti e alle tecnologie digitali necessarie, può svolgere meglio questa funzione. La gestione del sistema di eID e il rilascio dell'eID saranno dunque affidati a fornitori privati (identity provider, IdP). Lo Stato svolgerà comunque un ruolo importate in questo settore in quanto sottoporrà gli IdP e i sistemi che questi ultimi propongono a una severa procedura di riconoscimento e a controlli periodici. In questo modo i requisiti posti alla sicurezza e alla protezione dei dati saranno verificati e costantemente adattati agli sviluppi più recenti. Questo sfruttamento delle sinergie tra il settore pubblico e quello privato, offre condizioni ottimali per introdurre e utilizzare l'eID.

La legge sull'eID non disciplina esaustivamente l'identificazione in Internet, si limita a regolamentare il rilascio e l'utilizzo di eID. In futuro il mercato potrà offrire e utilizzare anche altri mezzi d'identificazione elettronica, privi tuttavia dell'affidabilità conferita dal riconoscimento statale.

Con un eID le persone fisiche possono registrarsi su portali Internet privati e pubblici (servizi che utilizzano l'eID) e accedervi successivamente in modo sicuro e agevole. L'eID faciliterà i contatti con le autorità che sempre più spesso offrono i propri servizi anche mediante «sportelli virtuali». In futuro, le applicazioni dell'e-government potrebbero essere utilizzate completamente in rete. Nell'ambito dei servizi e-health, l'eID integrerà in una prima fase gli strumenti d'identificazione emessi secondo la legge del 19 giugno 2015 per poi verosimilmente sostituirli a medio termine.

Il disegno non indica il supporto su cui gestire l'eID. Attualmente, i mezzi d'identificazione elettronica più usati sono disponibili su cellulari (p. es. la Mobile ID), su tessere o su supporti di memoria con chip integrati (la cosiddetta Integrated Circuit Card ICC o smartcard, p. es. SuisseID) oppure non richiedono alcun tipo di supporto materiale e possono essere impiegati via Internet con il nome utente, la password ed eventualmente un codice di transazione monouso inviato allo smartphone (cfr. soluzioni dell'online banking).

Il disegno di legge fissa tre differenti livelli di sicurezza. Non tutte le transazioni richiedono lo stesso livello di sicurezza e non tutti i supporti sono adatti per ciascun livello di sicurezza. Per questa ragione e per andare incontro alle esigenze del mercato, gli IdP devono dunque poter offrire sistemi di eID che corrispondono ai tre diversi livelli di sicurezza, come prescritto anche dall'UE e dal NIST (National Institute of Standards and Technology). Per poter essere riconosciuto, un sistema di eID deve soddisfare perlomeno il livello di sicurezza «basso». I sistemi di eID dei livelli di sicurezza «significativo» ed «elevato» soddisfano requisiti superiori a quelli minimi.

Il presente disegno prevede condizioni quadro severe in materia di protezione dei dati e disciplina in dettaglio lo scopo e le condizioni del trattamento e della trasmissione dei dati nell'ambito del rilascio e dell'utilizzo dell'eID. L'IdP può trattare i dati d'identificazione soltanto ai fini dell'identificazione secondo la LSIE e per un periodo di tempo determinato. Inoltre può trasmettere ai gestori di servizi che utilizzano l'eID solamente i dati d'identificazione personale necessari all'identificazione della persona, e quindi alla funzione dell'eID interessato, e alla cui trasmissione il titolare dell'eID ha acconsentito. La trasmissione è necessaria affinché il sistema di eID possa garantire un'identificazione semplice e sicura. Infine la LSIE prevede una base legale per il trattamento e la trasmissione dei dati da parte degli organi federali interessati.

Il disegno tiene conto della normativa internazionale e in particolare del regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Anche se non è ancora chiaro se, come e quando la Svizzera sarà integrata in questo sistema mediante un accordo bilaterale, la soluzione elvetica in tema di eID va impostata fin dall'inizio in modo tale da poter essere in linea di principio notificata.

Indice

Messaggio

1 Punti essenziali del progetto

1.1 Situazione iniziale

La diffusione di Internet e la grande disponibilità di dispositivi mobili altamente performanti rendono sempre più semplice trasferire le transazioni commerciali nel mondo digitale. Per svolgere in rete anche transazioni più complesse, i partner (qui di seguito denominati gestori di servizi che utilizzano l'eID*[1]) devono poter fare affidamento sull'identità della controparte. L'identificazione* sicura delle persone costituisce la base per la certezza del diritto, anche al di là delle frontiere nazionali. Al fine di soddisfare questa esigenza, in Svizzera saranno creati mezzi d'identificazione elettronica riconosciuti (denominati anche identità elettronica, E-ID o eID)* per persone fisiche. Per le persone giuridiche si dispone già, con il numero d'identificazione delle imprese (IDI), di un identificatore univoco che può essere integrato in adeguati strumenti informatici a fini identificativi. Un eID consente a un gestore di servizi che utilizzano l'eID di identificare in linea il titolare come avente diritto; eID affidabili contribuiscono pertanto all'implementazione di transazioni elettroniche.

Con decreto federale del 19 dicembre 2012, il Dipartimento federale di giustizia e polizia (DFGP) è stato incaricato di elaborare, in collaborazione con la Cancelleria federale (CaF), il Dipartimento federale dell'economia, della formazione e della ricerca (DEFR), il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) e il Dipartimento federale delle finanze (DFF), un piano e un avamprogetto legislativo per mezzi d'identificazione elettronica statale che possano essere rilasciati con la carta d'identità (CID). Nella prima bozza del piano, presentata nel documento interlocutorio del 28 febbraio 2014, si è partiti dal presupposto che lo Stato sarebbe intervenuto in funzione di fornitore principale dell'identità elettronica rilasciando a tutti gli Svizzeri, in aggiunta alla CID, anche un eID. Il piano è stato posto in consultazione presso gli Uffici e gli attori del mercato tra il 2014 e il 2015.

In seguito il piano è stato sostanzialmente rielaborato sulla base dei riscontri e delle esperienze di altri Paesi. Lo sviluppo di soluzioni statali proprie ed eID rilasciati direttamente dallo Stato comportano di regola costi informatici scoperti troppo elevati per l'ente pubblico poiché lo Stato non è in grado di reagire con sufficiente flessibilità alle esigenze e alle tecnologie in rapida evoluzione. Il piano si fonda dunque su una ripartizione dei compiti tra Confederazione e privati. Il settore privato offre già oggi possibilità d'identificazione elettronica di diversi livelli di sicurezza (p. es. Apple-ID, Google ID, Mobile ID, OpenID, SuisseID*, SwissID*, SwissPass ecc.), ma attualmente non è possibile stabilire quale tipo di eID, accanto agli eID rilasciati in base alla LSIE, supererà la prova del tempo.

[1] I termini contrassegnati con un asterisco sono spiegati nel glossario.

Il piano tiene conto anche dei più recenti sviluppi nell'UE ed è compatibile con il regolamento (UE) 910/2014[2] (regolamento eIDAS*).

Il 13 dicembre 2016, il nostro Consiglio ha preso atto del piano eID rivisto, incaricando il DFGP di elaborare una legge in materia e fissando le condizioni quadro per la legislazione. La consultazione sull'avamprogetto della legge federale sui mezzi d'identificazione elettronica riconosciuti (legge sull'eID) è durata dal 22 febbraio al 29 maggio 2017. Nella seduta del 15 novembre 2017, il nostro Consiglio, dopo aver preso visione dei risultati della consultazione, ha incaricato il DFGP di elaborare un disegno di legge.

1.2 La normativa proposta

1.2.1 Piano eID

Certezza del diritto e fiducia sono presupposti essenziali per le transazioni, il che include un'adeguata conoscenza dell'identità delle parti coinvolte. Per il mondo fisico, la Confederazione rilascia mezzi d'identificazione convenzionali quali il passaporto svizzero, la carta d'identità e la carta di soggiorno. Essendo inoltre documenti di viaggio, il passaporto e la carta d'identità permettono di viaggiare in altri Stati sulla base di convenzioni internazionali. Adesso la Confederazione intende introdurre la possibilità di provare l'identità di una persona fisica anche nel mondo digitale tramite l'eID. Gli eID secondo la LSIE consentiranno a chi le possiede di registrarsi in tutta sicurezza sui servizi in linea e quindi continuare a usufruirne in modo sicuro.

Il fornitore di servizi d'identificazione elettronica (identity provider, IdP)* può offrire anche altri servizi fiduciari, che vanno oltre alla sola identificazione, come la firma elettronica secondo la legge federale del 18 marzo 2016[3] sulla firma elettronica (FiEle). Non essendo tuttavia parte integrante dell'eID, questi servizi, non sono contemplati dal presente disegno, che non disciplina peraltro nemmeno i diritti d'accesso ai servizi in linea (*access management*). In questo caso infatti non si tratta soltanto di identificare le persone, ma anche di offrire l'accesso a un servizio a chi ne ha effettivamente il diritto. Oltre alle soluzioni di identificazione, gli IdP sono liberi di offrire anche un *access management* sicuro e quindi proporre ai servizi che utilizzano l'eID una soluzione globale nel cosiddetto «IAM – Identity and Access Management»*.

Il piano eID si basa sui lavori svolti da fedpol negli anni 2013–2015 nell'ambito dei quali sono stati consultati anche importanti operatori del mercato. Tiene inoltre conto delle conoscenze emerse da precedenti soluzioni di eID adottate da altri Paesi,

2 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 lug. 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. GU L 257 del 28 ago. 2014, pag. 73, rettificato in GU L 272 del 7 ott. 2016, pag. 96. Un elenco dei principi giuridici comunitari (con i link) è pubblicato sul sito dell'UFG > Stato & Cittadino > Progetti di legislazione in corso > Legge sull'eID.

3 RS **943.03**

degli sviluppi internazionali relativi a soluzioni pratiche per eID e delle prescrizioni sulla compatibilità UE previste dal regolamento eIDAS.

1.2.2 Interazione tra Stato e privati

Il disegno prevede un'interazione tra Stato e privati. L'affidabilità creata dal riconoscimento e dalla vigilanza da parte dello Stato è associata al *know how* tecnologico e al dinamismo del settore privato. Procedendo in questo modo si garantirà un'ampia accettazione dell'eID presso la popolazione. La Confederazione delega agli IdP che soddisfano le condizioni richieste il rilascio degli eID e la gestione dei sistemi di eID*. Tutti i sistemi di eID dovranno essere interoperabili affinché i titolari possano utilizzare l'eID a prescindere dal servizio che utilizza l'eID a vantaggio dei clienti.

Continuerà a spettare allo Stato verificare e confermare ufficialmente l'identità di una persona attraverso elementi presenti nei sistemi d'informazione della Confederazione. Questo compito sarà affidato a un servizio d'identità*, appositamente predisposto in seno a fedpol, che gestirà i registri ufficiali con i dati corrispondenti. Detto servizio verificherà se gli utenti soddisfano i presupposti personali e sarà competente per l'accertamento dell'identità delle persone al momento della prima identificazione. Attribuirà inoltre il numero di registrazione eID* ai dati d'identificazione personale* degli utenti. Dal canto loro gli IdP attribuiranno l'eID alle persone interessate e daranno a queste ultime i mezzi d'accesso.

Considerato il cambiamento tecnologico e la molteplicità delle possibili soluzioni tecniche, la Confederazione non sarebbe tuttavia in grado di sviluppare e produrre direttamente i supporti per questi dati relativi all'identità confermati dallo Stato, supporti che potranno essere ad esempio telefoni cellulari, carte di credito o abbonamenti per i mezzi di trasporto pubblici. Il settore privato, più vicino agli utenti e alle tecnologie digitali necessarie, può svolgere meglio questa funzione e proporre soluzioni innovative. Lo Stato, tuttavia, avrà un ruolo importante anche in questo settore, sottoponendo gli IdP e i loro sistemi a una severa procedura di riconoscimento* e a controlli regolari. Il Servizio di riconoscimento* sarà incorporato nell'Organo direzione informatica della Confederazione (ODIC).

L'interazione funzionale tra Stato e privati crea le condizioni migliori per un utilizzo semplice e accessibile dell'eID da parte dell'Amministrazione, dei privati e delle imprese, garantendo nel contempo i mezzi per adattarsi con flessibilità all'evoluzione tecnologica in particolare per quanto riguarda la sicurezza.

1.2.3 Funzione dell'eID

Con un eID le persone fisiche possono registrarsi su un portale Internet (servizi che utilizzano l'eID*) e accedervi successivamente in modo sicuro e agevole. Per la registrazione presso un servizio che utilizza l'eID non occorre inserire manualmente i dati personali; con un eID rilasciato secondo la LSIE, tali dati saranno trasmessi automaticamente nel momento in cui il titolare dell'eID avrà acconsentito a tale trasmissione. Se successivamente visita di nuovo il portale, il titolare si identifica e

autentica con l'eID. Una volta registrato, l'eID viene riconosciuto e garantisce un accesso affidabile. L'eID costituisce dunque una delle basi per un utilizzo sicuro dei servizi in rete e offre al singolo più sicurezza e agio in Internet.

L'eID faciliterà i contatti con le autorità che sempre più spesso offrono i propri servizi anche mediante «sportelli virtuali». Oggi una persona viene identificata per lo più mediante dati di accesso, ad esempio nome utente e password monouso o liste di stralcio, che gli vengono recapitati per posta. La procedura spesso si conclude quando la persona rispedisce un modulo cartaceo. Questi passaggi possono essere saltati se l'identificazione è garantita tramite l'eID. In futuro le applicazioni dell'*e-government* potrebbero essere utilizzate completamente in rete.

Nell'ambito dei servizi *e-health*, l'eID integrerà in una prima fase gli strumenti d'identificazione rilasciati secondo la legge del 19 giugno 2015[4] (LCIP) e potrebbe sostituirli a medio termine. L'accesso del paziente alla sua cartella sarà possibile con un eID del livello di sicurezza corrispondente, ma ogni caso, sarà semplificato.

L'eID dà certezza ai servizi che utilizzano l'eID nel commercio elettronico per quanto riguarda l'identità del cliente. Visto che le confusioni sull'identità del cliente sono escluse, anche la verifica della solvibilità ne risulta facilitata. Visto che l'introduzione dell'eID consente anche di stabilire l'età degli utenti in maniera affidabile, è possibile tutelare meglio bambini e adolescenti da contenuti mediatici inadatti, da messaggi pregiudizievoli nell'ambito della comunicazione in rete e dal trattamento poco trasparente di dati personali. Grazie all'introduzione dell'eID e agli sviluppi tecnici ad essa connessi, sarebbe inoltre possibile attuare in modo semplice e sicuro interventi normativi per proteggere l'infanzia e la gioventù dai rischi dei media, obbligando ad esempio per legge i fornitori a trasmettere contenuti potenzialmente pericolosi solo a utenti la cui età è comprovata da un eID[5].

Il disegno non stabilisce su quale supporto vada gestito l'eID. Attualmente, i mezzi d'identificazione elettronica* più usati sono disponibili su cellulari (p. es. la Mobile ID), su carte o su supporti di memoria con chip integrati (la cosiddetta Integrated Circuit Card ICC o smartcard, p. es. SuisseID) oppure non richiedono alcun tipo di supporto materiale e possono essere impiegati via Internet con il nome utente, la password ed eventualmente il codice di transazione monouso inviato sullo smartphone (cfr. soluzioni dell'online banking). Molto probabilmente saranno proposti diversi supporti in base alle preferenze del singolo utente.

1.2.4 Rilascio dell'eID

Prima di poter rilasciare un eID secondo la LSIE, fedpol attribuisce il numero di registrazione eID ai dati d'identificazione personale del richiedente. Ogni persona ottiene un numero univoco di registrazione eID. Il rilascio comprende un'identifica-

4 RS **816.1**

5 Cfr. Giovani e media, futura impostazione della protezione dell'infanzia e della gioventù dai rischi dei media in Svizzera, rapporto del Consiglio federale del 13 mag. 2015 in adempimento della mozione Bischofberger 10.3466 «Protezione dei giovani dai rischi dei media e lotta alla cibercriminalità. Maggiore efficacia ed efficienza».

zione che, a seconda del livello di sicurezza, è effettuata per via elettronica o di persona. Il processo di rilascio prevede diverse fasi (cfr. art. 6 LSIE):

1. Chi desidera un eID ne richiede il rilascio a fedpol tramite un IdP. Quest'ultimo indirizza il richiedente a fedpol che ne verificherà l'identità in base a un documento valido (passaporto, CID o carta di soggiorno).
2. Fedpol chiede al richiedente altri dati identificativi personali (p. es. informazioni sui genitori o altri documenti d'identità) e li confronta con i dati d'identificazione personale contenuti nei registri di persone della Confederazione. Se i dati corrispondono, fedpol acconsenta al rilascio di un eID.
3. Il richiedente acconsente che fedpol trasmetta i suoi dati d'identificazione personale e il numero di registrazione eID all'IdP[6].
4. Fedpol trasmette all'IdP il numero di registrazione eID con i dati d'identificazione personale che corrispondono al livello di sicurezza dell'eID richiesto.
5. L'IdP attribuisce al richiedente un mezzo di autenticazione con un nome utente che permetta a quest'ultimo di identificarsi in rete. In funzione del livello di sicurezza, l'IdP esige che il richiedente si presenti di persona o virtualmente (p. es. nel quadro di una videoidentificazione).
6. Con il mezzo d'autenticazione l'IdP provvede ad attribuire correttamente all'eID il relativo numero di registrazione e attiva l'eID per l'utilizzo da parte del titolare.

L'intera procedura non dovrebbe durare più di un paio di minuti. I processi tecnici alla base sono definiti tramite standard e protocolli tecnici.

La LSIE disciplina anche come procedere con i mezzi d'identificazione elettronica rilasciati dall'IdP prima dell'entrata in vigore della legge. Per un periodo transitorio di due anni, l'ODIC riconosce su richiesta di un IdP i mezzi di identificazione elettronica che quest'ultimo ha rilasciato prima dell'entrata in vigore della legge come eID del livello di sicurezza basso. L'ODIC riconosce come eID del livello di sicurezza significativo i mezzi d'identificazione elettronica rilasciati da un IdP prima dell'entrata in vigore della LSIE se l'identificazione è stata effettuata in base a una procedura sottoposta per legge a regole precise e a vigilanza, e se tale procedura garantisce un livello di sicurezza simile a quello garantito dalla LSIE.

Anche i titolari di un certificato qualificato valido secondo l'articolo 2 lettera h FiEle possono chiedere all'IdP il rilascio di un eID del livello di sicurezza significativo.

In tutti e tre casi i presupposti personali di cui all'articolo 3 devono essere soddisfatti, il titolare deve aver acconsentito al rilascio dell'eID e i dati d'identificazione personale (numero della carta d'identità, cognome, nome e data di nascita) devono corrispondere alle informazioni contenute nel sistema d'informazione di cui all'articolo 24.

Il nostro Consiglio emana prescrizioni più dettagliate sul processo di rilascio a livello d'ordinanza.

6 Sui dati d'identificazione personale si rimanda al commento all'art. 5.

1.2.5 Livelli di sicurezza

Non tutte le transazioni esigono il medesimo livello di sicurezza. Nella prassi, requisiti di sicurezza troppo elevati possono essere fastidiosi, favorire manovre elusive e aumentare i costi, il che penalizza sia l'accettazione sia la sicurezza di un sistema di eID. Pertanto vengono riconosciuti sistemi di eID che offrono tre diversi livelli di sicurezza. I livelli si distinguono per i dati d'identità personale che contengono, il processo di rilascio, la gestione del sistema e l'impiego degli eID nonché eventualmente per altre misure di sicurezza tecniche od organizzative.

La legge definisce unicamente le possibili categorie di eID, ossia i livelli di sicurezza (cfr. art. 4 LSIE), ognuno dei quali offre un diverso grado di affidabilità. Il livello di sicurezza richiesto per il tipo di utilizzo va definito in atti normativi speciali o dai gestori privati di servizi che utilizzano l'eID. Per la formazione in rete (*e-education*), ad esempio, potrà essere scelto un livello di sicurezza diverso da quello prescritto per il voto elettronico o per le applicazioni di *e-health*.

La definizione e le caratteristiche dei livelli di sicurezza sono state riprese dal regolamento eIDAS e dalle relative disposizioni esecutive. Si distingue tra livello *basso, significativo* ed *elevato.* In linea di massima gli eId del livello di sicurezza *significativo* ed *elevato* possono essere impiegati anche per servizi che utilizzano l'eID per i quali si richiede un livello *basso* (compatibilità discendente).

La Confederazione mette a disposizione degli IdP, mediante interfaccia elettronica, i dati d'identificazione personale gestiti dallo Stato (per il livello di sicurezza *basso*: il numero di registrazione eID, il cognome ufficiale, i nomi e la data di nascita; per il livello di sicurezza *significativo*: anche il sesso, il luogo di nascita e la cittadinanza e per il livello di sicurezza *elevato* inoltre, anche l'immagine del viso). La prima trasmissione dei dati a un IdP o a un gestore di servizi che utilizzano l'eID richiede il consenso esplicito della persona interessata (cfr. art. 6 cpv. 2 lett. c LSIE).

Questo modello consente ad esempio di registrare in un primo momento un eID, tecnicamente adatto per livello di sicurezza *significativo,* a un livello *basso*, e di portarlo successivamente, mediante un incontro personale, a un livello di sicurezza più elevato, agevolando in tal modo l'accesso a sistemi di eID secondo la LSIE. Con il livello di sicurezza *basso*, l'accesso a eID riconosciuti rimane semplice, il che costituisce un fattore essenziale per il successo sul mercato dei gestori di sistemi di eID riconosciuti. Se lo desidera, una persona può inoltre possedere numerosi eID di diversi IdP con vari livelli di sicurezza fermo restando che il suo numero di registrazione eID resta lo stesso.

I tre livelli di sicurezza per i sistemi di eID secondo la LSIE sono definiti in modo da soddisfare i requisiti in materia di sicurezza vigenti per i tre livelli di garanzia fissati dall'articolo 8 del regolamento eIDAS e dalle pertinenti disposizioni d'esecuzione. Questi livelli corrispondono anche a quelli definiti dal NIST*[7] per le applicazioni di *e-government* negli Stati Uniti e costituiscono a tutt'oggi degli standard internazionali. Visto lo scopo cui è destinato, ogni livello si distinguerà per le specifiche tecniche, le norme e le procedure – incluse le verifiche tecniche – e sarà disciplinato

7 National Institute of Standards and Technology, U.S. Department of Commerce.

in dettaglio a livello di regolamenti, istruzioni e standard tecnici. In questo modo il disegno garantisce in linea di massima la compatibilità con i sistemi dell'UE e degli USA.

Livello di sicurezza *basso*

L'eID di livello di sicurezza *basso* ha lo scopo di ridurre il rischio di un'usurpazione o di un'alterazione dell'identità. La registrazione può essere effettuata in rete sulla base di un documento statale. A tale livello sono attribuiti solo pochi dati (cognome, nome, data di nascita e numero di registrazione eID; cfr. art. 5 cpv. 1 LSIE). L'utilizzo di questo tipo di eID richiede almeno un fattore di autenticazione ed è quindi comparabile a un badge d'accesso o a una soluzione di pagamento senza contatto per piccoli importi.

Livello di sicurezza *significativo*

Questo livello di sicurezza si riferisce a un mezzo di identificazione elettronica che fornisce un grado di affidabilità significativo riguardo all'identità pretesa o dichiarata di una persona. L'eID di questo livello ha lo scopo di ridurre notevolmente il rischio di usurpazione o alterazione dell'identità. La registrazione si effettua mediante un incontro personale presso l'IdP, una videoidentificazione basata su un documento d'identità rilasciato dallo Stato o un confronto dell'immagine del viso assegnata al documento. Nel livello di sicurezza *significativo,* oltra al nome e alla data di nascita si assegnano altri dati d'identificazione personale (sesso, luogo di nascita e nazionalità; cfr. art. 5 cpv. 2 LSIE). L'utilizzo dell'eID di questo livello di sicurezza richiede almeno un'autenticazione a due fattori ed è dunque comparabile alle soluzioni di norma utilizzate nel settore bancario (carte del conto o carte di credito con PIN, soluzioni di *e-banking*).

Livello di sicurezza *elevato*

L'eID di livello di sicurezza *elevato* ha lo scopo di impedire l'usurpazione o l'alterazione dell'identità. La registrazione si effettua mediante un incontro personale presso l'IdP o una videoidentificazione basata su un documento d'identità rilasciato dallo Stato. Inoltre si verifica l'autenticità del documento e almeno una caratteristica biometrica (validità del documento e immagine del viso o un'altra caratteristica biometrica di riconoscimento) in base a una fonte ufficiale. I mezzi utilizzati per l'identificazione nell'impiego dell'eID (mezzi di autenticazione) devono soddisfare requisiti molto elevati in materia di sicurezza tecnica. Il mezzo di autenticazione va consegnato personalmente al richiedente.

L'impiego dell'eID di questo livello di sicurezza richiede almeno un'autenticazione a due fattori di cui uno biometrico. Inoltre il mezzo di autenticazione deve poter fornire una prova diretta dell'autenticità del titolare, prova che può essere verificata dal servizio fiduciario. L'eID è paragonabile a uno *smartphone* con riconoscimento tramite l'impronta digitale, il viso o la voce integrato in un settore protetto e munito di certificato personale. L'autenticazione biometrica crea un collegamento ancora più stretto tra l'eID e il suo titolare. In caso di perdita del mezzo di autenticazione dell'eID, l'autenticazione biometrica protegge il titolare dall'esecuzione di transazioni abusive in suo nome.

Tenendo conto dell'usurpazione dell'identità, il titolare deve poter essere protetto da attacchi informatici sia diretti allo stesso mezzo d'identificazione dell'eID sia ad altri dispositivi tecnici eventualmente necessari per l'utilizzo del mezzo di autenticazione dell'eID, ma non previsti dal campo di applicazione della legge. Transazioni abusive in nome altrui devono poter essere impedite anche se i dispositivi tecnici sono stati manipolati mediante un attacco informatico o se da essi sono state ricavate informazioni. Per garantire questa protezione, il mezzo di autenticazione dell'eID del livello di sicurezza *elevato* deve dunque fondarsi su componenti particolarmente affidabili e conformi allo stato della tecnica.

1.2.6 Funzione dello Stato in relazione ai sistemi di eID

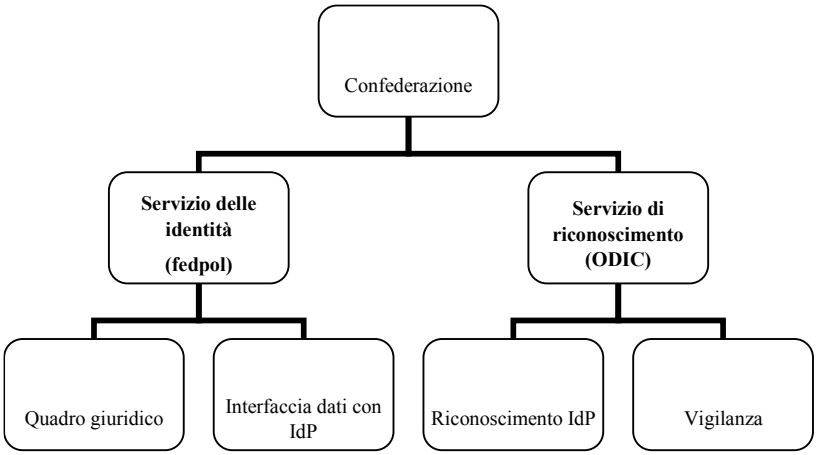
1.2.6.1 Panoramica

Un eID rilasciato in base alla LSIE conferma l'esistenza e l'identità di una persona fisica sulla base dei dati d'identificazione personale contenuti in registri tenuti e aggiornati dallo Stato. Per quanto riguarda l'esattezza dei dati sulle persone, lo Stato gode in effetti di particolare fiducia a tutti i livelli. Tale fiducia si fonda sul fatto che l'identificazione viene effettuata regolarmente presso un servizio statale in occasione del rilascio di un documento e anche grazie alla notifica ai registri statali di eventuali modifiche.

La Confederazione garantisce che i sistemi di eID secondo la LSIE siano affidabili e adempie a tal fine numerosi compiti nel settore degli eID:

1. elabora e aggiorna le basi legali creando trasparenza e sicurezza;
2. definisce gli standard nonché i requisiti in materia di sicurezza e interoperabilità da rispettare per gestire un sistema di eID;
3. gestisce una piattaforma di notifica per l'accertamento iniziale dell'identità del richiedente;
4. attribuisce il numero di registrazione eID a un'identità che ha verificato;
5. gestisce un'interfaccia elettronica tramite la quale gli IdP riconosciuti possono ottenere dati d'identificazione personale tenuti dallo Stato;
6. riconosce gli IdP e i loro sistemi di eID;
7. esercita la vigilanza sugli IdP riconosciuti e sui sistemi di eID; e
8. ritira, a determinate condizioni, il riconoscimento all'IdP e ai suoi sistemi di eID.

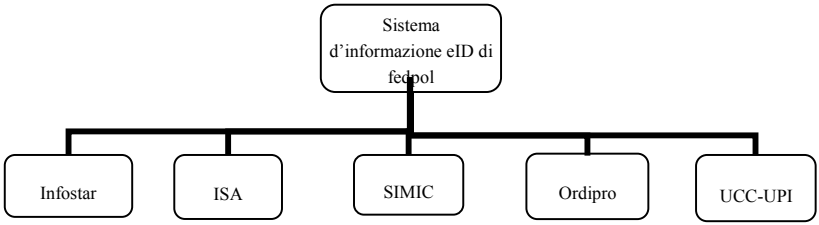
Questi compiti saranno assunti da due unità amministrative della Confederazione: fedpol (Servizio delle identità) e ODIC (Servizio di riconoscimento).



1.2.6.2 Registro con dati d'identificazione personale

Le autorità svizzere dei diversi livelli statali tengono numerosi registri contenenti dati d'identificazione personale, ad esempio i registri cantonali e comunali degli abitanti, il registro informatizzato dello stato civile (Infostar)* e il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC–UPI*[8]). Quest'ultimo è il registro centrale degli assicurati dell'AVS per l'identificazione personale nell'ambito dell'attribuzione e della gestione del numero AVS (NAVS13). Il sistema d'informazione sui documenti d'identità (ISA)*, inoltre, contiene dati d'identificazione personale dei cittadini svizzeri e funge da base per il rilascio di documenti (carta d'identità e passaporto). Le carte di soggiorno per stranieri, per contro, sono rilasciate sulla base dei dati del sistema d'informazione centrale sulla migrazione (SIMIC)* e la carta d'identità secondo la legislazione dello Stato ospite in base ai dati di Ordipro*.

I dati dei registri citati della Confederazione sono riuniti nel sistema d'informazione di fedpol di cui all'articolo 24:



8 UPI è l'acronimo di «Unique Person Identification».

1.2.6.3 Relazione tra il numero d'assicurato NAVS13 e il numero di registrazione eID

Il NAVS13 è un numero di identificazione personale univoco che, tuttavia, secondo la prassi attuale può essere impiegato soltanto nei settori per i quali vi è una base legale formale. La possibilità di utilizzare sistematicamente il NAVS13 cela il rischio del collegamento di record di dati d'identificazione tra singoli sistemi ed è pertanto ammessa unicamente alle condizioni di cui agli articoli 50*d* e 50*e* della legge federale del 20 dicembre 1946[9] sull'assicurazione per la vecchiaia e per i superstiti (LAVS). L'articolo 50*a* LAVS disciplina gli organi a cui possono essere comunicati i dati, in particolare il NAVS13, in deroga all'articolo 33 della legge federale del 6 ottobre 2000[10] sulla parte generale del diritto delle assicurazioni sociali (LPGA). Secondo l'articolo 50*e* capoverso 1 LAVS, l'utilizzazione sistematica del NAVS13, al di fuori delle assicurazioni sociali della Confederazione, è ammessa soltanto se lo prevede una legge federale e se sono definiti lo scopo d'utilizzazione e gli aventi diritto.

Il NAVS13 è spesso utilizzato nel quadro delle relazioni tra cittadini e servizi amministrativi. Se in futuro tale numero non dovesse poter essere rilevato e confermato attraverso fedpol (Servizio delle identità), andrebbero previste onerose soluzioni alternative, il che aumenterebbe notevolmente la complessità dei sistemi e ridurrebbe l'attrattiva dell'eID. Occorre pertanto autorizzare fedpol a utilizzare sistematicamente il NAVS13 soltanto per identificare le persone. Fedpol dovrebbe poter rendere accessibile il NAVS13 mediante una procedura di richiamo unicamente ai gestori di servizi che utilizzano l'eID e sono a loro volta autorizzati a utilizzare sistematicamente il NAVS13 (art. 8 cpv. 2 LSIE).

Gli IdP e gli altri privati vanno per contro esclusi dall'utilizzo sistematico del NAVS13. È pertanto necessario introdurre un numero d'identificazione supplementare che possa essere usato nello scambio di dati con privati e sia indipendente dal NAVS13, ossia il nuovo numero di registrazione eID utilizzato in particolare per collegare la persona con l'eID rilasciata. Visto che l'acquisizione di un eID è facoltativa e che non sussiste l'obbligo per gli aventi diritto di averne uno, il numero di registrazione eID non consente una copertura esaustiva e quindi non si presta come identificatore delle persone generale.

1.2.6.4 Ufficio federale di polizia (Servizio delle identità)

Quadro giuridico

In collaborazione con l'ODIC, fedpol emana le prescrizioni giuridiche, organizzative e tecniche. Definisce in particolare gli standard delle interfacce per l'interoperabilità* dei sistemi di eID e adegua i requisiti tecnici e organizzativi riguardanti il riconoscimento degli IdP e i sistemi di eID agli sviluppi tecnici, ai mutati requisiti di utilizzo e alle attuali esigenze in materia di sicurezza.

9 RS **831.10**
10 RS **830.1**

Pagine di login

Fedpol mette a disposizione un portale di login in Internet sul quale i richiedenti, indirizzati dagli IdP, devono comprovare la loro identità e nel contempo dare il proprio consenso alla trasmissione dei dati d'identificazione personale agli IdP.

Interfaccia

Fedpol mette a disposizione degli IdP riconosciuti i dati d'identificazione personale tramite un'interfaccia elettronica (art. 23 cpv. 1 LSIE). L'introduzione di un numero di registrazione eID consente di attribuire in modo univoco, duraturo e inconfutabile i dati d'identificazione personale a una persona e al suo eID. Questa interfaccia è accessibile solamente agli IdP riconosciuti per la prima identificazione e il regolare aggiornamento dei dati d'identificazione personale.

Fedpol è responsabile della gestione dell'interfaccia per la trasmissione dei dati d'identificazione personale. Funge da interlocutore per gli IdP riconosciuti e per i gestori dei registri statali connessi.

Fedpol ottiene i vari dati d'identificazione personale da diversi registri (art. 24 cpv. 3 LSIE). Il cognome della persona è confermato dai dati di Infostar, mentre per esempio il numero del documento d'identità proviene da ISA e l'immagine del volto da SIMIC. Se necessario per l'adempimento dei compiti assegnatigli dalla LSIE, fedpol può integrare i dati d'identificazione personali con metadati supplementari relativi all'ultimo aggiornamento dei dati nel sistema d'informazione di cui all'articolo 24 (art. 5 cpv. 4 LSIE).

Gli IdP sono tenuti ad aggiornare periodicamente i dati d'identificazione personale attribuiti a un numero di registrazione eID. A seconda del livello di sicurezza, gli IdP devono aggiornare i dati almeno annualmente (livello basso), trimestralmente (significativo) o settimanalmente (elevato) (art. 7 LSIE).

1.2.6.5 Organo direzione informatica della Confederazione ODIC (Servizio di riconoscimento)

Riconoscimento

Gli IdP che soddisfano i presupposti possono farsi riconoscere, assieme ai loro sistemi di eID, dall'ODIC a uno dei livelli di sicurezza previsti. Un IdP può gestire numerosi sistemi di eID a diversi livelli di sicurezza e farli riconoscere tutti o farne riconoscere solo alcuni. A tale scopo, il nostro Consiglio stabilisce i requisiti giuridici, organizzativi e tecnici per gli IdP, il cui adempimento è verificato dall'ODIC. Rinnovando il riconoscimento a intervalli regolari, la Confederazione fornisce un contributo fondamentale a soluzioni di eID sicure nel tempo.

L'ODIC pubblica un elenco degli IdP e dei sistemi di eID riconosciuti; in base a detto elenco, i gestori di servizi che utilizzano l'eID e le persone fisiche possono controllare concretamente lo statuto di un eID o del sistema di eID (art. 25 cpv. 2 D-LSIE). Gestisce un sistema d'informazione per il riconoscimento e la vigilanza degli IdP (art. 26 LSIE).

Vigilanza

L'ODIC esercita la vigilanza sugli IdP e sui sistemi di eID riconosciuti e reagisce in caso di non adempimento delle prescrizioni o di eventi relativi alla sicurezza informatica. A tal scopo esige e verifica le necessarie prove di conformità dagli IdP riconosciuti e le verifica. Può sottoporre un IdP a vigilanza e, a determinate condizioni, ritirare il riconoscimento (art. 19 LSIE).

1.2.6.6 Federazione Svizzera d'identità

La Federazione svizzera d'identità FSI offre una soluzione tecnica per semplificare le procedure di login nell'*e-government* e per la cooperazione in rete tra le autorità. La FSI è un progetto che rientra nelle linee guida della Strategia di e-Government Svizzera. L'organizzazione responsabile del progetto è la Segreteria di Stato per l'economia (SECO).

Sebbene sia possibile garantire l'interoperabilità anche senza la FSI, si era pensato di coinvolgerla nei sistemi di eID. Due studi indipendenti, uno del Politecnico di Zurigo[11] e l'altro dell'IBM Research Zurigo[12] hanno confermato questa ipotesi. Il nostro Consiglio intende impostare il sistema di eID nel modo più semplice possibile e omettere qualsiasi ruolo non assolutamente necessario. La funzione della FSI non è quindi oggetto del presente disegno.

1.3 Motivazione e valutazione della soluzione proposta

1.3.1 Soluzione Stato–privati

Già oggi sono in uso diversi eID: ad esempio per annunciarsi a un dispositivo mobile per navigare in Internet va di norma creato un profilo eID (p. es. AppleID, Google ID). Con quest'ultimo il titolare si può registrare in maniera semplice anche per altri servizi in rete. Questi eID, tuttavia, non essendo riconosciuti dallo Stato, e non ottenendo da quest'ultimo i dati d'identificazione personali, non possono assicurare il particolare grado di affidabilità che la LSIE conferisce agli eID rilasciati secondo la LSIE.

Molti servizi in Internet dipendono da un'identificazione univoca e affidabile che, mediante procedure standardizzate, garantisce che l'identità del titolare di un eID è stata verificata. Questo vale soprattutto per i servizi statali in rete dell'*e-government*. Per questo motivo diversi Stati rilasciano propri eID secondo soluzioni gestite completamente dal settore pubblico o da privati riconosciuti. Dalle esperienze raccolte finora emerge tuttavia che le soluzioni puramente statali non sono accettate dai

11 Basin, D., Sasse, R., Interoperable, State-approved Electronic Identities, 26 gen. 2018, consultabile sul sito dell'UFG: www.bj.admin.ch > Stato & Cittadino > Progetti di legislazione in corso > Legge sull'eID.

12 Camenisch, J., Dubovitskaya, M., Evaluation Report, Proof of Concept Interoperabilität E-ID, IBM Research, Zurigo, 31 gen. 2018, consultabile sul sito dell'UFG: www.bj.admin.ch > Stato & Cittadini > Progetti di legislazione in corso > Legge sull'eID.

cittadini e comportano per l'ente pubblico un onere elevato sotto il profilo degli investimenti e sotto l'aspetto operativo. Spesso i sistemi puramente statali riescono a tenere il passo con gli sviluppi tecnologici soltanto con grandi difficoltà e al prezzo di adeguamenti costosi. Inoltre le procedure possono essere molto gravose a causa delle prescrizioni in materia di acquisti e di eventuali adeguamenti delle basi legali. Di conseguenza, spesso le soluzioni statali non raggiungono il livello di diffusione auspicato e sono impiegate in parte per obbligo e solamente una volta all'anno ai fini della dichiarazione fiscale. Ulteriori osservazioni sullo sviluppo degli eID rilasciati dallo Stato sono illustrate al numero 1.5.

Proponendo queste soluzioni la Confederazione crea condizioni quadro affidabili e garanti di sicurezza, che attua nel quadro di procedure di riconoscimento e di vigilanza. Non deve tuttavia né occuparsi dello sviluppo degli aspetti tecnici degli eID né investire nella loro realizzazione. L'attuazione tecnica e la commercializzazione degli eID spetta agli attori privati.

Nel frattempo sono disponibili sul mercato anche diversi eID affidabili offerti da IdP svizzeri la cui accettazione è in continua crescita. Se soddisfano le condizioni questi sistemi di eID possono essere rafforzati mediante il riconoscimento dell'IdP in oggetto ed essere impiegati anche nell'ambito dell'*e-government*. Inoltre il disegno offre l'accesso a questo mercato anche ad altri IdP che hanno completato la procedura di riconoscimento.

I requisiti posti ai sistemi di eID secondo la LSIE sono concepiti in modo da adempiere il più possibile le condizioni per la notifica di sistemi di eID ai sensi del regolamento eIDAS.

1.3.2 Procedura di riconoscimento

Oggi la Confederazione può avvalersi di diversi modelli per disciplinare la procedura di riconoscimento. Nell'ambito della *firma elettronica*, la procedura di riconoscimento è effettuata da un servizio privato accreditato secondo il pertinente diritto per il riconoscimento e la sorveglianza di offerenti di servizi di certificazione. Anche in questo caso l'accreditamento è rilasciato da un servizio designato dal nostro Consiglio.

Nell'ambito delle *piattaforme per la trasmissione sicura*, per contro, è un'unità amministrativa del DFGP, ossia l'Ufficio federale di giustizia (UFG), a ricevere ed esaminare le domande di riconoscimento. L'UFG valuta in dettaglio, secondo le regole del diritto in materia di accreditamento, soltanto il rispetto degli standard tecnici. Le condizioni e la procedura per il riconoscimento delle piattaforme per la trasmissione sicura sono rette dall'ordinanza del 16 settembre 2014[13] sul riconoscimento di piattaforme di trasmissione. Le prescrizioni tecniche e la definizione esatta degli standard più attuali da rispettare figurano in allegato a questa ordinanza e sono pubblicate sul sito Internet dell'UFG. In tal modo si garantisce che si tenga conto per tempo degli sviluppi tecnici nel campo della trasmissione sicura.

13 RS **272.11**

Questo modo di procedere ha dato buoni risultati. La *procedura di riconoscimento degli IdP* s'ispira pertanto a quella adottata per le piattaforme di trasmissione: secondo il presente disegno, l'ODIC, preposto al riconoscimento, è competente per il ricevimento e l'esame delle domande di riconoscimento degli IdP e dei sistemi di eID, per cui assume la medesima funzione svolta dall'UFG nell'ambito del riconoscimento delle piattaforme di trasmissione. In una nuova ordinanza dipartimentale si prevede di emanare e aggiornare le prescrizioni tecniche e definire gli standard da rispettare. Tali parametri saranno armonizzati con le regole vigenti nel settore della firma elettronica, dell'*e-health* e delle piattaforme di trasmissione, cosicché gli IdP riconosciuti potranno beneficiare di sinergie nell'ambito delle certificazioni.

La Confederazione garantisce una parte della sua funzione di vigilanza attraverso il riconoscimento degli IdP e il periodico rinnovo di tale riconoscimento. In questo modo l'adattamento allo sviluppo tecnico in materia di sicurezza avviene tempestivamente. Sono fissate precise condizioni in materia di protezione dei dati il cui rispetto è regolarmente controllato.

La LSIE prevede determinate misure che garantiscono la massima continuità possibile del sistema di eID. Se, ad esempio, l'IdP non ottenesse o non chiedesse più il rinnovo del riconoscimento per il rilascio di eID del livello di sicurezza significativo o elevato, il sistema di eID potrà essere assunto da un altro IdP o, se non vi è un IdP interessato all'assunzione, dalla Confederazione (gratuitamente). I titolari dell'eID, gli IdP e i gestori di servizi che utilizzano l'eID devono potersi fidare dei sistemi di eID allestiti. Il rilevamento del sistema di eID da parte di un altro IdP o dalla Confederazione permetterà dunque di assicurare le prestazioni senza interruzione.

1.3.3 Consultazione e rielaborazione dell'avamprogetto

Sono stati invitati a partecipare alla consultazione i Cantoni, i partiti rappresentati in Parlamento, le associazioni mantello nazionali dei Comuni, delle città, delle regioni di montagna e dell'economia, nonché altre organizzazioni interessate.

Dei 65 destinatari invitati a esprimere il proprio parere hanno risposto in 48. Sono pervenuti i pareri di 26 Cantoni, 8 partiti e 54 tra organizzazioni e altri partecipanti; in totale sono giunti 88 pareri. Sono infatti pervenuti 40 pareri spontanei, provenienti da associazioni economiche, in particolare dai settori delle TIC (tecnologie dell'informazione e della comunicazione), dei servizi finanziari, dell'*e-government* dell'*e-health*, nonché da privati.

In base ai risultati della consultazione, l'elenco dei dati d'identificazione personale è stato notevolmente ridotto; in particolare il NAVS13 non compare più come attributo dell'eID. Il numero di registrazione eID viene generato in modo casuale e quindi non è riconducibile al NAVS13. Secondo l'articolo 24, il confronto tra il numero di registrazione eID e il NAVS13 ha luogo nel sistema d'informazione.

Molti pareri hanno chiesto l'introduzione di un eID per le persone giuridiche, il che conferma l'esigenza di poter identificare queste persone in Internet in modo sicuro. Tuttavia, visto che le persone giuridiche agiscono soltanto attraverso i loro organi, ossia, ad esempio, attraverso le persone fisiche registrate nel registro di commercio

come aventi diritto di firma, non è necessario introdurre un eID per le persone giuridiche. Per attribuire in modo sicuro un sito Internet a una persona giuridica, esistono peraltro già oggi possibilità di autenticazione sicura, ad esempio mediante i certificati secondo la FiEle. Del resto, il numero unico d'identificazione delle imprese (UID), attribuito a ogni impresa in Svizzera, ha segnatamente l'obiettivo di alleggerire l'onere amministrativo di identificazione delle imprese e aumentare l'efficienza dell'amministrazione in tale ambito. L'obiettivo dell'eID, invece, non è volto soltanto ad agevolare l'identificazione degli aventi diritto, ma anche a permettere al titolare di interagire nel mondo virtuale e di approfittare di un'ampia gamma di servizi.

Su iniziativa dei partecipanti alla consultazione, è stata valutata l'opportunità di istituire degli intermediari d'identità, i cosiddetti *identity brokers*. I due studi citati, quello del Politecnico di Zurigo e quello dell'IBM Research, hanno però dimostrato che l'interoperabilità dei sistemi di eID può essere assicurata attraverso protocolli e non richiede l'intervento di un simile intermediario. Di conseguenza, il presente disegno non disciplina l'attività degli *identity broker*. Nel quadro dei loro sistemi di eID, gli IdP possono tuttavia ricorrere alle prestazioni di simili intermediari, a condizione che questi ultimi siano stati riconosciuti dal Servizio di riconoscimento.

1.4 Compatibilità tra i compiti e le finanze

1.4.1 Identificazione sicura in rete

Diversi servizi della Confederazione potranno presumibilmente ricorrere all'eID, in particolare allorquando persone fisiche devono identificarsi in maniera sicura per entrare in contatto diretto con l'Amministrazione federale e con servizi statali. Con l'eID, i più svariati sistemi d'informazione dispongono di una soluzione adeguata per l'identificazione e l'autenticazione sicure delle persone, ad esempio nel quadro dell'ordinazione in rete di estratti del casellario giudiziale o del registro delle esecuzioni oppure dell'inserimento di dati in sistemi d'informazione agricoli o veterinari in rete.

L'eID può inoltre essere impiegato per svariati scopi d'identificazione e autenticazione anche da impiegati dell'Amministrazione federale. In tal modo costituisce una componente importante per i progetti che la Confederazione sta sviluppando in materia di IAM (Identity and Access Management).

Il fabbisogno di risorse e il finanziamento sono stati illustrati ai numeri 1.4.3 e 3.1. L'onere supplementare si limiterà ad adeguamenti delle soluzioni informatiche e all'acquisizione dei servizi degli IdP, ma anche in questo ambito sarà possibile risparmiare semplificando i processi.

1.4.2 Nuovi compiti

La legge sull'eID comporta nuovi compiti per l'Amministrazione federale. Fedpol dovrà allestire un sistema d'informazione provvisto di un'interfaccia per la trasmissione dei dati d'identificazione personale e l'ODIC dovrà riconoscere gli IDP e vigilare su di essi (cfr. n. 1.2.6).

Fedpol ha i seguenti compiti:

a. verifica l'identità del richiedente;

b. gestisce e mantiene l'infrastruttura informatica che gli è necessaria (pagina di login per il richiedente, interfaccia verso gli IdP e collegamento delle banche dati della Confederazione come ISA, Infostar, ecc.);

c. fornisce supporto tecnico alle banche dati della Confederazione coinvolte; e

d. fornisce supporto tecnico agli IdP riconosciuti.

Fedpol è responsabile dell'attività normativa nel settore dei documenti d'identità e ha elaborato i piani eID. La maggior parte delle banche dati che fungono da fonte per la conferma dei dati d'identificazione personale è gestita presso il DFGP.

L'ODIC ha i seguenti compiti:

a. riconosce gli IdP;

b. controlla gli IdP riconosciuti e vigila su di essi,

c. gestisce e pubblica l'elenco degli IdP riconosciuti;

d. elabora e aggiorna le prescrizioni tecniche e organizzative per il riconoscimento di IdP;

e. acquisisce informazioni sugli sviluppi tecnologici attuali nel settore dell'eID e sulle pertinenti questioni in materia di sicurezza informatica

Oltre alle funzioni di riconoscimento e vigilanza, l'ODIC assume pure quelle dell'organismo di vigilanza secondo il regolamento eIDAS. L'ODIC svolge già all'interno della Confederazione altre analoghe funzioni di vigilanza.

Sono fatte salve le competenze dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) secondo la legge federale del 19 giugno 1992[14] sulla protezione dei dati (LPD).

1.4.3 Finanziamento

1.4.3.1 Prestazioni preliminari della Confederazione

Il finanziamento delle spese di progetto pari a 6 920 000 franchi è già assicurato dai mezzi a disposizione del DFGP (comprese le quote dei mezzi centrali TIC e la partecipazione di e–Government Svizzera).

14 RS **235.1**

In base ai risultati della consultazione è necessario istituire e implementare un servizio supplementare per consultare il numero d'assicurato. A tal fine occorrono fondi supplementari pari a 750 000 franchi, da richiedere a titolo di credito aggiuntivo. Occorre inoltre sviluppare e garantire la manutenzione del simulatore, il che cagiona una spesa supplementare pari a 230 000 franchi. Per il biennio 2018–2020 si prevedono quindi costi supplementari pari a 980 000 franchi, anch'essi da richiedere a titolo di credito aggiuntivo. Visto che 100 000 franchi provengono dai mezzi di e–Government Svizzera occorre chiedere complessivamente 880 000 franchi dai mezzi centrali TIC.

Le spese per terzi saranno finanziate con il credito V0224.00 «Rinnovo del passaporto e della carta d'identità svizzeri» di fedpol, pari a 19,6 milioni di franchi.

1.4.3.2 Finanziamento mediante emolumenti

Per le prestazioni che la Confederazione fornisce all'IdP sono stati esaminati diversi modelli di finanziamento. Sono stati respinti sia il modello *prepaid*, secondo cui l'IdP versa alla Confederazione un emolumento che copra il più possibile i costi, senza tuttavia la certezza che la diffusione degli eID sia così rapida da generare entrate sufficienti, sia il modello che prevede una verifica gratuita dei dati confermati dopo la loro prima trasmissione che genererebbe notevoli perdite per la Confederazione. Si propone dunque un modello *pay-per-use* finanziato mediante emolumenti.

Per questo modello sarà emanata un'ordinanza sugli emolumenti. Per accelerare la diffusione degli eID, la prima trasmissione di dati d'identificazione personale in occasione dell'allestimento dell'eID, è gratuita a condizione che l'ottenimento dell'eID sia pure gratuito per il richiedente. Per ogni trasmissione successiva di dati d'identificazione personale è invece riscosso un emolumento moderato dell'ordine di qualche decina di centesimi, che sarà stabilito a livello di ordinanza. A seconda della diffusione di eID secondo la LSIE, in particolare dei livelli *significativo* ed *elevato*, questo modello permetterà di generare entrate sufficienti per coprire i costi.

1.4.3.3 Indennità versate dai gestori di servizi che utilizzano l'eID

Saranno in primo luogo i gestori di servizi che utilizzano l'eID, che si tratti di imprese private o di autorità, a beneficiare dell'utilizzo di eID, che consentirà loro di semplificare le procedure e dunque ridurre i costi (p. es. meno sportelli, meno carta e meno passaggi da un sistema a un altro, velocizzazione delle procedure, modelli di transazione innovativi, nessuna soluzione propria di eID). Essi dovranno quindi essere disposti a indennizzare l'applicazione di sistemi di eID. Spetterà al mercato stabilire le modalità di fatturazione della prestazione.

1.4.4 Osservazione in merito agli acquisti pubblici

Autorità in veste di gestori di servizi che utilizzano l'eID

L'autorità che offre un servizio che utilizza un eID rappresenta un gestore di servizi che utilizza l'eID secondo la LSIE e deve concludere con almeno un IdP un accordo sull'utilizzo di un sistema di eID.

Un'applicazione di *e-government* gestita in esecuzione di un compito d'interesse pubblico necessita dei servizi d'identificazione. L'autorità sottostà al diritto in materia di acquisti pubblici. I servizi d'identificazione costituiscono prestazioni informatiche che sottostanno dunque al diritto in materia di acquisti pubblici. Con la LSIE si crea un mercato per questo tipo di prestazioni fornite dietro compenso.

Per i servizi dell'IdP occorre quindi eseguire una procedura d'acquisto pubblico conformemente alle disposizioni applicabili in materia (legge federale del 16 dicembre 1994[15] sugli acquisti pubblici [LAPub] o diritto cantonale) a meno che il nostro Consiglio non designi un'unità amministrativa che gestisca un sistema di eID per le esigenze delle autorità (art. 10 LSIE).

Riconoscimento degli IdP

Il riconoscimento degli IdP non costituisce per contro una procedura d'acquisto, ma un atto di polizia economica che si fonda sull'articolo 95 capoverso 1 della Costituzione federale (Cost.)[16] (cfr. n. 5.1).

Il riconoscimento non ha per effetto una regolazione economica: il numero dei riconoscimenti non è limitato e gli IdP riconosciuti non beneficiano di alcun diritto d'esclusività. Gli IdP non riconosciuti possono rilasciare mezzi d'identificazione elettronica che però non sono eID secondo la LSIE. Un riconoscimento viene rilasciato e rinnovato a condizione che i relativi presupposti (art. 13 cpv. 2 LSIE) siano soddisfatti e le prescrizioni tecniche e organizzative siano rispettate.

1.5 Mezzi d'identificazione elettronica statali nel contesto internazionale, in particolare europeo

1.5.1 Premessa

La Svizzera non è l'unico Paese a introdurre un mezzo d'identificazione elettronico. Questo tema è all'ordine del giorno di numerosi Stati da oltre 15 anni. In considerazione della natura globale dei servizi in rete è importante che un mezzo d'identificazione elettronica riconosciuto dallo Stato sia pianificato, dal punto di vista progettuale, tecnico e giuridico, in modo da poter poi essere impiegato a livello internazionale, soprattutto europeo. Il regolamento eIDAS e i pertinenti standard tecnici specificano condizioni quadro che garantiscono l'interoperabilità dei singoli sistemi dei diversi Paesi. Il progetto dei sistemi di eID secondo la LSIE si orienta a

15 RS **172.056.1**
16 RS **101**

queste prescrizioni internazionali cosicché gli eID svizzeri potrebbero essere usati anche nel contesto internazionale.

Il quadro giuridico presentato in questa sede per il riconoscimento di sistemi di eID e di IdP è strutturato in modo da consentire un successivo riconoscimento reciproco dei sistemi di eID tra la Svizzera e l'UE (in base al regolamento eIDAS), singoli Stati membri o Stati terzi. Per l'attuazione sarebbero necessari accordi internazionali.

1.5.2 Sviluppi degli ultimi quindici anni

In una prima fase la maggior parte degli Stati pensava di sviluppare un eID ispirato alle carte d'identità esistenti. Le domande che ci si era posti in un primo momento concernevano soprattutto aspetti tecnici. Negli ultimi quindici anni molti Stati europei hanno introdotto un eID connesso con la carta d'identità come elemento centrale di un sistema di eID nazionale. Apripista è stata la Finlandia, nel 1999, seguita da Estonia, Belgio, Spagna e Portogallo. La Germania ha introdotto un documento personale elettronico nel 2010. Inoltre negli ultimi anni alcuni Paesi del Vicino Oriente e dell'Asia hanno rilasciato nuove carte d'identità statali con funzione di eID. L'avvio di progetti di eID era spesso dettato dalla volontà di non restare assolutamente al palo nel raffronto internazionale. Né gli Stati Uniti né il Regno Unito hanno invece introdotto un eID statale, confermando il loro generale scetticismo nei confronti delle carte d'identità, diversi Stati federali americani invece hanno rilasciato patenti di guida elettroniche.

Le prime soluzioni di eID erano ispirate ad esempio alle *smartcard* con chip basati sul contatto, fondate essenzialmente sulla tecnologia delle carte per la firma elettronica. Esempi di questo tipo sono l'eID finlandese, quello estone, quello belga e sostanzialmente anche quello svizzero.

Un'altra soluzione alternativa diffusa è scaturita dagli sforzi dell'industria europea dei microprocessori per definire un insieme di standard che consentisse la creazione di una carta d'identità europea (*European Citizen Card*, ECC). La Svezia, Monaco, la Lettonia, la Finlandia (2ª ed.) e i Paesi Bassi hanno queste carte d'identità contenenti la funzione ePass secondo l'ICAO nonché una funzione, supportata dalla precedente, per l'identificazione elettronica in rete. Lo standard ECC non ha mai potuto affermarsi completamente. Tuttavia un suo utilizzo si è imposto in particolare nel caso dei documenti per stranieri (documenti di soggiorno per cittadini di Stati terzi) negli Stati membri dell'UE, poiché in questo settore – a differenza di quello delle carte d'identità – l'UE ha facoltà di legiferare. Anche la carta di soggiorno biometrica svizzera soddisfa questo standard.

Un passo importante in quest'evoluzione è costituito dal documento personale elettronico (*elektronischer Personalausweis*, ePA), introdotto dalla Germania nel 2010, che contiene sostanzialmente le componenti summenzionate, ma è stato migliorato in alcuni aspetti e in particolare integrato con numerose procedure tecniche complesse volte a rafforzare la protezione della personalità. I fornitori di servizi (*service provider*, gestori di servizi che utilizzano l'eID) devono ad esempio essere

registrati dallo Stato per acquisire determinati attributi e farsi autentificare per utilizzare il documento.

Negli ultimi anni l'ePA tedesco è divenuto in un certo senso la misura per i nuovi eID statali a livello mondiale. Nel frattempo, circa la metà della popolazione in Germania dispone dell'ePA, ma soltanto nel 3 per cento circa delle carte la funzione eID è stata attivata e anche utilizzata. Non è quindi ancora chiaro se la funzione eID sarà effettivamente impiegata su vasta scala. È un dato di fatto che l'ePA è poco accettato in particolare dall'economia privata e dai cittadini in quanto, pur essendo molto sicuro, è troppo complicato per l'utilizzo quotidiano e troppo caro. I cittadini devono acquistare e impiegare componenti infrastrutturali come lettori e programmi. Lo Stato, inoltre, deve costantemente sviluppare e distribuire modifiche e aggiornamenti di queste componenti, il che rende la gestione molto costosa.

Il 22 agosto 2017 la Repubblica federale di Germania ha notificato alla Commissione europea il proprio regime di identificazione elettronica del documento d'identità nazionale e del titolo di soggiorno con il livello di garanzia più elevato possibile secondo il regolamento eIDAS. La notifica è stata pubblicata il 26 settembre 2017 sulla Gazzetta ufficiale dell'UE. Oltre alla Germania anche Danimarca, Francia, Gran Bretagna, Italia (notifica preventiva) e Spagna si stanno accingendo a notificare all'UE i loro servizi nazionali di eID.

Anche altre soluzioni di eID che richiedono ai cittadini l'acquisto di componenti infrastrutturali supplementari incontrano problemi di accettazione. L'eID classica, basata su una carta, non è riuscita a imporsi in nessuno Stato; si è invece constatato che diverse soluzioni flessibili su *smartphone* godono di un'accettanza migliore. Anche in Estonia, che ha un ruolo guida in materia, attualmente l'eID è impiegata principalmente su *smartphone*.

1.5.3 Soluzioni alternative

Negli ultimi anni, le riflessioni sulla promozione statale dell'eID hanno preso una nuova direzione, soprattutto perché il ciclo di produzione di una carta d'identità statale è molto lungo rispetto alla rapidità dell'evoluzione del mondo digitale e perché spesso una soluzione statale non tiene sufficientemente conto delle esigenze sempre più diversificate degli utenti

Ispirandosi al progetto statunitense di sviluppo comune di un ecosistema d'identità elettronica (*identity ecosystem*[17]), in numerosi Paesi si è cominciato a riflettere, coinvolgendo tutti gli attori, sulle possibili basi di un'architettura efficace per l'intero ecosistema nazionale e internazionale in materia di eID e sul contributo che potrebbe essere fornito dallo Stato. I singoli Paesi sono giunti a conclusioni differenti. Negli Stati Uniti lo Stato si limita a organizzare e promuovere l'ecosistema di eID. Non fornisce servizi, ma influisce massicciamente sul mercato in quanto utilizza eID per i suoi collaboratori e gestisce servizi che utilizzano l'eID nel quadro di offerte di *e-government*. Negli Stati Uniti sono pure state elaborate importanti basi progettuali per una gestione delle identità interoperabile e affidabile.

17 National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem.

In Svezia, Norvegia e Danimarca, le banche sono divenute i più importanti offerenti di eID per tutti i settori, dato che già da tempo le propongono per le proprie prestazioni. Requisiti minimi definiti dallo Stato garantiscono la qualità e l'interoperabilità dei sistemi. Questi eID sono accettati da enti statali e possono essere utilizzati nel quadro delle applicazioni di *e-government*.

Nel citato regolamento eIDAS, l'UE ha seguito questa evoluzione e, ai fini del riconoscimento reciproco, accetta non solo gli eID rilasciati dallo Stato, ma anche i sistemi di eID gestiti dall'economia privata e riconosciuti a livello statale.

1.5.4 Conseguenze per la Svizzera

I sistemi statali che si basano su una connessione stretta tra l'eID e un documento d'identità convenzionale, ad esempio mediante un chip sul documento, riescono solo con grandi difficoltà e ingenti costi a tenere il passo con l'evoluzione delle tecnologie. Alla luce delle esperienze maturate nei Paesi limitrofi, per la Svizzera s'impone un'altra soluzione.

La soluzione proposta combina la fiducia conferita dallo Stato attraverso il riconoscimento e la vigilanza con il *know how* tecnologico e il dinamismo dell'iniziativa privata. Dispensa inoltre la Confederazione dalla presa di decisioni difficili relative a complessi processi d'innovazione tecnologica e la sgrava al contempo da ingenti costi di sviluppo e implementazione. Offre inoltre il margine necessario per trovare soluzioni innovative flessibili e adeguate alle sue esigenze. Il ruolo della Confederazione si limita alla definizione delle condizioni quadro necessarie e all'emanazione di prescrizioni da attuare nel quadro del riconoscimento e della vigilanza.

Da un raffronto tra il piano per il riconoscimento di mezzi d'identificazione elettronica, realizzato nel disegno, e gli sviluppi, le esperienze e le riflessioni attuali constatati nel contesto internazionale risulta quanto segue:

- la Svizzera tiene conto delle esperienze degli ultimi 15 anni e con il suo piano di un eID riconosciuto ha intrapreso un percorso considerato paradigmatico da più parti;
- il piano svizzero garantisce un sistema di eID sicuro attraverso prescrizioni precise, una procedura di riconoscimento e la vigilanza statale;
- il piano svizzero è sostanzialmente conforme con l'UE e il regolamento eIDAS;
- il piano svizzero tiene conto delle basi teoriche e tecniche più recenti per una gestione dell'identità in ecosistemi digitali, ad esempio quelle elaborate dal NIST;
- il piano svizzero è molto flessibile e può pertanto tenere il passo con sviluppi tecnologici ed economici anche di ampia portata.

1.5.5 Regolamento eIDAS e requisiti di compatibilità

Se è importante poter utilizzare in tutto il mondo il classico documento d'identità con dati visibili come documento di viaggio e mezzo d'identificazione all'estero, lo è ancor più per l'eID. Anche se non viene utilizzato come documento di viaggio, l'eID è impiegato in Internet, che per natura non ha frontiere. Questo aspetto è particolarmente importante per l'UE, che si è impegnata a realizzare un mercato interno europeo uniforme e privo di confini.

Il 23 luglio 2014 l'UE ha emanato il regolamento eIDAS che, oltre a disciplinare il settore dei prestatori della firma elettronica e di altri servizi fiduciari, nonché la loro certificazione, comprende, quale nuovo tema, la notifica e il riconoscimento reciproco di regimi nazionali per l'identificazione elettronica. Tutti gli Stati membri sono obbligati ad accettare, laddove richiedono un eID per l'accesso a servizi pubblici, anche un eID straniero appartenente a un regime notificato (art. 6 del regolamento eIDAS). Questo obbligo vale anche per uno Stato membro che non dispone di un regime di eID notificato.

Quali requisiti deve soddisfare un sistema di eID svizzero per essere conforme al regolamento eIDAS e poter essere successivamente notificato? Ovviamente, la Svizzera non è giuridicamente vincolata a riprendere il regolamento eIDAS. In considerazione degli stretti rapporti commerciali e sociali che intrattiene con la maggior parte degli Stati membri dell'UE, occorre presuppore che la Svizzera abbia tutto l'interesse a essere prima o poi integrata nel sistema europeo per l'interoperabilità dei sistemi d'identificazione elettronici. Anche se al momento non è ancora chiaro se, quando e come la Svizzera sarà integrata in questo sistema mediante un accordo bilaterale, in linea di massima il sistema di eID elvetico deve essere concepito sin dall'inizio in modo da poter essere notificato.

Il presente disegno di legge crea tra l'altro un quadro giuridico e di standardizzazione per il riconoscimento di sistemi di eID e degli IdP strutturato in modo da preservare la possibilità di un riconoscimento reciproco successivo tra il sistema svizzero di eID e i sistemi di eID notificati secondo il regolamento eIDAS, i sistemi di eID di singoli Stati membri dell'UE o di Stati terzi.

1.6 Attuazione

Il presente disegno regola in generale i principi e i requisiti posti al rilascio e all'utilizzo dei mezzi d'identificazione elettronica secondo la LSIE. Per poter essere attuate, le disposizioni proposte vanno precisate in ordinanze emanate dal nostro Collegio e dal dipartimento. I particolare vanno disciplinati gli aspetti seguenti:

- le procedure che permettono di verificare i documenti d'identità dei cittadini svizzeri e i documenti di legittimazione nonché l'identità dei cittadini stranieri;
- i vari livelli di sicurezza e in particolare i requisiti minimi per l'identificazione, tenuto conto dell'attuale stato della tecnica;
- la procedura di rilascio;

- il blocco e la revoca di un eID;
- gli obblighi di diligenza dei titolari di un eID;
- le condizioni del riconoscimento;
- le diverse comunicazioni previste dalla legge;
- le norme tecniche per assicurare l'interoperabilità e le interfacce;
- la procedura di ritiro del riconoscimento;
- le norme e i protocolli tecnici applicabili alla trasmissione dei dati e la procedura da seguire nel caso in cui diversi registri di persone trasmettessero dati contraddittori;
- le misure tecniche e organizzative da adottare per garantire il trattamento e la trasmissione sicuri dei dati d'identificazione personale;
- la procedura di rilascio dell'eID in base alla disposizione transitoria.

Il nostro Consiglio disciplinerà, sempre a livello di ordinanza, la riscossione di emolumenti conformemente all'articolo 46*a* della legge del 21 marzo 1997[18] sull'organizzazione del Governo e dell'Amministrazione (LOGA).

Infine il disegno s'ispira alle misure tecniche e organizzative applicabili ai settori della firma elettronica e della cartella informatizzata del paziente. Le disposizioni esecutive del progetto di legge (ordinanze o direttive) terranno conto di questi standard.

1.7 Interventi parlamentari

Finora l'eID è stato oggetto di un intervento parlamentare trasmesso al nostro Consiglio:

- mozione del Gruppo liberale-radicale 17.3083 «Digitalizzazione. Un'identità elettronica per ridurre la burocrazia a livello nazionale». Il nostro Consiglio ne ha raccomandato l'accettazione. La mozione chiede che il progetto sia attuato in via prioritaria tenendo conto in particolare dell'interoperabilità e della definizione e del controllo delle norme di sicurezza. Il presente messaggio soddisfa le richieste della mozione adottata dal Consiglio nazionale il 20 settembre 2017 e dal Consiglio degli Stati il 28 febbraio 2018.

Con il presente messaggio, il nostro Consiglio propone di togliere dal ruolo l'intervento parlamentare in oggetto.

18 RS **172.010**

2 Commento ai singoli articoli

2.1 Struttura

La prima sezione del disegno contiene le disposizioni generali e le definizioni. La seconda disciplina il rilascio dell'eID: i presupposti personali per i richiedenti, i livelli di sicurezza, il processo di rilascio, i dati d'identificazione personale e il loro aggiornamento, l'utilizzo sistematico del numero d'assicurato per lo scambio di dati, il trattamento e la conservazione dei dati, il sistema di eID sussidiario della Confederazione nonché il blocco e la revoca. La terza sezione illustra gli obblighi dei titolari di eID, la quarta disciplina i requisiti posti agli IdP, i loro obblighi, la procedura di riconoscimento, la trasmissione dei dati, l'accessibilità degli eID, l'interoperabilità nonché le misure di vigilanza e il ritiro del riconoscimento. I requisiti dei gestori di servizi che utilizzano l'eID sono definiti nella quinta sezione. Le sezioni sesta e settima illustrano l'organizzazione e i compiti di fedpol (Servizio delle identità) e dell'ODIC (Servizio di riconoscimento). L'ottava sezione regola la competenza per stabilire gli emolumenti e la nona la responsabilità civile. La decima sezione è dedicata alle diposizioni finali e transitorie. Un allegato illustra le modifiche di altri atti normativi.

2.2 Ingresso

La competenza per disciplinare i mezzi d'identificazione elettronica risulta dalla Costituzione. Sono in particolare menzionati l'articolo 95 capoverso 1 Cost., che autorizza la Confederazione a emanare prescrizioni sull'esercizio dell'attività economica privata. Il rilascio degli eID spetta a fornitori di servizi d'identificazione che per essere riconosciuti devono soddisfare diverse condizioni, il che limita l'esercizio dell'attività economica privata.

Inoltre l'articolo 96 capoverso 1 Cost. conferisce alla Confederazione la competenza di emanare prescrizioni contro gli effetti economicamente o socialmente nocivi di cartelli e di altre forme di limitazione della concorrenza. Il disegno prevede determinate misure per contrastare le conseguenze nocive legate all'attività economica degli IdP dalla posizione di mercato dominante e gli abusi che ne possono derivare.

La legge si fonda inoltre sull'articolo 97 capoverso 1 Cost. che conferisce alla Confederazione la competenza di legiferare in materia di protezione dei consumatori. Il disegno introduce infatti un sistema di riconoscimento degli IdP e di vigilanza su di essi che mira a tutelare anche i consumatori.

La legge disciplina determinati aspetti di diritto civile relativi ai rapporti contrattuali tra i fornitori di servizi d'identificazione elettronica, i titolari di eID e i gestori di servizi che utilizzano l'eID. Tuttavia, data l'importanza limitata di questi aspetti nella fattispecie, nell'ingresso non si cita l'articolo 122 capoverso 1 Cost., che conferisce alla Confederazione la competenza di legiferare nel campo del diritto civile.

2.3 Disposizioni generali

Art. 1 Oggetto e scopo

Cpv. 1

La legge disciplina l'identificazione del titolare dell'eID da parte dello Stato, il riconoscimento degli IdP e la vigilanza su di essi, i diritti e gli obblighi dei titolari di un eID e dei gestori di servizi che l'utilizzano, nonché il contenuto, il rilascio, l'utilizzo, il blocco e la revoca degli eID.

Cpv. 2

La LSIE contribuisce a creare sicurezza e fiducia nelle transazioni elettroniche (*e-business* ed *e-government*). Inoltre mira a garantire la protezione dei dati: la lettera b riprende quindi lo scopo fissato all'articolo 1 LPD.

I cittadini svizzeri e stranieri con corrispondenti documenti d'identità dovranno poter dimostrare la propria identità in modo affidabile anche nel mondo digitale. Esattamente come accade con un documento d'identità nel mondo fisico, l'eID permette di dimostrare nel mondo virtuale i dati d'identificazione personale quali il cognome, i nomi o l'età. L'utilità principale di un eID consiste nell'effettuare in rete diverse transazioni in modo affidabile, ad esempio nel contesto dell'*e-government* o del commercio elettronico, senza che le parti si debbano incontrare fisicamente. L'eID assolve a un compito importante nel quadro della digitalizzazione dell'economia, dello Stato e della società in Svizzera.

Art. 2 Definizioni

Lett. a

Un IdP gestisce almeno un sistema di eID. La distinzione tra IdP e sistema di eID è importante per il riconoscimento, nell'ambito del quale si esaminano in particolare l'adempimento dei presupposti di cui all'articolo 13 capoverso 2 LSIE, le procedure di rilascio e i processi operativi. Per il riconoscimento di un sistema di eID è invece prioritario il rispetto delle prescrizioni tecniche. È comunque possibile che un IdP riconosciuto gestisca vari sistemi di eID a differenti livelli di sicurezza e magari non tutti riconosciuti. Altre disposizioni sul riconoscimento e l'estinzione o il ritiro sono riportate agli articoli 14 e 19 LSIE.

Lett. b

Un servizio che utilizza l'eID è un'applicazione informatica il cui gestore consente agli utenti d'identificarsi con un eID, attraverso un sistema di eID. Si tratta ad esempio di ditte che offrono in rete beni o servizi e utilizzano un sistema d'identificazione per effettuare le transazioni.

2.4 Rilascio, tipologie, contenuto, blocco e revoca degli eID

Art. 3 Presupposti personali

Osservazione preliminare

La formulazione potestativa al capoverso 1 garantisce a un IdP di non dover rilasciare un eID soltanto perché il richiedente adempie i presupposti per riceverne uno. L'articolo 17 LSIE limita detto principio se il mercato non funziona perché l'IdP abusa della sua posizione dominante.

Acquisendo un eID, il richiedente ne diventa il titolare.

Minorenni

L'eID può essere rilasciato anche a minorenni e a persone a cui è stato parzialmente o completamente revocato l'esercizio dei diritti civili. La persona con diritto di rappresentanza è comunque tenuta a richiedere l'eID a nome della persona rappresentata che ne diventa titolare ma può poi utilizzarlo sotto la vigilanza del suo rappresentante. Alla persona rappresentata deve essere rilasciato un corrispondente documento d'identità. I dettagli saranno fissati in un'ordinanza.

Cpv. 1

Documento d'identità come prova dell'identità

Per ottenere un eID è sufficiente un documento d'identità svizzero valido (lett. a), un documento di legittimazione valido e riconosciuto in base all'articolo 13 capoverso 1 della legge federale del 16 dicembre 2005[19] sugli stranieri o una carta di legittimazione in base alla legislazione sullo Stato ospite (lett. b n. 1). Possono ottenere un eID anche gli stranieri che, pur non essendo in possesso di un documento, sono identificabili in modo attendibile con procedura speciale d'identificazione al momento del rilascio (lett. b n. 2).

Requisiti posti agli stranieri

Affinché anche gli stranieri possano accedere ai servizi che utilizzano l'eID, comprese le applicazioni di *e-government*, è previsto di autorizzare il rilascio di un eID agli stranieri in possesso di una carta di soggiorno contenente un permesso di soggiorno (art. 41 cpv. 1 LStr in combinato disposto con l'art. 71 cpv. 1 dell'ordinanza del 24 ottobre 2007[20] sull'ammissione, il soggiorno e l'attività lucrativa [OASA]; permessi L, B, C), agli stranieri in possesso di una carta di legittimazione (art. 17 cpv. 1 dell'ordinanza del 7 dicembre 2007[21] sullo Stato ospite [OSOsp] in combinato disposto con l'art. 71*a* cpv. 1 OASA) e ai frontalieri (art. 71*a* OASA, permesso G).

In questo modo gli stranieri titolari di una carta di soggiorno valida secondo l'articolo 41 LStr potranno utilizzare un eID, come anche le applicazioni di

19 RS **142.20**
20 RS **142.201**
21 RS **192.121**

e-governement. Rientrano nella categoria i titolari di permessi C, B, L e G poiché, in base all'articolo 89 LStr, lo straniero che soggiorna in Svizzera deve essere in possesso di un documento di legittimazione valido secondo l'articolo 13 capoverso 1 LStr. I dettagli saranno fissati in un ordinanza (cfr. cpv. 2).

Le carte di soggiorno di categoria N, F, S e Ci non danno sistematicamente diritto a un eID in quanto non si può partire dal presupposto che l'identità dell'interessato abbia potuto essere stabilita in modo attendibile.

Al momento si rinuncia a concedere l'accesso a funzioni eID agli altri stranieri, in particolare ai titolari di permessi N, F ed S. Molti richiedenti l'asilo non possono presentare un documento d'identità in sede procedurale, il che rende impossibile un'identificazione sicura. Persino le persone ammesse provvisoriamente presentano al DFGP (SEM) numerose domande di modifica o rettifica dei propri dati personali, domande che spesso si basano su documenti non idonei. Attualmente, nel settore dell'asilo non sono previsti servizi elettronici cui i titolari di permessi N, F o S debbano accedere direttamente. Il rilascio di un eID a queste categorie di persone non è pertanto prioritario.

Cpv. 2

Per poter reagire in modo flessibile ai più recenti sviluppi tecnologici, le procedure per verificare i documenti d'identità dei cittadini svizzeri e i documenti di legittimazione nonché l'identità dei cittadini stranieri sono disciplinate a livello di ordinanza. I processi d'identificazione possono eventualmente essere strutturati ispirandosi ai metodi d'identificazione impiegati nel settore bancario. La legislazione sul riciclaggio di denaro, ad esempio, definisce meticolosamente i metodi ammessi per l'identificazione dei nuovi clienti. A tale riguardo un eID varrà come prova dell'identità.

Al numero 5.7 figura una panoramica sulla delega di competenze legislative.

Art. 4 Livelli di sicurezza

Cpv. 1

Non tutte le transazioni richiedono il medesimo livello di sicurezza. Sovente, un livello di sicurezza superiore comporta un onere maggiore per l'acquisizione, un utilizzo più complicato e maggiori costi. Al fine di andare incontro alle esigenze del mercato, gli IdP devono poter offrire tre diversi livelli di sicurezza, come prescritto anche dall'UE e dal NIST. I gestori di servizi che utilizzano l'eID possono decidere autonomamente quale livello di sicurezza intendono applicare (cfr. art. 20 LSIE).

Per poter essere riconosciuto, un sistema di eID deve soddisfare perlomeno il livello di sicurezza *basso*. I sistemi di eID dei livelli di sicurezza *significativo* ed *elevato* soddisfano requisiti superiori a quelli minimi. Un eID del livello *elevato* soddisfa dunque anche i requisiti posti ai livelli *significativo* e *basso*; non vale invece il contrario (compatibilità discendente).

In funzione del livello di sicurezza del sistema, l'eID offre un differente grado di affidabilità. Il livello *basso* mira a ridurre il rischio di usurpazione e di alterazione dell'identità, mentre il livello *significativo* offre una protezione elevata contro tale rischio e quello *elevato* garantisce la massima protezione possibile.

Cpv. 2

I livelli di sicurezza si distinguono per i dati d'identificazione personale trasmessi, il processo di rilascio dell'eID, le regole per la sua applicazione e la gestione del sistema di eID (in particolare l'aggiornamento dei dati d'identificazione personale). La legge riporta i requisiti tecnici evitando per quanto possibile riferimenti tecnologici, da definire in dettaglio a livello di ordinanza e di istruzione, dove saranno specificati anche i diversi supporti per l'eID.

Cpv. 3

Un eID di un livello di sicurezza superiore deve poter essere impiegato anche presso un servizio che utilizza l'eID con un livello di sicurezza inferiore. I titolari possono dunque utilizzare il loro eID presso tutti i servizi che utilizzano l'eID a condizione che l'eID abbia un livello di sicurezza equivalente o superiore a quello del servizio.

Cpv. 4

Il Consiglio federale disciplina i diversi livelli di sicurezza, in particolare i requisiti minimi per l'identificazione alla luce dello stato attuale della tecnica.

Art. 5 Dati d'identificazione personale

Cpv. 1, 2 e 3

Il tipo e la quantità di dati d'identificazione personale attribuiti a un eID dipendono dal relativo livello di sicurezza. Mentre per un eID del livello di sicurezza *basso* sono richiesti solamente i dati identificativi di base (numero di registrazione eID, cognome ufficiale, nomi e data di nascita), per un eID del livello di sicurezza *significativo* o *elevato* sono necessari dati supplementari (sesso, luogo di nascita e cittadinanza), inoltre per il livello di sicurezza *elevato* è richiesta anche l'immagine del viso.

La trasmissione di dati d'identificazione personale secondo il capoverso 2 presuppone che il processo di registrazione, il sistema di eID e l'identificazione soddisfino requisiti tecnici e organizzativi elevati.

Cpv 4

Nella misura in cui è necessario per l'adempimento dei compiti conferitigli dalla LSIE, fedpol può completare i dati d'identificazione personale con informazioni supplementari relative all'ultimo aggiornamento dei dati nel sistema d'informazione di cui all'articolo 24.

Un IdP privato che offre prestazioni supplementari può trattare anche dati non contemplati dalla LSIE, come ad esempio l'indirizzo di consegna o informazioni sul pagamento, a condizione che il titolare dell'eID vi acconsenta; viceversa un IdP pubblico (ai sensi dell'art. 10) può farlo soltanto se tale competenza gli è conferita da una base legale.

Art. 6 Processo di rilascio

Osservazione preliminare

Il processo di rilascio coinvolge il richiedente e fedpol. A seconda del livello di sicurezza, il rilascio presuppone che il richiedente si presenti personalmente presso l'IdP o si identifichi in modo equivalente. Il nostro Consiglio disciplina il processo di rilascio a seconda del livello di sicurezza; le pertinenti deleghe figurano in diverse disposizioni del disegno (in particolare art. 3 cpv. 2, 4 cpv. 4 e 6 cpv. 5).

Cpv. 1

L'eID non è obbligatoria. Chi desidera un eID deve contattare fedpol tramite un IdP. La richiesta deve provenire dal futuro titolare dell'eID (richiedente). L'IdP non è autorizzato a rilasciare un eID di sua spontanea volontà, anche se conosce la persona in questione poiché è già sua cliente.

Pur dovendosi rivolgere a un IdP per ottenere un eID, il richiedente dovrà identificarsi direttamente presso fedpol. È stato ad esempio previsto che, durante la procedura d'identificazione, il richiedente sia trasferito dal sito Internet dell'IdP a quello di fedpol affinché fornisca le informazioni richieste. In questo modo il richiedente può depositare la sua domanda d'identificazione direttamente nel sistema d'informazione di fedpol.

Cpv. 2

Fedpol verifica che il richiedente soddisfi i presupposti personali di cui all'articolo 3. In caso affermativo, fedpol lo identifica grazie alle informazioni richieste per il livello di sicurezza in oggetto. Queste informazioni sono riprese dai registri di persone di cui all'articolo 24 capoverso 3. Se il richiedente è stato identificato conformemente al livello di sicurezza richiesto e se vi acconsente, fedpol trasmette all'IdP i dati d'identificazione personale di cui all'articolo 5.

Cpv. 3

Fedpol mette a verbale le trasmissioni di dati effettuate nel corso del processo di rilascio. Questi verbali garantiscono la tracciabilità delle operazioni e possono fungere da prova nel caso di divergenze tra le parti in oggetto. Fedpol è inoltre tenuto a verbalizzare tali dati in base all'obbligo d'informazione che ha nei confronti dei titolari dell'eID.

Cpv. 4

L'IdP attribuisce i dati d'identificazione personale all'eID e si assicura che l'eID sia attribuito alla persona fisica in questione (collegamento). Ciò avviene, ad esempio nel caso di una Mobile ID, attribuendo l'eID alla carta SIM utilizzata per l'abbonamento del richiedente e inserita nel suo dispositivo. A seconda del livello di sicurezza questa attribuzione è soggetta a differenti requisiti, ma affinché l'eID possa essere utilizzato occorre comunque perlomeno verificare un fattore d'autenticazione, ad esempio il possesso di un dispositivo personalizzato, la conoscenza di un segreto o una caratteristica biometrica.

Cpv. 5

Il Consiglio federale precisa il processo di rilascio in un'ordinanza, disciplinando in particolare lo svolgimento e indicando gli altri dati personali noti solamente al richiedente che possono essere utilizzati per l'identificarlo in modo affidabile.

Art. 7 Aggiornamento dei dati d'identificazione personale

Alcuni degli attributi identificativi sono modificabili, in particolare il cognome. Il disegno tiene conto di tale circostanza introducendo l'obbligo di un aggiornamento regolare.

Per migliorare l'affidabilità dell'eID sono previsti regolari aggiornamenti dei dati d'identificazione personale ossia il loro confronto con quelli riportati nei sistemi d'informazione statali. Gli intervalli massimi di questi adeguamenti sono prescritti per ogni livello di sicurezza. La relativa competenza spetta all'IdP, che inoltra a fedpol una richiesta automatizzata in base al numero di eID. Per gli aggiornamenti regolari sono riscossi emolumenti.

Art. 8 Utilizzo sistematico del numero d'assicurato per lo scambio di dati

Osservazione preliminare

Il numero d'assicurato (NAVS13) secondo la LAVS non deve poter essere comunicato ad ampio raggio e in modo incontrollato dato che ciò consentirebbe di utilizzarlo sistematicamente anche a quelle cerchie di persone che non vi sono autorizzate. L'articolo 8 contiene la base legale e i principi di trattamento applicabili all'utilizzo sistematico del NAVS13 per l'eID da parte di fedpol.

Cpv. 1

Nello scambio elettronico di dati con i registri di persone di cui all'articolo 24 capoverso 3, fedpol è autorizzata a utilizzare sistematicamente il NAVS13 per identificare le persone. Il NAVS13 serve a identificare in modo univoco una persona consultando altre banche dati che pure lo utilizzano sistematicamente. Il NAVS13 è imprescindibile per confrontare o inoltrare automaticamente i dati ripresi da diverse banche dati. Solo questo numero può garantire che una persona sia identificabile in modo univoco nei diversi registri anche dopo che ha cambiato il cognome. Cambiando cognome è possibile modificare l'identità originaria e costruirsene legalmente una nuova. Con il cambiamento del cognome, infatti, vengono rilasciati nuovi documenti d'identità, che non consentono di risalire alla precedente identità. Il NAVS13 permette per contro un'attribuzione univoca.

Cpv. 2

Per identificare le persone, fedpol può rendere accessibile il NAVS13 mediante procedura di richiamo unicamente ai gestori di servizi che utilizzano l'eID e sono autorizzati a impiegare sistematicamente tale numero in base alla LAVS. La trasmissione del NAVS13 a terzi non autorizzati a utilizzarlo sistematicamente va impedita adottando provvedimenti tecnici.

Poiché il NAVS13 non può fungere da numero di registrazione eID, va sviluppata un'altra applicazione che consenta agli enti autorizzati a utilizzare sistematicamente il NAVS13 di stabilire la corrispondenza tra i due numeri.

Art. 9 Trattamento e conservazione dei dati

Osservazione preliminare

Il trattamento, la conservazione e la trasmissione di dati corrispondono all'effettiva attività degli IdP. L'identificazione e l'autenticazione sono prestazioni fornite sia ai gestori di servizi che utilizzano l'eID sia ai titolari di eID. Gli IdP fungono da intermediari tra di loro. Il disciplinamento della protezione dei dati risulta pertanto particolarmente importante. La LPD e gli atti normativi subordinati valgono per tutte le parti coinvolte. L'articolo fissa lo scopo e le condizioni specifiche per il trattamento e la conservazione dei dati da parte degli IdP, precisando inoltre le condizioni per il trattamento dei dati secondo la LPD e inasprendole per quanto riguarda le misure di sicurezza da adottare.

Cpv. 1 e 2

Le disposizioni a protezione dei dati nei capoversi 1 e 2 sono in linea con quelle della pertinente legislazione. Quando impiega l'eID, il titolare può scegliere i dati d'identificazione personale da far trasmettere dall'IdP al gestore del servizio che utilizza l'eID. Possono tuttavia essere trasmessi unicamente i dati corrispondenti al livello di sicurezza richiesto dal servizio in questione. L'IdP può trattare e conservare i dati fino alla revoca dell'eID, inoltre possono essere utilizzati unicamente per l'identificazione secondo la LSIE. Per gli eID del livello di sicurezza significativo, l'IdP può utilizzare l'immagine del viso del titolare dell'eID (registrata nel sistema d'informazione di cui all'art. 24) unicamente durante il processo di rilascio.

Cpv. 3

La disposizione impone agli IdP particolari misure di sicurezza, per cui è più restrittiva delle prescrizioni della LPD. Garantisce che i dati d'identificazione personale, i dati di utilizzo di un eID e gli altri dati siano trattati e conservati in modo sicuro. Queste tre categorie di dati vanno conservate separatamente le une dalle altre, in termini sia fisico sia organizzativi. Tale separazione tiene conto del tipo di dati e dello scopo del loro trattamento e costituisce una misura supplementare in materia di sicurezza atta a impedire che le persone non autorizzate abbiano accesso a tutti i dati riguardanti il titolare di un eID. In tal modo s'intende in particolare limitare le conseguenze nefaste di un accesso non autorizzato al sistema.

Art. 10 Sistema di eID sussidiario della Confederazione

La legge presuppone un mercato funzionante. Se tuttavia nessun IdP privato ha interesse a far riconoscere sistemi di eID dei livelli di sicurezza *significativo* o *elevato*, la Confederazione si riserva la possibilità di gestire un proprio sistema di eID per questi livelli di sicurezza. In tal caso, l'unità amministrativa incaricata di gestire un sistema di eID è soggetta alla LSIE allo stesso modo degli IdP: le disposizione vigenti per gli IdP si applicano anche a detta unità.

Ad ogni modo il nostro Consiglio può assegnare tale incarico soltanto a un'unità amministrativa autorizzata a fornire prestazioni commerciali a terzi in virtù dell'articolo 41*a* della legge del 7 ottobre 2005[22] sulle finanze della Confederazione (LFC), ossia al Centro servizi informatici del DFGP, all'Ufficio federale delle costruzioni e della logistica o all'Ufficio federale dell'informatica e delle telecomunicazioni (cfr. art. 41*a* cpv. 1 LFC).

Art. 11 Blocco e revoca

Cpv. 1–4

Fedpol garantisce che l'IdP possa verificare sistematicamente la validità del numero di registrazione eID seguendo una procedura usuale (cfr. art. 23 cpv. 2 LSIE); a tale proposito al momento è prevista la tenuta di un elenco elettronico che gli IdP devono consultare periodicamente al fine di bloccare o revocare immediatamente gli eID il cui numero di registrazione eID vi figura come non valido. La consultazione regolare migliora l'affidabilità degli eID riconosciuti e pertanto è gratuita. Gli IdP sono pure tenuti ad allestire un sistema gratuito che consenta tale consultazione per i soli eID da essi rilasciati (art. 15 cpv. 1 lett. c LSIE).

A seconda dell'esito della consultazione, l'eID va bloccato o revocato. È necessario distinguere tra blocco o revoca di un eID e blocco o revoca del numero di registrazione eID. Se ad esempio il titolare notifica la perdita del supporto, e quindi dell'eID, con il rischio che terzi se ne impossessino, l'eID in oggetto è invalidato per un certo periodo. Lo stato del numero di registrazione eID resta però immutato, in quanto è associato all'identità ufficiale della persona, valida indipendentemente dall'eID. Per impedire gli abusi, l'IdP verifica la provenienza della notifica prima di bloccare l'eID.

L'eID può essere riattivato e riutilizzato non appena il motivo del blocco cessa. Si procede invece alla revoca di tutte gli eID attribuiti a un numero di registrazione eID quando tale numero non può più essere utilizzato, ad esempio in caso di decesso del titolare (*cpv. 3*). Un eID revocato non può essere riattivato, mentre un eID temporaneamente bloccato sì. L'IdP informerà immediatamente del blocco il titolare dell'eID.

Cpv. 5

Il Consiglio federale disciplina il blocco e la revoca di un eID; definisce in particolare i casi di revoca dell'eID.

22 RS **611.0**

2.5 Titolari di un eID

Art. 12

Cpv. 1 e 2

Gli obblighi che la LSIE impone ai titolari di un eID corrispondono agli obblighi di diligenza usuali da osservare utilizzando una carta di credito o di conto bancario. Ad esempio è imprescindibile e ragionevole non rivelare e non conservare insieme al supporto dell'eID il PIN eventualmente necessario, attivare la protezione contro l'accesso (p. es. PIN o riconoscimento dell'impronta digitale) e installare una protezione contro i virus sul dispositivo mobile usato come supporto dell'eID.

Pur prendendo tutte le possibili precauzioni, l'usurpazione dell'identità non si può totalmente evitare. Andrebbero pertanto introdotte sanzioni penali adeguate per punire un tale abuso. Il progetto di legge del 15 settembre 2017[23] per la revisione totale della legge federale sulla protezione dei dati e la modifica di altri atti normativi sulla protezione dei dati introduce nel Codice penale (CC)[24] l'articolo 179^{decies}, una disposizione che punisce l'usurpazione d'identità con una pena detentiva sino a un anno o con una pena pecuniaria. Per evitare doppioni, il disegno non contiene disposizioni che sanzionano lo stesso comportamento.

Cpv. 3

Nel quadro della responsabilità delittuale, l'articolo 12 del disegno costituisce una norma di protezione in materia di responsabilità civile. Il nostro Consiglio può in particolare disciplinare in un'ordinanza gli obblighi supplementari di diligenza da rispettare, la cui chiara definizione consente lo sgravio in caso di responsabilità extracontrattuale (delittuale). Nell'ordinanza va stabilito ad esempio che gli errori nei dati d'identificazione personale, così come la perdita o il sospetto di abuso dell'eID devono essere immediatamente segnalati all'IdP.

2.6 Fornitori di servizi d'identificazione

Art. 13 Riconoscimento

Osservazione preliminare

Nel quadro della procedura di riconoscimento, gli IdP sono sottoposti a un esame approfondito che comprende il controllo dei dati del casellario giudiziale e delle condizioni finanziarie, nonché una serie di audit al fine di verificare che l'IdP sia in grado di svolgere debitamente la sua funzione. Con il riconoscimento degli IdP sono controllati e riconosciuti anche i loro sistemi di eID. I requisiti tecnici posti ai sevizi che utilizzano l'eID sono invece disciplinati soltanto indirettamente tramite i requi-

23 FF **2017** 6173
24 RS **311.0**

siti e gli oneri posti ai sistemi di eID. Questi oneri soddisferanno i requisiti del NIST-Cybersecurity Framework per quanto riguarda la sicurezza e l'affidabilità[25].

Cpv. 1

Se un IdP intende rilasciare un eID secondo la LSIE, deve adempire vari requisiti tecnici e organizzativi. L'ODIC controlla regolarmente il rispetto di tali presupposti garantendo così la possibilità di esercitare un controllo sufficiente sugli IdP e sui dati che hanno memorizzato.

Lett. a

Le persone fisiche e giuridiche non iscritte nel registro di commercio non possono ottenere il riconoscimento. In generale anche le autorità possono gestire sistemi di eID riconosciuti dal momento che possono iscriversi nel registro di commercio[26].

Lett. b e c

Un presupposto organizzativo riguarda le persone che controllano i documenti d'identità presentati nell'ambito della procedura di rilascio e che possono influire sulla trasmissione dei dati. Tali persone devono essere sufficientemente formate, disporre delle conoscenze tecniche, dell'esperienza e delle qualifiche necessarie e in particolare non devono rappresentare un rischio per la sicurezza.

Come rischio per la sicurezza s'intende ad esempio l'impiego di un persona condannata in via definitiva per determinati reati o che a causa dei suoi debiti potrebbe essere corrompibile. Le prove in tal senso possono essere acquisite con gli estratti dal casellario giudiziale e dai registri delle esecuzioni.

Lett. d

Il rispetto degli standard di sicurezza vigenti e la certificazione delle procedure provano la sicurezza e l'affidabilità dei sistemi di eID.

Lett. e

L'IdP deve garantire che i dati saranno trattati e conservati esclusivamente in Svizzera. Qualsiasi accesso non autorizzato ai dati da parte di terzi dall'estero va impedito. Per trattamento dei dati s'intende qualsivoglia impiego dei dati indipendentemente dai mezzi e dalle procedure utilizzati, in particolare l'acquisizione, la conservazione, l'archiviazione o la distruzione. Questa disposizione concerne tutti i dati trattati dall'IdP nel quadro dei servizi secondo la LSIE, in particolare anche dati provvisori, dati provenienti da memorizzazioni temporanee e dati marginali.

Lett. f

L'IdP deve stipulare un'assicurazione di responsabilità civile retta dal Codice delle obbligazioni (CO)[27] (cfr. art. 28 LSIE).

25 National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Cybersecurity Framwork, il testo è consultabile sul sito del NIST: www.nist.gov.
26 Cfr. art. 2 lett. a n. 13 dell'O. del 17 ott. 2007 sul registro di commercio (RS **221.411**) con rinvio all'art. 2 lett. d della legge del 3 ott. 2003 sulle fusioni (RS **221.301**).
27 RS **220**

Lett. g

È evidente che l'IdP può essere riconosciuto solamente se rispetta il diritto vigente: anzitutto la LSIE e le relative disposizioni d'esecuzione, ma anche altri atti e in particolare la LPD.

Cpv. 3

Poiché il settore dell'identificazione e dell'autenticazione elettronica è in costante evoluzione, il riconoscimento va rinnovato a intervalli regolari. Il nostro Collegio fissa la forma e il contenuto della verifica in un'ordinanza, che potrebbe ad esempio prevedere l'obbligo degli IdP di redigere e sottoporre all'ODIC un rapporto annuale sulla sicurezza.

Cpv. 4

Come in altri punti, anche qui il disciplinamento della procedura e dei dettagli tecnici è delegato al nostro Consiglio, competente per legiferare a livello di ordinanza.

A livello di ordinanza e di istruzione sono emanate prescrizioni più dettagliate sui requisiti del riconoscimento, in particolare sui requisiti tecnici e di sicurezza, sugli standard applicabili ai protocolli tecnici per i sistemi di eID nonché in relazione alla necessaria copertura assicurativa. Queste disposizioni sono regolarmente verificate dall'ODIC; in questo modo anche i sistemi di eID sono riconosciuti.

Art. 14 Estinzione del riconoscimento

Cpv. 1

Per poter gestire un sistema di eID, l'IdP deve essere in grado di esercitare la sua attività. Con l'avvio della procedura fallimentare, questa capacità economica viene a mancare e il riconoscimento si estingue in virtù della legge. I sistemi di eID non sono pignorabili e non rientrano nella massa fallimentare. I dati confermati attraverso i sistemi di eID non sono commerciabili e sono dunque privi di valore economico. Il riconoscimento si estingue anche nel momento in cui l'IpP cessa l'attività.

Cpv. 2 e 3

Queste disposizioni intendono preservare le reti di eID esistenti. Dato che il ricavato dell'assunzione può rientrare nella massa fallimentare, i sistemi di eID hanno un valore economico, anche se i singoli dati non sono commerciabili.

Cpv. 4

In caso di estinzione del riconoscimento, va rispettata la volontà del titolare dell'eID: se costui non acconsente all'assunzione dei sui dati da parte di un altro IdP o della Confederazione, i suoi dati non saranno trasferiti, bensì distrutti.

Cpv. 5

La disposizione intende garantire che, nel caso in cui nessun IdP sia in grado di assumere i sistemi di eID di un altro IdP, le reti di eID esistenti possano comunque continuare a funzionare; questo nell'interesse sia degli utenti sia dei partner com-

merciali che utilizzano tali identità e vi fanno affidamento. In una simile situazione, l'ODIC dispone che la Confederazione assuma gratuitamente tali sistemi di eID o che i dati ivi contenuti siano distrutti se i sistemi non vengono più gestiti.

Art. 15 Obblighi

Cpv. 1

Lett. a

L'IdP gestisce almeno un sistema di eID, può offrirne e farne riconoscere anche altri di differenti livelli di sicurezza, ma non è obbligato. La sicurezza dell'ambiente operativo costituisce uno dei presupposti organizzativi e tecnici per il riconoscimento disciplinati a livello di ordinanza o istruzione.

Lett. b

L'IdP è responsabile, nell'ambito della procedura di rilascio, per la corretta attribuzione dell'eID ai dati d'identificazione personale e alla persona fisica nonché per il rilascio dell'eID. Tale processo è suddiviso nelle tre fasi seguenti e può essere strutturato diversamente a seconda del livello di sicurezza:

1. L'IdP attribuisce in modo univoco all'eID i dati d'identificazione personale trasmessi da fedpol (art. 5 LSIE) con il numero di registrazione eID e il pertinente mezzo di autenticazione che autentifica il titolare. Almeno ai livelli di sicurezza superiori, il mezzo di autenticazione è direttamente integrato in un'unità di supporto (p. es. chip sulla carta o applicazione SIM nel cellulare).
2. L'IdP garantisce che l'eID sia attribuito alla persona fisica identificata (p. es. che i restanti dati registrati sul chip appartengano alla persona identificata o che l'abbonamento del cellulare sia intestato al nome della stessa).
3. Provvede affinché l'eID sia consegnato a questa persona (p. es. per raccomandata o durante un colloquio personale sul posto o ancora nel quadro di un collegamento in rete sicuro, a condizione che il mezzo di autenticazione sia collegato alla persona giusta).

Lett. c

Il settore della trasmissione sicura dei dati è soggetto a un rapido sviluppo tecnico, pertanto la verifica della validità di tutti gli eID mediante una procedura usuale è prescritta nella legge con una formulazione che corrisponde a quella della FiEle riveduta. Fedpol può ad esempio tenere e pubblicare un elenco dei numeri di registrazione eID temporaneamente o permanentemente non validi per l'acquisizione o l'utilizzo di un eID, in particolare in caso di dichiarazione di scomparsa o di decesso di una persona, eventualmente anche in caso di scadenza del permesso di dimora per stranieri. L'IdP è tenuto a consultare regolarmente questo elenco dei numeri di registrazione eID bloccati o revocati e aggiornarlo con la sua procedura usuale.

Lett. d

L'IdP è obbligato a informarsi attivamente in merito ai più recenti requisiti di sicurezza e a verificare che i sistemi che gestisce li rispettino.

Lett. e

L'aggiornamento dei dati d'identificazione personale migliora la sicurezza. La periodicità di questi aggiornamenti dipende dal livello di sicurezza ed è stabilita all'articolo 7 capoverso 1.

Lett. f e g

Per garantire il buon funzionamento del sistema di eID, l'IdP è tenuto a trasmettere alle autorità competenti determinate informazioni di cui è venuto a conoscenza. Deve segnalare a fedpol eventuali errori nei dati d'identificazione personale e comunicare all'ODIC gli eventi rilevanti per la sicurezza nel sistema di eID o nell'utilizzo dell'eID che gli sono stati segnalati o che ha scoperto da sé.

Lett. h

Ogni volta che per l'utilizzo di un eID sono trasmessi i dati d'identificazione personale, l'IdP deve chiedere il consenso del titolare dell'eID, il quale deve esplicitamente indicare i dati d'identificazione personale da trasmettere al gestore di servizi che utilizzano l'eID.

Lett. i

La LSIE disciplina il diritto di accesso ai dati in modo più severo rispetto all'articolo 8 LPD imponendo all'IdP di trasmettere su richiesta tutti i dati che tratta e che riguardano il richiedente. Per motivi di trasparenza e fiducia, il titolare dell'eID avrà accesso in linea ai suoi dati d'identificazione personali e ai dati generati dall'utilizzo dell'eID. La lettera i impone dunque agli IdP di concedere l'accesso a questi dati sempreché non abbia già distrutto i dati verbalizzati in base alla lettera j.

Lett. j

I dati messi a verbale dall'IdP sull'utilizzo dell'eID vanno cancellati dopo sei mesi. Un termine identico è previsto ad esempio nel settore della sorveglianza delle telecomunicazioni (cfr. art. 26 cpv. 5 della legge federale del 18 mar. 2016[28] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni). I dati a verbale sono utilizzati per la trasmissione di informazioni di cui alla lettera i e per la ricostruzione delle transazioni in caso di controversia.

Questa disposizione non concerne né il verbale né i dati di registrazione e di transazione presso il servizio che utilizza l'eID.

Lett. k

L'FPDT può prendere posizione sui modelli degli accordi che l'IdP intende concludere con i servizi che utilizzano l'eID; pertanto gli vanno previamente sottoposti.

28 RS **780.1**

Lett. l

Poiché il riconoscimento va rinnovato ogni tre anni al più tardi, l'IdP è tenuto a notificare tutte le modifiche che intende apportare al suo sistema di eID e tutti i cambiamenti pianificati nella sua attività. Ne consegue che le modifiche effettuate in questo arco di tempo devono essere separatamente approvate dall'ODIC. È quindi possibile che il riconoscimento non possa essere mantenuto durante questo periodo se, in seguito a questi cambiamenti, i presupposti per il riconoscimento di cui all'articolo 13 capoverso 2 non sono più adempiuti.

Cpv. 2

L'IdP garantisce che i problemi di utilizzo e la perdita del supporto possano essere notificati. Spetta al mercato stabilire le modalità di questa notifica: tramite una hotline telefonica o la posta elettronica oppure altri canali.

Cpv. 3

Infine il nostro Consiglio emana prescrizioni più dettagliate sulle diverse procedure di notifica e di comunicazione previste dalla legge, ossia in caso di cessazione programmata dell'attività dell'IdP, di errori nei dati d'identificazione personale, di eventi rilevanti per la sicurezza nel sistema di eID o nell'utilizzo degli eID o di accordi modello con i servizi che utilizzano l'eID.

Art. 16 Trasmissione dei dati

Cpv. 1

Gli IdP possono trasmettere ai gestori di servizi che utilizzano l'eID determinati dati d'identificazione personale di cui all'articolo 5 solamente se sono necessari per l'identificazione dell'interessato e se corrispondono al livello di sicurezza richiesto. Inoltre il titolare dell'eID deve acconsentire alla loro trasmissione.

La trasmissione dei dati è necessaria per assicurare che il sistema di eID possa svolgere la propria funzione e garantire i livelli di comodità, flessibilità e semplicità richiesti dagli utenti. Questo tipo di trasmissione rispetta il principio della proporzionalità in quanto l'ingerenza nella sfera privata è limitata agli aspetti necessari per realizzare lo scopo. Inoltre i dati personali trasmessi non sono degni di particolare protezione secondo l'articolo 3 lettera c LPD.

Cpv. 2

È vietato sia all'IdP che al gestore di servizi che utilizzano l'eID trasmettere al di fuori dell'utilizzo dell'eID, e soprattutto commercializzare, i dati d'identificazione personale riportati all'articolo 5 e confermati dallo Stato. Il modello aziendale degli IdP e dei gestori di servizi che utilizzano l'IdP non può fondarsi sulla vendita di dati o di profili di utilizzo confermati dallo Stato e dunque particolarmente significativi. Inoltre questi dati non devono poter essere trasmessi gratuitamente, ad esempio per scopi commerciali da parte di un'altra impresa dello stesso gruppo.

Art. 17 Accessibilità degli eID

La disposizione intende tutelare sia chi adempie i presupposti personali per ottenere un eID sia chi è già titolare di un eID da conseguenze nocive che potrebbero verificarsi nel caso in cui uno o due IdP occupassero una posizione dominante sul mercato. Una simile situazione potrebbe in particolare presentarsi se un IdP decidesse di non rilasciare un eID a parte della popolazione o di non offrirgliela alle stesse condizioni applicate alla maggior parte della popolazione.

In base al capoverso 1, tuttavia, devono sussistere fondati sospetti che l'IdP in oggetto abbia a più riprese negato il rilascio di un eID a richiedenti che soddisfano i presupposti personali, o non gliel'abbia offerta alle stesse condizioni. La disposizione non precisa però chi abbia la facoltà di rendere verosimile l'esistenza di una simile situazione. Potrebbero pertanto far valere la disparità di trattamento gli aventi diritto, i titolari di un eID, gli altri IdP, i gestori di un servizio che utilizza l'eID o le associazioni dei consumatori. In presenza delle condizioni indicate al capoverso 1, l'ODIC o l'IdP deve intervenire.

Al fine di facilitare l'interpretazione e l'applicazione dell'articolo, i criteri di cui tener conto nel valutare il singolo caso sono stati formulati nel modo più concreto possibile. Il margine di apprezzamento dell'ODIC e dell'IdP è pertanto limitato, il che rende più efficace il relativo processo decisionale.

Art. 18 Interoperabilità

L'interoperabilità tra i sistemi di eID costituisce un presupposto importante per la diffusione degli eID. L'articolo 18 stabilisce pertanto che gli IdP debbano reciprocamente riconoscere i sistemi di eID. L'interoperabilità è garantita da interfacce definite e standard tecnici stabiliti in un'ordinanza o un'istruzione.

Secondo la disposizione, i titolari possono impiegare il loro eID presso tutti i servizi che utilizzano l'eID a condizione che l'eID soddisfi almeno il livello di sicurezza richiesto, e questo indipendentemente dal fatto che il gestore del servizio abbia concluso un accordo con l'IdP. Per raggiungere tale obiettivo, gli IdP devono consociare i loro servizi d'identificazione elettronica, analogamente a una rete di carte di credito o al roaming della telefonia mobile, attraverso standard e regole d'interoperabilità che tutti gli IdP devono rispettare.

Al riguardo si rimanda anche ai commenti di cui al numero 1.2.6.6.

Art. 19 Misure di vigilanza e ritiro del riconoscimento

Cpv. 1

L'ODIC adotta le misure necessarie se nell'ambito dei controlli regolari o sulla base di una notifica constata che un IdP non rispetta le prescrizioni o non adempie più i presupposti per il riconoscimento (art. 13 cpv. 2 LSIE). Le misure necessarie possono consistere in particolare in requisiti tecnici, ad esempio in merito al rispetto dei più recenti standard tecnici, o in misure organizzative come oneri per la formazione dei collaboratori. L'ODIC stabilisce un termine entro il quale l'IdP deve colmare le lacune constatate.

Cpv. 2

Se entro il termine stabilito le lacune non sono colmate, l'ODIC ritira il riconoscimento. Il ritiro del riconoscimento deve sempre rispettare il principio della proporzionalità.

Cpv. 3

Il nostro Consiglio disciplina la procedura di ritiro del riconoscimento in un'ordinanza.

2.7 Gestori di servizi che utilizzano l'eID

Art. 20 Accordo con un IdP

Ogni gestore di servizi che utilizzano l'eID ha stipulato un accordo con almeno un IdP. Tale accordo disciplina per lo meno il livello di sicurezza e le procedure tecniche e organizzative applicabili.

Art. 21 Utilizzo del numero di registrazione eID

La disposizione autorizza i gestori di servizi che utilizzano l'eID a identificare le persone attraverso il numero di registrazione eID. Nella maggior parte dei casi si tratterà verosimilmente di soggetti privati, ma non è escluso che anche determinate autorità possano offrire servizi che utilizzano l'eID secondo la presente legge. Potrebbero ad esempio proporre un'applicazione di *e-government* basata su un servizio che utilizza l'eID per adempiere un compito d'interesse pubblico. Affinché in questi casi le autorità siano autorizzate a impiegare il numero di registrazione eID per l'identificazione, è necessaria una base legale.

Art. 22 Obbligo di accettare gli eID

I gestori di servizi che utilizzano l'eID, le autorità o gli altri servizi che, nell'adempimento di compiti amministrativi, ricorrono all'identificazione elettronica in esecuzione del diritto federale devono accettare tutti gli eID del livello di sicurezza richiesto. La disposizione si applica anche alle autorità cantonali e comunali se, attuando il diritto federale, ricorrono all'identificazione elettronica. Questo non esclude la possibilità di impiegare ancora i mezzi d'identificazione elettronica già in uso.

Questa disposizione sottolinea l'importanza e il grado di accettazione di un eID riconosciuto dallo Stato come definito nella strategia «Svizzera digitale» e nella Strategia di *e-government* del nostro Consiglio (cfr. n. 3). In tal modo s'intende proteggere gli investimenti della Confederazione per l'introduzione dell'eID e creare un'ampia base di consenso per l'impiego dell'eID nelle procedure di *e-government*. Ciò va a beneficio non soltanto della Confederazione, dei Cantoni e dei Comuni, che grazie all'eID riconosciuto a livello statale possono risparmiare sui costi, ma anche di tutti gli abitanti della Svizzera.

2.8 Funzione di fedpol

Art. 23 Compiti e obblighi

Cpv. 1

Fedpol attribuisce i dati d'identificazione personale a un numero di registrazione eID univoco e li trasmette all'IdP. La quantità di dati trasmessi varia in funzione del livello di sicurezza (cfr. art. 6 LSIE).

Cpv. 2

Fedpol garantisce che l'IdP possa verificare sistematicamente la validità del numero di registrazione eID in una procedura usuale. Attualmente è stato previsto che fedpol tenga un elenco elettronico che gli IdP consultano regolarmente e in base al quale bloccano o revocano immediatamente gli eID corrispondenti a un numero di registrazione eID contrassegnato come non valido. Questa procedura aumenta l'affidabilità degli eID riconosciuti ed è pertanto gratuita. A loro volta gli IdP sono tenuti ad allestire un sistema gratuito che consenta la consultazione per i soli eID da essi rilasciati (art. 15 cpv. 1 lett. c LSIE).

Si rimanda ai commenti all'articolo 11 capoversi 1–4.

Cpv. 3

I vari sistemi d'informazione sono alimentati con dati da diverse fonti. Infostar è il registro centrale dello stato civile ed è alimentato con dati provenienti dagli uffici regionali di stato civile di tutta la Svizzera. ISA riprende dati da Infostar o dai registri di controllo degli abitanti, nella misura in cui sono tenuti sulla base degli atti d'origine o del registro delle famiglie. SIMIC è gestito dalla SEM e contiene dati personali del settore degli stranieri e dell'asilo in merito a stranieri che hanno il diritto di soggiornare in Svizzera in base ad accordi internazionali.

Se una persona che figura in SIMIC annuncia un evento di stato civile (p. es. matrimonio, divorzio, nascita, ecc.), la registrazione delle modifiche può presentare differenze (p. es. grafia del nome). In questi casi il nostro Consiglio disciplina il modo di procedere. Per quanto riguarda il numero NAVS13, il servizio di clearing dell'UCC-UPI effettua già delle verifiche sui dati d'identificazione personale contraddittori. Anche gli accertamenti corrispondenti nell'ambito dell'eID potrebbero essere affidati a tale servizio.

Art. 24 Sistema d'informazione

Cpv. 1 e 2

Fedpol gestisce un sistema d'informazione per il trattamento dei dati personali di cui all'articolo 5, del numero d'assicurato e dei dati verbalizzati nella procedura di rilascio degli eID. L'elenco è esaustivo.

Lo scopo del trattamento dei dati è disciplinato in modo esaustivo al capoverso 2. Il sistema d'informazione permette di ricevere le domande e le dichiarazioni di consenso dei richiedenti, di adempiere in modo automatizzato i compiti di fedpol ine-

renti al rilascio di eID, di aggiornare i dati d'identificazione personale e di verificare i numeri di registrazione eID.

Cpv. 3

Per ottenere e confrontare i dati d'identificazione personale, il sistema d'informazione accede, mediante interfaccia, ai seguenti registri di persone:

- il sistema d'informazione per documento d'identità (ISA) di cui all'articolo 11 della legge del 22 giugno 2001[29] sui documenti d'identità e all'articolo 10 della relativa ordinanza del 20 settembre 2002[30];
- il sistema d'informazione centrale sulla migrazione (SIMIC) di cui all'articolo 101 e seguenti della legge sugli stranieri e dell'ordinanza SIMIC del 12 aprile 2006[31];
- il registro informatizzato dello stato civile (Infostar) secondo l'articolo 39 del Codice civile (CC)[32] e l'articolo 6*a* dell'ordinanza del 28 aprile 2004[33] sullo stato civile;
- il sistema d'informazione Ordipro del Dipartimento federale degli affari esteri (DFAE) secondo l'articolo 5 della legge federale del 24 marzo 2000[34] sul trattamento di dati personali in seno al Dipartimento federale degli affari esteri e l'articolo 2 dell'ordinanza Ordipro del 7 giugno 2004[35]; e
- il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI) secondo l'articolo 71 LAVS.

L'IdP è tenuto a collaborare con fedpol. Il suo sistema va dunque collegato con il sistema d'informazione di fedpol affinché vengano trasmessi i dati d'identificazione personale. Fedpol concederà all'IdP accesso al suo sistema d'informazione tramite un'interfaccia di modo che quest'ultimo possa memorizzare i dati d'identificazione personale del titolare dell'eID e trasmetterli ai gestori di servizi che utilizzano l'eID. Dal canto suo, l'IdP gestirà un proprio sistema d'informazione nel quale memorizza i dati d'identificazione personale ricevuti da fedpol e i dati relativi all'utilizzo degli eID da parte del titolare. In base all'articolo 15 capoverso 1 lettera i, deve accordare al titolare di un eID l'accesso in linea a questi dati. In nessun caso l'IdP avrà accesso ai registri delle persone elencati all'articolo 24 capoverso 3. Inoltre deve chiedere al titolare dell'eID l'esplicito consenso alla prima trasmissione dei dati d'identificazione personale a un gestore di servizi che utilizzano l'eID (art. 15 cpv. 1 lett. h). Gli articoli 9 e 16 prevedono ulteriori requisiti in merito al trattamento, alla conservazione e alla trasmissione dei dati da parte dell'IdP.

29 RS **143.1**
30 RS **143.11**
31 RS **142.513**
32 RS **210**
33 RS **211.112.2**
34 RS **235.2**
35 RS **235.21**

2.9 Funzione dell'ODIC

Art. 25 Competenza

Cpv. 1

Il servizio di riconoscimento per IdP (Servizio di riconoscimento) è gestito dall'ODIC. La procedura di riconoscimento di IdP si rifà a quella per le piattaforme di trasmissione (cfr. n. 1.3.2).

Cpv. 2

Il Servizio di riconoscimento pubblica un elenco sempre aggiornato di tutti gli IdP e sistemi di eID riconosciuti con i loro livelli di sicurezza. Questa disposizione si ispira a quella sulla pubblicazione delle piattaforme di trasmissione riconosciute.

Art. 26 Sistema d'informazione

Per adempiere i compiti previsti dalla legge, l'ODIC gestisce un sistema d'informazioni proprio che contiene: i dati, le informazioni e le prove fornite dall'IdP nel corso della procedura di riconoscimento, le notifiche della cessazione programmata dell'attività dell'IdP (art. 14 cpv. 2), degli eventi rilevanti per la sicurezza nel sistema di eID o nell'utilizzo dell'eID (art. 15 cpv. 1 lett. g), di tutte le modifiche previste nel sistema di eID e nell'attività (art. 15 cpv. 1 lett. l), nonché le informazioni sulle misure di sorveglianza. Il sistema d'informazione serve al riconoscimento degli IdP e alla sorveglianza su di essi.

2.10 Emolumenti

Art. 27

Fedpol e ISB riscuotono emolumenti dagli IdP per decisioni e prestazioni di servizio. Le domande relative alla validità dei numeri di registrazione eID sono esentasse. Per fissare l'importo di tali emolumenti si possono prendere in considerazione varie opzioni. Sarà il nostro Consiglio a stabilire la soluzione da adottare valutando le circostanze esecutive concrete. In particolare dovrà decidere se le spese amministrative, ossia quelle del servizio d'identità (fedpol), andranno interamente coperte nei primi anni. Riscuotere emolumenti ridotti dagli IdP che rilasciano eID gratuitamente potrebbe incoraggiare la rapida diffusione dell'eID e anche migliorare a medio o lungo termine l'efficacia delle transazioni elettroniche tra privati o con le autorità.

2.11 Responsabilità

Art. 28

Osservazione preliminare

Le responsabilità per danni cagionati utilizzando l'eID sono rette dalle pertinenti disposizioni, note e consolidate, del Codice delle obbligazioni o della legge del 14 marzo 1958[36] sulla responsabilità e dei pertinenti atti normativi cantonali.

Questo articolo ha carattere dichiaratorio e serve a chiarire che sono applicabili tutte le disposizioni sulla responsabilità, ad esempio per quanto riguarda la definizione di danno, le possibilità di sgravio o la responsabilità per gli ausiliari. Si rinuncia a formulare ulteriori norme in materia.

In particolare non vi è motivo di estendere ai titolari di un eID la regolamentazione sulla responsabilità dei titolari di chiavi crittografiche utilizzate per generare firme nei confronti di terzi, di cui all'articolo 59*a* CO. L'eID da sola non consente di concludere negozi giuridici; la LSIE tratta esclusivamente l'identificazione sicura dei partecipanti alle comunicazioni elettroniche.

Al momento si rinuncia pure a introdurre una responsabilità causale dell'IdP analoga a quella prevista dall'articolo 17 della FiEle riveduta. Di conseguenza, anche le regole sulla prescrizione sono rette dal Codice delle obbligazioni. Al momento di negoziare un accordo bilaterale per la notifica degli eID all'UE, occorrerà apportare i necessari adeguamenti alla LSIE, prestando particolare attenzione alle disposizioni in materia di responsabilità transfrontaliera.

Cpv. 1

La responsabilità del titolare dell'eID, del gestore di servizi che utilizzano l'eID e degli IdP, ossia degli attori privati, è retta dal Codice delle obbligazioni. Va valutato caso per caso se si tratti di una responsabilità contrattuale o extracontrattuale (art. 41 segg. CO).

Cpv. 2

In quanto unità amministrative della Confederazione, fedpol e l'ODIC sono sottoposte alla legge sulla responsabilità.

2.12 Disposizioni finali

Art. 29 Disposizioni transitorie

Lo scopo di queste disposizioni transistorie è di agevolare il riconoscimento dei mezzi d'identificazione elettronici rilasciati prima dell'entrata in vigore della LSIE. Nella maggior parte dei casi, il titolare di un mezzo d'identificazione elettronica è già stato sottoposto a una severa procedura di rilascio presso un IdP o un organo simile.

36 RS **170.32**

Durante una fase transitoria di due anni, l'ODIC riconosce, su richiesta di un IdP, i mezzi d'identificazione elettronica rilasciati da quest'ultimo come eID del livello di sicurezza basso. Riconosce inoltre i mezzi d'identificazione elettronica rilasciati da un IdP come eID del livello di sicurezza significativo, se, in aggiunta, è stata effettuata un'identificazione seguendo una procedura legale e sorvegliata che offra un livello di sicurezza simile a quello della procedura prevista dalla LSIE. Anche chi è in possesso di un certificato qualificato secondo l'articolo 2 lettera h FiEle può quindi farsi rilasciare da un IdP un eID del livello di sicurezza significativo, senza che sia necessario verificare nuovamente la sua identità. In tutti e tre i casi, occorre che siano adempite le condizioni di cui al capoverso 1 lettera a: il titolare deve soddisfare i presupposti personali secondo l'articolo 3, deve aver acconsentito al rilascio dell'eID e i dati d'identificazione personale (quali il numero della carta d'identità, il cognome, il nome e la data di nascita) devono corrispondere ai dati registrati nel sistema d'informazione di cui all'articolo 24.

Il nostro Consiglio emanerà in un'ordinanza prescrizioni dettagliate sulla procedura di rilascio. Definirà segnatamente i requisiti posti alla procedura, le diverse fasi procedurali e le competenze dell'organo competente per il riconoscimento.

Dovrà in particolare anche stabilire le modalità di attribuzione del numero di registrazione eID ai mezzi d'identificazione elettronica rilasciati da un IdP prima dell'entrata in vigore della LSIE.

Art. 30 Modifica di altri atti normativi

In allegato alla LSIE figurano le proposte di modifica di altri atti normativi. In particolare, fedpol sarà autorizzato ad accedere ai sistemi d'informazione ISA, SIMIC e Infostar. Non è necessario che il sistema d'informazione UCC–UPI sia accessibile mediante procedura di richiamo.

Art. 31 Referendum ed entrata in vigore

Come ogni legge federale, anche la LSIE sottostà a referendum facoltativo e il nostro Consiglio ne determina l'entrata in vigore.

2.13 Modifica di altri atti normativi

Osservazione preliminare

Dagli accertamenti condotti finora è emerso che le condizioni d'identificazione e di autenticazione per le applicazioni di *e-government* sono disciplinate tutt'al più a livello di ordinanza o di direttiva. L'elaborazione delle disposizioni d'esecuzione relative alla LSIE implica pertanto un adeguamento di svariate ordinanze e direttive, quali, ad esempio, l'ordinanza del 6 giugno 2014[37] concernente i sistemi d'informazione per il servizio veterinario pubblico (O–SISVet) o l'ordinanza del 23 ottobre 2013[38] sui sistemi d'informazione nel campo dell'agricoltura (OSIAgr).

37 RS **916.408**
38 RS **919.117.71**

1. Legge federale del 20 giugno 2003[39] sul sistema d'informazione per il settore degli stranieri e dell'asilo

Art. 9 cpv. 1 lett. c e 2 lett. c n. 3 (nuovo)

L'articolo 9 capoverso 1 elenca le autorità cui la SEM può permettere di accedere con procedura di richiamo ai dati del settore degli stranieri che ha trattato o fatto trattare nel sistema d'informazione secondo la LSISA. La lettera c definisce le finalità dell'accesso accordato alle autorità federali competenti in materia di polizia. La presente legge integra questo elenco con uno scopo nuovo: l'identificazione di persone, nonché l'attribuzione e l'aggiornamento dei dati d'identificazione personale secondo la LSIE.

L'articolo 9 capoverso 2 elenca le autorità cui la SEM può permettere di accedere con procedura di richiamo ai dati del settore dell'asilo che ha trattato o fatto trattare nel sistema d'informazione secondo la LSISA. La lettera c definisce per quali finalità un tale accesso può essere accordato alle autorità federali competenti in materia di polizia. La presente legge integra questo elenco con uno scopo nuovo: l'adempimento dei compiti secondo la LSIE.

2. Legge del 22 giugno 2001[40] sui documenti d'identità

Art. 1 cpv. 3, secondo periodo

In linea di massima, i passaporti diplomatici e di servizio sono rilasciati unicamente a cittadini svizzeri. Per determinati Stati accreditanti o l'adempimento di determinati compiti nell'interesse e su incarico della Confederazione, è tuttavia necessario, per motivi di sicurezza, rilasciare tali documenti anche a persone prive della cittadinanza svizzera. S'intende di fatto evitare che accompagnatori stranieri di diplomatici svizzeri o di altri impiegati di una rappresentanza svizzera siano confrontati a gravi difficoltà. A volte è necessario disporre di un passaporto diplomatico o di servizio anche per annunciarsi nello Stato accreditante o per ottenere un visto. La problematica si è ulteriormente acuita in seguito all'evolvere della società sul tema delle unioni personali e, in questo contesto, al fatto che un crescente numero di diplomatici ha coniugi o partner stranieri. Si tratta inoltre anche di agevolare ai collaboratori stranieri l'adempimento della propria funzione in determinati casi. Il DFAE è spesso costretto a reclutare specialisti di nazionalità straniera, perché non vi sono cittadini svizzeri disposti a lavorare in una regione di crisi o di conflitto in cui potrebbero rischiare la vita e l'integrità fisica. Va tuttavia precisato che questi specialisti non acquisiscono la cittadinanza svizzera e che nella pagina dei dati personali del passaporto, alla rubrica nazionalità, viene indicato il loro Paese d'origine, mentre il campo del luogo d'origine recherà il simbolo «***».

39 RS **142.51**
40 RS **143.1**

Art. 11 cpv. 1 lett. k e cpv. 2

I dati personali registrati in ISA vanno integrati con il numero d'assicurato ed eventualmente con il numero di registrazione eID, affinché i dati provenienti dai diversi registri federali e necessari all'utilizzo di un eID possano essere attribuiti a una persona in maniera univoca.

Art. 12 cpv. 2 lett. g

Non soltanto fedpol (lett. a), ma anche il DFAE (Direzione consolare) deve poter consultare ISA per ottenere i dati necessari al rilascio di un eID. Si tratta in particolare di accedere a dati non disponibili in Infostar, quali il numero del documento d'identità, l'immagine del viso e l'immagine della firma. Il NAVS13 o il numero di registrazione eID consentono di attribuire correttamente a una persona i dati per il rilascio di un eID.

Art. 14

Poiché con l'introduzione dell'eID riconosciuta i dati provenienti da ISA saranno registrati anche nei sistemi d'informazione degli IdP riconosciuti e di fedpol, questi servizi devono essere esclusi dal divieto di gestire banche dati parallele.

3. Codice civile[41]

Art. 43a cpv. 4 n. 5

L'articolo 43*a* CC disciplina l'accesso mediante procedura di richiamo ai registri elettronici al fine di gestire lo stato civile. All'elenco dei servizi che hanno accesso a Infostar viene aggiunto fedpol.

4. Legge federale del 20 dicembre 1946[42] su l'assicurazione per la vecchiaia e per i superstiti

*Art. 50a cpv. 1 lett. b^quater^*

L'articolo 50*a* LAVS determina i servizi cui possono essere comunicati dati, in particolare il numero d'assicurato, in deroga all'articolo 33 della legge federale del 6 ottobre 2000[43] sulla parte generale del diritto delle assicurazioni sociali (LPGA; RS *830.1*). Il disegno include fedpol tra questi servizi. Il presupposto legale formale per l'utilizzo sistematico del numero d'assicurato da parte di fedpol e degli IdP figura all'articolo 8 capoverso 1 LSIE.

41 RS **210**
42 RS **831.10**
43 RS **830.1**

5. Legge del 18 marzo 2016[44] sulla firma elettronica

Art. 9 cpv. 1bis

Chi chiede il rilascio di una firma elettronica deve presentarsi di persona. Quest'obbligo viene a cadere se l'identità è dimostrata con un eID del livello di sicurezza significativo.

3 Ripercussioni

3.1 Ripercussioni sulle finanze e sul personale

Vista l'importanza strategica del progetto sull'identità elettronica, le ripercussioni sulle finanze e sul personale sono illustrate sia per la fase di realizzazione sia per la fase di gestione. Va precisato che la fase di realizzazione comprende anche un progetto preliminare, concluso nel 2017.

3.1.1 Realizzazione

3.1.1.1 Progetto preliminare (fino al 2017)

Nel quadro del progetto preliminare, concluso alla fine del 2017, sono state analizzate possibili varianti teoriche per gli eID riconosciuti dallo Stato ed è stato elaborato un avamprogetto. È stato sviluppato anche un simulatore di eID per presentare il progetto e definire i requisiti tecnici nell'ordinanza e nelle disposizioni d'esecuzione. Il simulatore serve quindi come strumento di sviluppo e di test di queste normative. Il progetto preliminare ha cagionato spese complessive pari a 390 000 franchi, 290 000 dei quali sono stati stanziati dal DFGP e 100 000 da e-Government Svizzera.

3.1.1.2 Organizzazione

Tra il 2018 e il 2020 è prevista la creazione di un Servizio delle identità presso fedpol e di un Servizio di riconoscimento presso l'ODIC. Le conseguenti spese comprendono il reclutamento del personale e la messa a punto di processi e interfacce. Il Servizio delle identità sarà competente per l'infrastruttura tecnica e il relativo supporto (assistenza tecnica in rete e linea telefonica per gli utenti), nonché per l'aggiornamento delle prescrizioni in merito al riconoscimento. Il Servizio di riconoscimento attuerà la LSIE per quanto riguarda il riconoscimento degli IdP, effettuerà i controlli richiesti e vigilerà sul rispetto delle norme.

44 RS **943.03**

Spese in giorni–persone	2018	2019	2020	Totale
Creazione Servizio delle identità	–	150	75	225
Creazione Servizio di riconoscimento	–	50	25	75
Totale	–	200	100	300
Spese	–	160 000	80 000	**240 000**

Base di calcolo: 220 giorni di progetto per persona e anno

Con una tariffa di 800 franchi per giorno-persona, il totale delle spese per la creazione del Servizio delle identità e del Servizio di riconoscimento ammonta a **240 000 franchi**.

3.1.1.3 Sistemi

La gestione del Servizio delle identità sarà automatizzata entro limiti ragionevoli. A tal fine occorre creare un'applicazione informatica specifica che preveda interfacce con gli IdP e con i registri delle persone federali (ISA, SIMIC, Infostar e UCC–UPI) attraverso le quali i dati d'identità riconosciuti dallo Stato saranno trasmessi agli IdP. L'applicazione comprenderà anche l'allestimento di un sito Internet della Confederazione sul quale i richiedenti di un eID potranno confermare la loro identità e dare il loro consenso. Infine, attraverso un'interfaccia pubblica e accessibile gratuitamente, l'applicazione permetterà anche di verificare la validità di un numero di registrazione eID e di definire gli IdP riconosciuti dallo Stato.

Visto che il numero d'assicurato non può essere utilizzato direttamente come numero di registrazione eID, occorre creare un servizio supplementare grazie al quale gli organi autorizzati a usare sistematicamente il numero d'assicurato potranno determinare il numero d'assicurato abbinato a un determinato numero di registrazione eID.

Le altre spese comprendono, tra l'altro, il ricorso a esperti esterni per domande specifiche, ad esempio nel campo della sicurezza informatica.

Le spese legate all'allestimento dei sistemi informatici (2018–2020) e le spese complessive del progetto, incluso il suo finanziamento, sono illustrate al numero 3.1.1.4.

3.1.1.4 Spese complessive e finanziamento della fase di realizzazione

	Prog. preliminare			Attuazione	Totale
Spese in CHF	2015–2017	2018	2019	2020	
Spese di personale (incl. gestione del progetto)	200 000	240 000	320 000	250 000	1 010 000
Sviluppo del sistema (simulatore eID)	180 000	110 000	100 000	50 000	440 000
Sviluppo del sistema (applicazione specifica/banca dati)	–	260 000	2 580 000	1 950 000	4 790 000
Sviluppo del sistema (interfaccia NAVS13)	–	50 000	400 000	300 000	750 000
Altre spese (esperti sicurezza IT)	10 000	150 000	240 000	270 000	670 000
Creazione del Servizio delle identità e del Servizio di riconoscimento	–	–	160 000	80 000	240 000
Totale	**390 000**	**810 000**	**3 800 000**	**2 900 000**	**7 900 000**
./. Mezzi centrali TIC	–	700 000	800 000	–	1 500 000
./. e-Government Svizzera	100 000	450 000	900 000	–	1 450 000
./. Mezzi propri DFGP	290 000	–	1 660 000	1 920 000	3 970 000
./. Riserve specifiche		–340 000	340 000	–	–
Onere supplementare per spese di progetto *una tantum*	–	–	**100 000**	**880 000**	**980 000**
./. Mezzi centrali TIC	–	–	–	880 000	880 000
./. e-Government Svizzera	–	–	100 000	–	100 000

Il finanziamento delle spese di progetto è già assicurato per un importo pari a 6 920 000 franchi, a disposizione del DFGP (comprese le quote dei mezzi centrali TIC e la partecipazione di e-Government Svizzera).

Alla luce dei risultati della consultazione, occorre creare e implementare un servizio supplementare per consultare il numero d'assicurato. A tal fine occorrono fondi supplementari pari a 750 000 franchi, da richiedere a titolo di credito aggiuntivo. Occorre inoltre sviluppare e garantire la manutenzione del simulatore, il che cagiona una spesa supplementare pari a 230 000 franchi. Per il biennio 2018 – 2020 si prevedono quindi costi supplementari pari a 980 000 franchi, anch'essi da richiedere a titolo di credito aggiuntivo (e-Government Svizzera: CHF 100 000, mezzi centrali TIC: CHF 880 000).

Le spese per terzi saranno finanziate con il credito V0224.00 «Rinnovo del passaporto e della carta d'identità svizzeri» di fedpol, pari a 19,6 milioni di franchi.

3.1.2 Gestione (dal 2020)

Per il Servizio delle identità e il Servizio di riconoscimento è prevista la creazione di un massimo di otto posti supplementari dal 2020.

I costi legati alla gestione informatica sono attualmente preventivati al 15 per cento degli investimenti effettuati, il che equivale a circa un milione di franchi. Le spese di gestione saranno conteggiate dal 2020. Durante il primo anno, la fase di realizzazione e quella di gestione si sovrapporranno parzialmente. Sarà necessario impiegare ulteriori fondi per la comunicazione della soluzione eID, il ricorso a periti esterni e gli imprevisti.

Le spese di gestione necessarie all'attuazione della LSIE sono stimate a un massimo di 2,4 milioni di franchi (1,4 mio. per gli otto posti supplementari e 1 mio. per le spese materiali). Il fabbisogno in termini di risorse sarà definito più precisamente in occasione dell'elaborazione delle ordinanze d'esecuzione e alla luce delle deliberazioni parlamentari. Il nostro Collegio presenterà una domanda di credito e fisserà la data d'entrata in vigore della LSIE. A quel punto sarà anche possibile appurare l'entità della domanda di eID presso i potenziali IdP.

3.1.3 Conto economico a lungo termine

Con decisione del 22 febbraio 2017, intitolata «Legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID): indizione della procedura di consultazione», abbiamo incaricato il DFGP di presentarci, assieme al messaggio relativo alla LSIE, un piano di finanziamento, in linea di massima senza incidenza sul bilancio, per la gestione del Servizio delle identità e del Servizio di riconoscimento, compreso il fabbisogno in termini di posti. Lo scenario si fonda su ipotesi prudenti e su una crescita costante del numero di eID, partendo da zero.

Le spese sono state calcolate in base a quanto esposto in precedenza. Per quanto riguarda le entrate, s'ipotizzano i seguenti due scenari.

Il Servizio di riconoscimento riscuote emolumenti per il riconoscimento degli IdP e dei loro sistemi di eID. Gli emolumenti variano a seconda del livello di sicurezza da riconoscere. Il riconoscimento deve essere rinnovato ogni tre anni. Nell'ipotesi che, a medio termine, gli emolumenti per il riconoscimento ammonteranno in media a 50 000 franchi l'anno, si può preventivare un entrata annuale dello stesso importo.

Il Servizio delle identità riscuote emolumenti per le sue prestazioni. Le entrate dipendono fortemente dal grado di diffusione degli eID. Gli emolumenti riscossi per la consultazione dei dati d'identificazione personale da parte degli IdP ammonteranno a circa 26 centesimi (livello di sicurezza basso: 1× anno; significativo: 1× trimestre; elevato: 1× settimana). Ipotizzando che il 24 per cento degli eID sono del livello di sicurezza basso, il 75 per cento del livello di sicurezza significativo e l'1 per cento del livello di sicurezza elevato, l'entrata sarà pari a circa 1 franco l'anno per ogni eID. Questo scenario parte inoltre dal presupposto che la prima trasmissione è gratuita, visto che gli IdP forniscono le loro eID gratuitamente.

Riassumendo, si ottiene il quadro seguente:

Spese	2020	2021	2022	2023	2024	2025	2026
Spese di personale	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000
Costi operativi TIC	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000
Totale	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000
Ricavi							
Numero di eID	–	400 000	800 000	1 200 000	1 600 000	2 000 000	2 400 000
Emolumenti: riconoscimento	50 000	50 000	50 000	50 000	50 000	50 000	50 000
Emolumenti: trasmissione dei dati	–	400 000	800 000	1 200 000	1 600 000	2 000 000	2 400 000
Totale	50 000	450 000	850 000	1 250 000	1 650 000	2 050 000	2 450 000
Risultato	–2 350 000	–1 950 000	–1 550 000	–1 150 000	–750 000	–350 000	50 000

Si prevede che il progetto, considerato separatamente, passerà alle cifre nere circa sei anni dopo il suo avvio. Se la diffusione degli eID sarà più rapida, ad esempio perché un fornitore di eID con numerosi clienti ottiene il riconoscimento, la soglia di redditività potrà essere raggiunta molto prima.

La neutralità dei costi degli eID non può tuttavia essere considerata soltanto in base al relativo progetto. La progressiva digitalizzazione dei processi amministrativi a livello di Confederazione, Cantoni e Comuni permetterà di conseguire ulteriori benefici in termini di costi e risparmi. Il risparmio sui costi, attualmente non quantificabile, va tenuto in considerazione per avere una corretta visione d'insieme del rapporto costi-benefici degli eID, che potrà peraltro considerarsi indicativo soltanto a qualche anno di distanza dall'introduzione degli eID e tenendo conto di tutti gli attori coinvolti nell'ecosistema degli eID. Soltanto allora si saprà quanti gestori di servizi che utilizzano l'eID avranno optato per l'eID e quindi rinunciato a un proprio, costoso, servizio di gestione dell'identità.

3.2 Ripercussioni per i Cantoni e i Comuni, per le città, gli agglomerati e le regioni di montagna

I Cantoni e i Comuni utilizzano molte soluzioni di *e-government*. L'eID semplifica notevolmente i processi di identificazione e di autenticazione per accedere a questi sistemi. Oggi nel Cantone di Berna, ad esempio, è possibile compilare elettronicamente la dichiarazione fiscale, ma soltanto dopo aver inserito una parola chiave ricevuta per posta e inviando un modulo firmato a mano. Se il contribuente avesse un eID, questa procedura non sarebbe più necessaria.

L'identificazione semplice e sicura favorisce l'utilizzo delle prestazioni di *e-government* offerte dalle città e dai Comuni. Se i processi sono adeguati, i privati

non devono più presentarsi personalmente alle autorità e possono curare i contatti con le autorità cantonali e comunali indipendentemente dal luogo in cui si trovano, utilizzando dispositivi collegati a Internet.

È difficile quantificare il fabbisogno finanziario legato agli eventuali adeguamenti delle soluzioni di *e-government* offerte dai Cantoni, dalle città e dai Comuni. Il dispendio legato all'introduzione di un processo d'identificazione basato sull'eID dipende dal tipo di soluzione informatica adottata. Secondo la legge saranno i Cantoni, le città e i Comuni che gestiscono un servizio che utilizza l'eID ad assumersi i costi legati all'utilizzo dei dati d'identificazione trasmessi dagli IdP. Il processo d'identificazione basato sull'eID permetterà tuttavia agli enti pubblici di conseguire risparmi superiori ai costi sopportati.

3.3 Ripercussioni per l'economia

Scambi regolamentati e sicuri anche in Internet contribuiscono in maniera sostanziale a rendere attrattiva e concorrenziale la piazza economica svizzera. Il nostro Consiglio intende fornire il contributo necessario a un passaggio riuscito della Svizzera alla società dell'informazione. A tal fine, ha deciso numerose misure che riguardano perlopiù l'adeguamento del quadro giuridico o l'allestimento di elementi infrastrutturali, tra cui la FiEle o la creazione di numeri d'identificazione univoci per le persone e le imprese e l'allestimento dei relativi registri.

Mezzi d'identificazione elettronici riconosciuti e ampiamente disponibili costituiscono un elemento fondamentale per la creazione di un vasto e globale ecosistema di eID che garantisca transazioni elettroniche sicure e affidabili. Le transazioni complesse con lo Stato o tra privati possono essere effettuate elettronicamente e quindi più efficacemente. Questo progetto crea inoltre nuovi e importanti settori d'attività.

3.4 Ripercussioni per la società

L'identificazione sicura del partner di scambi elettronici complica o impedisce gli abusi e favorisce la fiducia nello spazio digitale.

Gli abusi in Internet si fondano spesso sull'impossibilità di identificare con sicurezza il proprio interlocutore. Lo *spamming* è una realtà, da un lato perché è impossibile distinguere tra mittenti affidabili e mittenti di messaggi indesiderati, dall'altro perché non è possibile chiamare in causa la responsabilità di questi ultimi. Nel caso del *phishing,* i mittenti di e-mail si spacciano per qualcun altro, ad esempio per la banca del destinatario, e possono così provocare danni ingenti. I mezzi d'identificazione elettronica riconosciuti aiutano a proteggere l'identità dei titolari nell'attuale società globalizzata e altamente interconnessa. Il furto d'identità, potenzialmente molto pericoloso per la persona interessata, è notevolmente ostacolato. In molti casi, l'introduzione di un numero di registrazione eID potrebbe far venire meno la necessità di indicare il cognome, il nome e la data di nascita. Questo numero diverrebbe quindi uno pseudonimo univoco che non consente a terzi di risalire ad altri dati

personali. La sfera privata sarebbe meglio protetta, visto che il nome, facilmente associabile a una persona in particolare, non deve più essere comunicato.

3.5 Ripercussioni per l'ambiente

Il disegno non ha ripercussioni dirette per l'ambiente. Il passaggio da transazioni fisiche a transazioni elettroniche permetterebbe però di risparmiare risorse, il che avrebbe effetti positivi sull'ambiente. Venendo ad esempio meno la necessità di presentarsi di persona alle autorità, si sgraverebbero le infrastrutture di trasporto pubblico e, di conseguenza, si ridurrebbero le emissioni inquinanti.

3.6 Altre ripercussioni

Dato che non si attendono ripercussioni negative importanti per l'economia o per le imprese, si rinuncia a un'analisi formale più approfondita dell'impatto della regolamentazione.

4 Programma di legislatura e strategie nazionali del Consiglio federale

La legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID) è annunciata nel messaggio del 27 gennaio 2016[45] sul programma di legislatura 2015–2019 e nel decreto federale del 14 giugno 2016[46] sul programma di legislatura 2015–2019.

Il presente disegno mira in particolare a conseguire gli obiettivi di diverse strategie del nostro Consiglio, altresì incluse nelle grandi linee del programma di legislatura 2015–2019. Nell'aprile 2016, ad esempio, il nostro Consiglio ha aggiornato la strategia «Svizzera digitale» definendo i campi d'intervento in cui il potenziale d'innovazione delle TIC possa esplicare effetti particolarmente importanti. I mezzi d'identificazione elettronica sicuri costituiscono i presupposti per l'attuazione di diversi campi d'intervento della strategia e rientrano nell'obiettivo prioritario «Trasparenza e sicurezza». Tali mezzi d'identificazione consentono agli abitanti della Svizzera di muoversi nel mondo virtuale con la medesima sicurezza che in quello reale e di esercitare la loro autodeterminazione in materia di informazione.

L'obiettivo operativo numero 5 delle linee guida della Strategia di e-government Svizzera punta a definire un'identità elettronica con validità nazionale e internazionale. Per promuovere l'innovazione e la piazza economica, la Svizzera deve disporre di un piano d'attuazione affidabile in vista di un'identità durevole nello spazio virtuale, il che crea prospettive a lungo termine per l'economia e la società digitale.

45 FF **2016** 909, 966 e 1026
46 FF **2016** 4605, 4607

5 Aspetti giuridici

5.1 Costituzionalità

La competenza per disciplinare l'eID risulta dalla Costituzione federale. Il rilascio di eID è delegato a gestori d'identità privati, che per essere riconosciuti dallo Stato devono soddisfare diversi presupposti, il che limita l'attività economica privata. L'articolo 95 capoverso 1 autorizza la Confederazione a emanare prescrizioni sull'esercizio dell'attività economica privata.

Inoltre, gli IdP che occupano una forte posizione sul mercato devono offrire gli eID agli aventi diritto alle stesse condizioni di quelle applicate alla gran parte della popolazione. Il progetto è volto a combattere gli effetti nocivi dell'attività economica di certi IdP importanti, segnatamente di quelli che dominano il mercato, vincolando la loro offerta di eID a condizioni e disciplinando così il loro campo d'attività. Il disegno si fonda quindi sull'articolo 96 capoverso 1 Cost., che conferisce alla Confederazione la competenza di emanare prescrizioni contro gli effetti economicamente o socialmente nocivi di cartelli e di altre forme di limitazione della concorrenza.

La LSIE contiene disposizioni che permettono di garantire agli aventi diritto un migliore accesso agli eID. Prevede anche un sistema di riconoscimento, di vigilanza e di sanzionamento degli IdP e va così a rafforzare la protezione dei consumatori. Si fonda quindi sull'articolo 97 capoverso 1 Cost., che conferisce alla Confederazione la facoltà di adottare misure di protezione dei consumatori.

Nella misura in cui riguarda i rapporti contrattuali tra i fornitori di servizi d'identificazione elettronica, i titolari e i gestori di servizi che utilizzano l'eID, la LSIE disciplina aspetti di diritto civile. Visto che questo aspetto non riveste un'importanza capitale, si rinuncia a menzionare l'articolo 122 capoverso 1 Cost., che conferisce alla Confederazione la competenza per legiferare nel campo del diritto civile.

5.2 Compatibilità con gli impegni internazionali della Svizzera

Il progetto è compatibile con gli impegni internazionali vigenti. Nel corso della sua elaborazione si è provveduto a preservare la possibilità di notifica secondo il regolamento eIDAS. Se auspicato in un secondo tempo, gli eID riconosciuti in Svizzera potranno ottenere il riconoscimento europeo. A tal scopo, sarebbe necessario concludere trattati internazionali.

5.3 Forma dell'atto

In ragione dell'oggetto, del contenuto e della portata del progetto legislativo, in virtù dell'articolo 164 capoverso 1 Cost. è necessario emanare le disposizioni sui servizi d'identificazione elettronica sotto forma di legge federale.

5.4 Subordinazione al freno alle spese

Secondo l'articolo 159 capoverso 3 lettera b Cost., il disegno richiede l'approvazione della maggioranza dei membri di ciascuna Camera, visto che comporta nuove spese ricorrenti di oltre 2 milioni di franchi.

5.5 Rispetto del principio di sussidiarietà e del principio dell'equità fiscale

L'introduzione dell'eID è incontestata. La prevista ripartizione dei compiti e il loro adempimento non violano né il principio di sussidiarietà né quello dell'equità fiscale. Le ripercussioni finanziarie per la Confederazione e i Cantoni sono inferiori a 10 milioni di franchi. Il progetto è quindi conforme ai citati principi.

5.6 Conformità alla legge sui sussidi

La LSIE non prevede né aiuti finanziari né indennità. L'attuazione è prevista sul libero mercato. I modelli commerciali corrispondenti sono già a disposizione. Il nostro Collegio rinuncia quindi a formulare ulteriori commenti.

5.7 Delega di competenze legislative

Procedure di verifica dell'identità e dei documenti d'identità

Il nostro Consiglio definirà in un'ordinanza le procedure per controllare i documenti d'identità dei cittadini svizzeri e verificare i documenti di legittimazione e l'identità dei cittadini stranieri. Tali procedure consentono di valutare la particolare situazione della persona interessata nel caso specifico. Questo non autorizza il nostro Collegio a escludere determinate categorie di persone, ma gli consente di introdurre procedure per valutare oggettivamente nel singolo caso se la persona interessata può essere identificata in modo affidabile e se soddisfa i requisiti per un eID. La competenza corrispondente è sancita all'articolo 3 capoverso 2 LSIE.

Prescrizioni tecniche e organizzative

Per poter reagire tempestivamente agli sviluppi tecnici, i presupposti per le procedure (riconoscimento degli IdP e livelli di sicurezza), le prescrizioni tecniche e gli standard sono disciplinati a livello di ordinanza o di direttiva.

Secondo l'articolo 4 capoverso 4, il nostro Consiglio disciplina i diversi livelli di sicurezza, in particolare i requisiti minimi dell'identificazione, tenendo conto dello stato della tecnica.

L'articolo 6 capoverso 5 conferisce al nostro Collegio la competenza di emanare prescrizioni dettagliate sulla procedura di rilascio degli eID e sui dati d'identificazione personale da utilizzare in occasione dell'identificazione. Vista la comples-

sità e l'elevato livello di dettaglio della materia da disciplinare, la normativa proposta va inserita in un'ordinanza piuttosto che nella legge. Il nostro Collegio definirà in un'ordinanza anche i dettagli sulla procedura di rilascio di eID per persone in possesso di un mezzo d'identificazione valido e conforme al diritto federale secondo l'articolo 29. Anche gli standard tecnici che garantiscono l'interoperabilità dei diversi sistemi di eID devono poter essere adeguati rapidamente alle nuove possibilità tecniche e vanno pertanto disciplinati in un'ordinanza (art. 18 cpv. 2 LSIE).

In virtù dell'articolo 13 capoverso 4, il nostro Consiglio può emanare prescrizioni sui presupposti per il riconoscimento degli IdP, in particolare sui requisiti tecnici e di sicurezza e il controllo degli stessi, la copertura assicurativa necessaria (o garanzie finanziarie equivalenti), nonché gli standard applicabili e i protocolli tecnici per i sistemi di eID e il controllo di questi ultimi. Gli standard internazionali e nazionali da applicare vengono rielaborati e ripubblicati a intervalli brevi. Emanando un'ordinanza, il nostro Consiglio può reagire più rapidamente a questi sviluppi rispetto al Parlamento.

Fedpol è il destinatario di un'ordinanza sui più recenti standard applicabili e sui protocolli tecnici per la trasmissione di dati d'identificazione personale. Il nostro Consiglio disciplinerà la procedura di rettifica per il caso in cui differenti registri di persone forniscano dati contradditori (art. 23 cpv. 3 LSIE).

Infine, il nostro Collegio disciplinerà le misure tecniche e organizzative per il trattamento e la trasmissione sicuri dei dati d'identificazione personale in base all'articolo 24 capoverso 4. Queste misure devono poter essere adeguate rapidamente agli sviluppi tecnici, per cui conviene disciplinarle in un'ordinanza.

Sistema di eID sussidiario della Confederazione

Se nessun IdP rilascia eID del livello di sicurezza significativo o elevato, il nostro Consiglio può designare un'unità amministrativa che gestisca un sistema di eID e rilasci eID (art. 10 cpv. 1 LSIE).

Norme di protezione di responsabilità civile per titolari

Il nostro Consiglio può disciplinare in un'ordinanza gli obblighi di diligenza del titolare di un eID (art. 12 cpv. 3 LSIE), nonché il blocco e la revoca di un eID (art. 11 cpv. 5 LSIE). Tali obblighi devono poter essere modificati rapidamente in funzione dell'evoluzione tecnica. È quindi opportuno disciplinare questi dettagli in un'ordinanza.

Riscossione di emolumenti

Rimandiamo ai commenti all'articolo 27.

5.8 Protezione dei dati

5.8.1 Osservazioni generali

Uno degli scopi della LSIE è la protezione dei dati. L'articolo 1 capoverso 2 lettera b riprende peraltro lo scopo enunciato all'articolo 1 LPD. Le norme in materia di protezione dei dati (LPD e relative ordinanze) si applicano a tutte le parti coinvolte. Gli IdP e i gestori di servizi che utilizzano l'eID in particolare sottostanno alle disposizioni applicabili ai privati, mentre fedpol e l'ODIC sono soggetti alle normative riferite agli organi federali. Per motivi di trasparenza, la LSIE riprende e precisa determinati requisiti della legge sulla protezione dei dati inasprendone le condizioni in alcuni casi.

Vengono introdotte disposizioni esplicite riguardo all'obbligo di ottenere il consenso del titolare dell'eID nonché restrizioni al trattamento dei dati d'identificazione personale confermati dallo Stato. Gli IdP possono trattare questi dati soltanto ai fini dell'identificazione secondo la LSIE (art. 9 cpv. 1 LSIE). Infine, gli IdP non possono comunicare a terzi né i dati d'identificazione personale né i dati generati dall'utilizzo dell'eID, compresi i profili basati su tali dati (art. 16 cpv. 2 LSIE).

5.8.2 Consenso alla trasmissione

Laddove vengono utilizzati dati d'identificazione personali, è importante che siano rispettate le condizioni della protezione dei dati e adottati i necessari provvedimenti di sicurezza. I titolari dell'eID devono acconsentire esplicitamente alla trasmissione dei dati d'identificazione personale. Il rilascio dell'eID autorizza gli IdP a procurarsi questi dati presso fedpol (art. 6 cpv. 2 lett. c LSIE), e ogni qualvolta che gli IdP utilizzano l'eID presso un gestore di servizi che utilizza l'eID dovranno chiedere nuovamente il consenso al titolare prima di trasmettere i dati al gestore (art. 16 cpv. 1 lett. c LSIE).

5.8.3 Separazione dei dati d'identificazione personale dai dati generati dall'utilizzo dell'eID

La LSIE prevede misure di sicurezza specifiche, più rigide della legge sulla protezione dei dati quanto all'obbligo di garantire la sicurezza dei dati. L'articolo 9 capoverso 3 esige che l'IdP conservi i dati d'identificazione personale di cui all'articolo 5, i dati di utilizzo dell'eID e gli altri dati separatamente gli uni dagli altri. La separazione fisica e organizzativa, a seconda del tipo di dati e dello scopo del loro trattamento, rappresenta un'ulteriore misura di sicurezza volta a impedire che persone non autorizzate accedano a tutti i dati che riguardano il titolare dell'eID. S'intende così limitare le conseguenze negative di un accesso non autorizzato al sistema. La separazione garantisce inoltre la sicurezza dei dati di una categoria anche quando quella di una delle altre è compromessa.

5.8.4 Accesso ai dati d'identificazione personale e ai dati generati dall'utilizzo dell'eID

La legge intende rafforzare il principio di cui all'articolo 4 capoverso 4 LPD, in base al quale la finalità del trattamento dei dati dev'essere riconoscibile, e il diritto d'accesso ai dati personali di cui all'articolo 8 LPD. Secondo l'articolo 15 capoverso 1 lettera i LSIE, l'IdP accorda al titolare dell'eID l'accesso in linea ai dati generati dall'utilizzo dell'eID e ai suoi dati d'identificazione personale di cui all'articolo 5. Questa misura contribuisce al contempo a rendere il sistema di eID più trasparente e rafforza la fiducia degli utenti nella procedura di rilascio dell'eID.

5.8.5 Scopo e limitazioni

Le finalità e le condizioni per il trattamento, la conservazione e la trasmissione dei dati sono rigorosamente disciplinate dalla presente legge. L'articolo 9 capoverso 1 LSIE prevede segnatamente che l'IdP può trattare i dati d'identificazione personale trasmessi da fedpol soltanto fino alla revoca dell'eID e al solo scopo di effettuare identificazioni secondo la legge. In virtù dell'articolo 16 capoverso 1, l'IdP può trasmettere ai gestori di servizi che utilizzano l'eID unicamente i dati d'identificazione personale corrispondenti al livello di sicurezza richiesto e necessari all'identificazione della persona interessata nel caso specifico, sempreché il titolare abbia acconsentito alla trasmissione. Alle immagini del viso registrate nel sistema d'informazione di fedpol si applicano regole particolari: possono essere impiegate per gli eID del livello di sicurezza significativo unicamente durante la procedura di rilascio ed essere inserite soltanto negli eID del livello di sicurezza elevato.

La trasmissione dei dati secondo la LSIE è necessaria per garantire il corretto funzionamento del sistema di eID nonché la comodità, la flessibilità e la semplicità richieste dagli utenti. Il principio di proporzionalità è rispettato poiché la prevista ingerenza nella sfera privata non va oltre a quanto strettamente necessario all'adempimento dello scopo previsto. I dati personali da trasmettere, del resto, non sono degni di particolare protezione secondo l'articolo 3 lettera c LPD.

Secondo gli articoli 17 capoverso 1 e 19 capoverso 1 LPD, gli organi federali hanno il diritto di trattare e comunicare i dati personali soltanto se esiste una pertinente base legale. In applicazione degli articoli 3 lettera i e 4 capoversi 3 e 4 LPD, lo scopo del sistema previsto deve essere definito chiaramente ed essere riconoscibile per le persone interessate. Di conseguenza, la legge prevede disposizioni precise che consentono a fedpol di gestire un sistema d'informazione per l'identificazione dei richiedenti. L'articolo 24 definisce il tipo, il contenuto e lo scopo del sistema. Secondo l'articolo 24 capoverso 1, il sistema contiene i dati verbalizzati nella procedura di rilascio secondo l'articolo 6 capoverso 5, i dati d'identificazione personale di cui all'articolo 5, nonché la loro origine e le informazioni sul loro aggiornamento, e i numeri d'assicurato. L'articolo 24 capoverso 2 precisa le finalità del sistema: ricevere le domande e le dichiarazioni di consenso del richiedente, adempiere in modo automatizzato i compiti di fedpol nel quadro del rilascio degli eID, aggiornare i dati d'identificazione personale secondo l'articolo 7 e verificare la validità di un numero di registrazione eID secondo l'articolo 23 capoverso 2.

5.8.6 Divieto della commerciabilità dei dati

La vendita di dati trattati, conservati e trasmessi secondo la LSIE è rigorosamente limitata. Secondo l'articolo 16 capoverso 2, l'IdP non può comunicare a terzi né i dati d'identificazione personale di cui all'articolo 5 né i dati generati dall'utilizzo dell'eID, compresi i profili basati su tali dati. Il divieto vale indipendentemente dal livello di sicurezza degli eID. I dati secondo la LSIE non possono pertanto essere venduti a terzi.

Il divieto della commerciabilità riduce il valore economico dei dati d'identificazione personale confermati a livello statale, che sono pertanto esplicitamente non pignorabili e non rientranti nella massa fallimentare (art. 14 cpv. 1 LSIE). Per garantire la continuità di un sistema di eID secondo la LSIE e delle corrispondenti eID, un IdP in difficoltà finanziarie potrà vendere l'insieme del suo sistema di eID a un altro IdP. Il relativo importo fa parte di un'eventuale massa fallimentare (art. 14 cpv. 3 LSIE).

Glossario

Termine	Definizione
autenticazione f = authentification d = Authentifizierung	Processo di verifica di un'identità asserita in occasione dell'utilizzo di un eID nel quadro del quale il titolare dell'eID prova la propria identità all'IdP. A tal fine deve innanzitutto identificarsi comunicando al sistema il proprio nome d'utente, che dovrà poi autenticare inviando al sistema la parola chiave corrispondente; in questo modo il sistema potrà verificare se il titolare dell'eID è veramente la persona che afferma di essere.
dati d'identificazione personale f = données d'identification personnelle d = Personenidentifizierungsdaten	Insieme di dati gestito dallo Stato in Infostar, ISA, SIMIC e Ordipro e che consente di stabilire l'identità di una persona.
fornitori di servizi d'identificazione elettronica (*identity provider; IdP)* f = fournisseur d'identité d = Identity Provider (IdP)	Fornitori di servizi d'identificazione elettronica riconosciuti secondo la LSIE.
gestori di servizi che utilizzano l'eID f = exploitant d'un service utilisateur d = Betreiberin von E-ID-verwendenden Diensten	Persona fisica o giuridica che gestisce, ai fini dell'esercizio della sua attività, uno o più servizi in rete riservati a utenti con un'identità affidabile e autenticata. Termine inglese: *relying party*.
identificazione f = identification d = Identifizierung	Processo di accertamento dell'identità di una persona attraverso i dati d'identificazione personale che la rappresentano in modo univoco.
Identity and Access Management (IAM) f = gestion des identités et des accès (GIA) d = Identity and Access Management (IAM)	Insieme di processi e applicazioni che permettono di gestire le identità e i diritti d'accesso a diverse applicazioni, sistemi e risorse.

Termine	Definizione
interoperabilità f = interopérabilité d = Interoperabilität	La capacità di diversi sistemi, tecniche o organizzazioni di interagire grazie al rispetto di standard comuni. I sistemi di radiotelefonia mobile, ad esempio, sono interoperabili.
mezzo d'identificazione elettronica f = moyen d'identification électronique d = elektronische Identifizierungseinheit	Mezzo elettronico utilizzato per l'identificazione e l'autenticazione di una persona fisica.
mezzo d'identificazione elettronica riconosciuto f = moyen d'identification électronique reconnu (e-ID) d = anerkannte elektronische Identifizierungseinheit (E-ID)	Mezzo d'identificazione elettronica rilasciato da un IdP secondo quanto stabilito nella LSIE. Può fungere da supporto uno *smartphone* o una carta elettronica.
National Institute of Standards and Technology (NIST)	Agenzia statunitense aggregata all'amministrazione tecnologica del Dipartimento del commercio e competente per i processi di standardizzazione.
numero di registrazione eID f = numéro d'enregistrement de l'e-ID d = E-ID-Registrierungsnummer	Numero d'identificazione univoco attribuito a una persona.
Ordipro	Sistema d'informazione del Dipartimento federale degli affari esteri. Serve in particolare al disbrigo amministrativo di questioni legate all'accreditamento, al rilascio e alla gestione delle diverse categorie di documenti di legittimazione per le persone beneficiarie secondo l'articolo 2 capoverso 2 della legge del 22 giugno 2007 sullo Stato ospite (RS *192.2*).
procedura di riconoscimento f = procédure de reconnaisance d = Anerkennungsverfahren	Nel quadro di questa procedura, il servizio federale competente riconosce gli IdP e i loro sistemi di eID, purché questi soddisfino le condizioni professionali, organizzative, tecniche e di sicurezza. Il riconoscimento è controllato e rinnovato periodicamente.

Termine	Definizione
registro informatizzato dello stato civile (Infostar) f = registre de l'état civil (Infostar) d = Personenstandregister (Infostar)	Registro informatizzato dello stato civile che documenta tutti gli eventi di stato civile. Tutti gli ufficiali dello stato civile svizzeri sono collegati a Infostar.
regolamento eIDAS f = règlement eIDAS d = eIDAS-Verordnung	Regolamento dell'UE in materia di identificazione elettronica e servizi fiduciari (*electronic IDentification, Authentication and trust Services*), volto ad assicurare l'interoperabilità dei sistemi d'identificazione e a semplificare notevolmente l'identificazione ai fini della fornitura transfrontaliera di servizi amministrativi a livello europeo.
servizi che utilizzano l'eID f = service utilisateur d = E-ID-verwendender Dienst	Applicazione informatica che utilizza un sistema eID a fini d'identificazione e di autenticazione.
servizio d'informazione per documenti d'identità (ISA) f = système d'information relatif aux documents d'identité (ISA) d = Informationssystem Ausweisschriften (ISA)	Sistema d'informazione contenente i dati registrati in occasione del rilascio di un documento d'identità a un cittadino svizzero.
Servizio delle identità f = service d'identité d = Identitätsstelle	L'Ufficio federale di polizia (fedpol) è il Servizio delle identità secondo la LSIE. Al Servizio compete in particolare l'esame delle indicazioni fornite dal richiedente nel quadro dell'identificazione.
Servizio di riconoscimento f = organisme de reconnaisance d = Anerkennungsstelle	L'Organo direzione informatica della Confederazione (ODIC) è il Servizio di riconoscimento secondo la LSIE. Al Servizio compete in particolare il ricevimento e l'esame delle domande di riconoscimento degli IdP e dei loro sistemi di IdP.

Termine	Definizione
sistema d'informazione centrale sulla migrazione (SIMIC) f = système d'information central sur la migration (SYMIC) d = Zentrales Migrations-informationssystem (ZEMIS)	Sistema d'informazione della Segreteria di Stato della migrazione SEM. In SIMIC sono trattati i dati del settore degli stranieri e dell'asilo.
sistema di eID f = système e-ID d = E-ID-System	Sistema elettronico per il rilascio, la gestione e l'utilizzo di eID.
SuisseID	Mezzo d'identificazione elettronica ideato dalla SECO e disponibile sotto forma di tessera elettronica o di chiave USB. SuisseID consente agli utenti di fruire di prestazioni elettroniche, a condizione che si siano identificati in modo sicuro e abbiano apportato una firma elettronica legalmente valida su un documento.
SwissID	Mezzo d'identificazione elettronica di SwissSign. Nello sviluppare SwissID, si è tenuto conto delle esperienze raccolte con SuisseID. Il nuovo Servizio sarà istituito a tappe – a medio termine SwissID sostituirà SuisseID.
Unique Person Identification (UCC-UPI) f = (CdC-UPI) d = (ZAS-UPI)	Strumento che consente di identificare le persone fisiche e di amministrare l'identificatore NAVS13 (numero d'assicurato) nel registro centrale degli assicurati delle assicurazioni sociali federali.