Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di giustizia UFG

Berna, 22 febbraio 2017

Legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID)

Rapporto esplicativo sull'avamprogetto

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 l'esecuzione di transazioni nel mondo digitale. I giovani utenti di Internet, che sono adeguatamente formati, hanno familiarità con le tecnologie, sono molto ben connessi e sempre online, favoriscono questo cambiamento di natura socioeconomica. Per svolgere in rete anche transazioni più complesse, i partner (qui di seguito denominati gestori di servizi che utilizzano identità elettroniche) devono poter fare affidamento sull'identità e sull'autenticazione 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 d'identificazione. Un'eID consente a un gestore di un servizio che utilizza l'eID di identificare e autenticare online il titolare come avente diritto.

L'affidabilità delle eID contribuisce dunque a implementare le 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 messi a disposizione 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 (Identity Provider, IdP) 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 nel 2014 e nel 2015.

Il piano è stato sostanzialmente rielaborato sulla base dei riscontri e delle esperienze di altri Paesi. Lo sviluppo di soluzioni statali proprie ed eID rilasciate dallo Stato comporta di regola costi informatici scoperti troppo elevati per l'ente pubblico (p. es. per il supporto, i dispositivi di lettura, il software) poiché queste soluzioni non consentono di reagire con sufficiente flessibilità alle esigenze e alle tecnologie in rapida evoluzione. Per contro si stanno diffondendo offerte d'identificazione elettronica a diversi livelli dell'economia privata (p. es. Apple-ID, Google ID, Mobile ID, OpenID, SuisseID, SwissPass ecc.), ma per ora risulta molto difficile valutare quali delle eID attualmente diffuse supereranno la prova del tempo. Il nuovo piano si fonda dunque su una ripartizione dei compiti tra Stato e privati.

Parallelamente ai risultati della consultazione sono stati considerati anche i più recenti sviluppi nell'UE, verificando tra l'altro la compatibilità giuridica del piano con il regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identifica-

zione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE[1] (regolamento eIDAS).

Il 13 gennaio 2016 il Consiglio federale ha preso atto del piano eID, incaricato il DFGP di elaborare una pertinente legge e stabilito le condizioni quadro per la legislazione.

1.2 La nuova normativa proposta

1.2.1 Piano eID

La certezza del diritto e la sicurezza sono premesse essenziali per lo svolgimento delle transazioni. Ciò include un'adeguata conoscenza dell'identità delle parti coinvolte. Per il mondo fisico, la Confederazione rilascia già oggi mezzi d'identificazione tradizionali: il passaporto svizzero, la carta d'identità e la carta di soggiorno. A integrazione di tutto questo, ora dovrà essere possibile provare l'identità di una persona fisica anche in un ambiente elettronico. Le eID riconosciute a livello statale consentiranno a chi ne è in possesso di registrarsi in modo sicuro sui servizi online e successivamente di fare il login sempre in sicurezza. I gestori dell'identità digitale possono offrire ulteriori servizi fiduciari, come la firma elettronica, che però non costituiscono un elemento dell'eID.

Il piano per l'eID, ora attuato, si basa sui lavori svolti da fedpol negli anni 2013-2015, nel cui ambito sono stati consultati anche importanti attori del mercato. Tiene inoltre conto delle conoscenze relative a soluzioni precedenti per sistemi di eID di altri Paesi, degli sviluppi internazionali relativi a soluzioni pratiche per sistemi di eID e delle prescrizioni relative alla compatibilità UE del regolamento eIDAS.

1.2.2 Ripartizione dei compiti tra Stato e mercato

L'avamprogetto (AP) si fonda su una ripartizione dei compiti tra Stato e mercato. La necessaria accettazione dell'eID va raggiunta tramite condizioni quadro giuridiche e organizzative che infondano fiducia e dipende dalla capacità performativa e dal dinamismo del mercato. Recentemente sono divenute di pubblico dominio due iniziative private che confermano la soluzione scelta. Le grandi banche Credit Suisse e UBS collaborano assieme a Swisscom a un progetto volto a introdurre un «passepartout» per Internet. Nel quadro di un altro progetto, la SBB e la Posta intendono offrire soluzioni comuni per l'accesso a portali in rete.

Secondo l'avamprogetto, la Confederazione autorizzerà gli IdP che soddisfano i presupposti a rilasciare eID riconosciute e a gestire sistemi di eID riconosciuti. Tutti i sistemi di eID riconosciuti dovranno essere interoperabili tra loro per procurare un grande beneficio ai clienti.

1.2.3 Funzione dell'eID

Con un'eID le persone fisiche possono registrarsi su un portale Internet (servizio che utilizza l'eID) e accedervi successivamente in modo sicuro e agevole. Per la registrazione non occorre inserire manualmente i dati personali, che sono trasmessi elettronicamente tramite l'eID dopo il consenso del titolare. Se successivamente visita di nuovo il portale, il titolare si identifica e autentica con l'eID. Una volta registrata, l'eID viene riconosciuta e garantisce un

[1] Il link al riferimento nella banca dati giuridica dell'UE Eur-Lex è riportato nella bibliografia.

accesso affidabile. L'eID costituisce dunque una delle basi per un utilizzo sicuro di servizi in rete.

Si distingueranno tre livelli di sicurezza, come previsto pure dall'UE per le eID dei suoi Stati membri e dagli Stati Uniti per i servizi fiduciari. Dal canto suo, mediante un'interfaccia elettronica la Confederazione mette a disposizione degli IdP i dati d'identificazione personale gestiti a livello statale (numero di registrazione eID, cognome, nomi, ecc.). La prima trasmissione dei dati a un IdP o a un gestore di un servizio che utilizza l'eID richiede il consenso esplicito della persona in questione (cfr. art. 6 e 17 cpv. 1 lett. f AP). L'utilizzo quotidiano dell'eID avviene però senza dover ricorrere ulteriormente all'infrastruttura della Confederazione.

Il rispetto delle prescrizioni in materia di processi e standard tecnici da parte degli IdP è verificato regolarmente dal Servizio di riconoscimento dei fornitori di servizi identitari (Servizio di riconoscimento, unità amministrativa della Confederazione, art. 21 AP; cfr. artt. 4, 11 e 12 AP). Se l'esito della verifica è positivo, il riconoscimento è conferito o prorogato. I dettagli relativi ai processi e standard da rispettare vengono disciplinati a livello di ordinanza ed eventualmente di istruzioni e sono armonizzati con le esistenti regole per le firme elettroniche[2] e le piattaforme di trasmissione, così che gli IdP possano beneficiare di sinergie nell'ambito delle certificazioni richieste. La procedura di riconoscimento dei sistemi di eID è simile a quella vigente per le piattaforme per la trasmissione sicura di documenti elettronici nel quadro di processi civili e penali nonché a quelle del settore dell'esecuzione e del fallimento. È pubblicato un elenco degli IdP riconosciuti e dei loro sistemi di eID (art. 22 AP).

1.2.4 Rilascio di un'eID

Di norma, un'eID è rilasciata dopo che il richiedente si è presentato personalmente a un IdP. La registrazione comprende un'identificazione che, a dipendenza del livello di sicurezza, è effettuata elettronicamente o nel quadro di un incontro. La procedura di registrazione è suddivisa in varie fasi (cfr. art. 6 e 17 cpv. 1 lett. b AP).

1. Chi desidera un'eID ne richiede il rilascio a un IdP. A seconda del livello di sicurezza l'IdP esige che il richiedente si presenti di persona o virtualmente (p. es. nel quadro di una videoidentificazione).
2. L'IdP controlla il documento presentato (passaporto, CID o carta di soggiorno) e inoltra al Servizio svizzero delle identità elettroniche (Servizio delle identità) una domanda elettronica di conferma dei dati del documento.
3. Il Servizio delle identità confronta i dati trasmessi dall'IdP con i dati d'identificazione personale contenuti nei registri di persone della Confederazione.
4. Il richiedente dà il suo consenso all'attribuzione dei suoi dati d'identificazione personale a un numero di registrazione eID e alla trasmissione di entrambi all'IdP.
5. Il Servizio delle identità trasmette all'IdP il numero di registrazione eID con i dati confermati.
6. L'IdP attribuisce un mezzo di autenticazione (supporto dell'eID) al richiedente che permetta a quest'ultimo di identificarsi in rete.
7. L'IdP provvede ad attribuire correttamente all'eID il numero di registrazione eID e il mezzo d'autentificazione 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

[2] Cfr. legge del 18 marzo 2016 sulla firma elettronica, FiEle; RS 943.03

sono definiti tramite standard e protocolli tecnici.

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 e favorire manovre elusive, nonché aumentare i costi. Questo non è positivo né per l'accettazione né per la sicurezza di un sistema di eID. Pertanto vengono riconosciuti sistemi di eID che offrono tre livelli di sicurezza distinti per il rilascio, la gestione e l'utilizzo nonché, eventualmente, per altre misure di sicurezza tecniche e organizzative.

La legge definisce unicamente le possibili categorie di eID, ossia i livelli di sicurezza (cfr. art. 5 AP), ognuno dei quali offre un diverso grado di affidabilità. I livelli di sicurezza che entrano in considerazione per i diversi tipi di applicazione sono definiti dallo Stato nelle relative disposizioni speciali o dai gestori privati di servizi che utilizzano l'eID. Per la formazione in rete (e-education), ad esempio, potrà essere scelto un altro livello di sicurezza rispetto a 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 pertinenti disposizioni d'esecuzione[3]. Si distingue tra livelli di sicurezza *basso*, *significativo* ed *elevato*. Ognuno di questi offre un diverso grado di affidabilità dei dati attribuiti. In linea di massima, i livelli di sicurezza *significativo* ed *elevato* possono essere impiegati anche per servizi che utilizzano l'eID per i quali è sufficiente un livello basso.

I tre livelli di sicurezza per le eID riconosciute in Svizzera sono definiti in modo da soddisfare i requisiti in materia di sicurezza vigenti per i livelli di garanzia fissati dall'articolo 8 del regolamento eIDAS e dalle pertinenti disposizioni d'esecuzione. Questi livelli, pure corrispondenti a quelli definiti dal NIST[4] per le applicazioni di governo elettronico negli Stati Uniti, costituiscono a tutt'oggi degli standard internazionali. Al fine di adempiere al suo scopo, ogni livello si distinguerà per le specifiche tecniche, norme e procedure - incluse le verifiche tecniche – che gli saranno proprie. I vari livelli dovranno essere ancora oggetto di riflessioni approfondite.

Questo modello consentirà ad esempio di registrare in un primo *significativo* a un livello *basso* un'eID che dal punto di vista tecnico richiederebbe un livello *significativo*, per poi portarla successivamente, mediante un incontro personale, a un livello di sicurezza più elevato, agevolando in tal modo l'accesso a sistemi di eID riconosciuti. Con il livello di sicurezza *basso*, l'accesso a eID riconosciute 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 numerose eID di diversi IdP a vari livelli di sicurezza.

Livello di sicurezza *basso*
L'eID di livello di sicurezza *basso* ha lo scopo di ridurre il rischio di un uso abusivo o di un'alterazione dell'identità. A tale livello sono attribuiti soltanto pochi dati (cognome, nomi, data di nascita e numero di registrazione eID; cfr. art. 7 cpv. 1 AP). La registrazione può essere effettuata in rete fondandosi su un documento statale. L'utilizzo dell'eID richiede almeno un fattore di autenticazione ed è dunque comparabile a un badge d'accesso o a una soluzio-

[3] Cfr. la sintesi nella bibliografia.

[4] National Institute of Standards and Techonology, U.S. Department of Commerce

ne di pagamento senza contatto per piccoli importi.

Livello di sicurezza *significativo*
Questo livello si riferisce a un mezzo d'identificazione elettronica con un grado *significativo* di affidabilità dell'identità pretesa o dichiarata. L'eID di questo livello ha lo scopo di ridurre notevolmente il rischio di un uso abusivo o di un'alterazione dell'identità. La registrazione è effettuata sulla base di un incontro personale presso l'IdP o di una videoidentificazione supportata da un documento statale. Nel livello di sicurezza *significativo*, al nome e alla data di nascita si aggiungono altri dati d'identificazione personale (p. es. il sesso, il luogo di nascita, lo stato civile; cfr. art. 7 cpv. 2 AP). L'utilizzo dell'eID richiede almeno due fattori di autenticazione ed è quindi comparabile ad esempio alle soluzioni usuali nel settore bancario (carte di conto, carte di credito con PIN, soluzioni di e-banking).

Livello di sicurezza *elevato*
L'eID di livello di sicurezza *elevato* ha lo scopo di prevenire il rischio di un uso abusivo o di un'alterazione dell'identità. La registrazione è effettuata sulla base di un incontro personale presso l'IdP o di una videoidentificazione supportata da un documento statale; si procede inoltre a verificare l'autenticità del documento e almeno una caratteristica biometrica fondandosi su una fonte dell'autorità (validità del documento e immagine del viso o un'altra caratteristica biometrica di riconoscimento). Con il livello di sicurezza *elevato*, al numero di registrazione eID sono attribuiti tutti i dati d'identificazione personale disponibili (cfr. art. 7 cpv. 2 AP). Il mezzo di autenticazione dell'eID deve infine soddisfare requisiti molto elevati in materia di sicurezza tecnica.

L'utilizzo dell'eID richiede almeno due fattori di autenticazione, di cui uno deve essere biometrico («fattore inerente» secondo il regolamento d'esecuzione eIDAS). L'eID corrisponde a uno smartphone con riconoscimento tramite l'impronta digitale, il volto o la voce. L'autenticazione biometrica crea un collegamento ancora più stretto tra l'eID e il 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. Nell'ottica dell'uso abusivo dell'identità, il titolare deve poter essere protetto anche da attacchi informatici contro il mezzo di autenticazione dell'eID stesso e contro altri dispositivi tecnici eventualmente necessari per l'impiego del mezzo di autenticazione dell'eID ma non rientranti nel campo d'applicazione della presente legge. Transazioni abusive in nome altrui devono poter essere impedite anche se i dispositivi tecnici sono stati manipolati mediante un attacco informatico o se ne sono state estratte informazioni. Per garantire questa protezione, il mezzo d'autenticazione deve fondarsi su componenti particolarmente affidabili e conformi allo stato della tecnica.

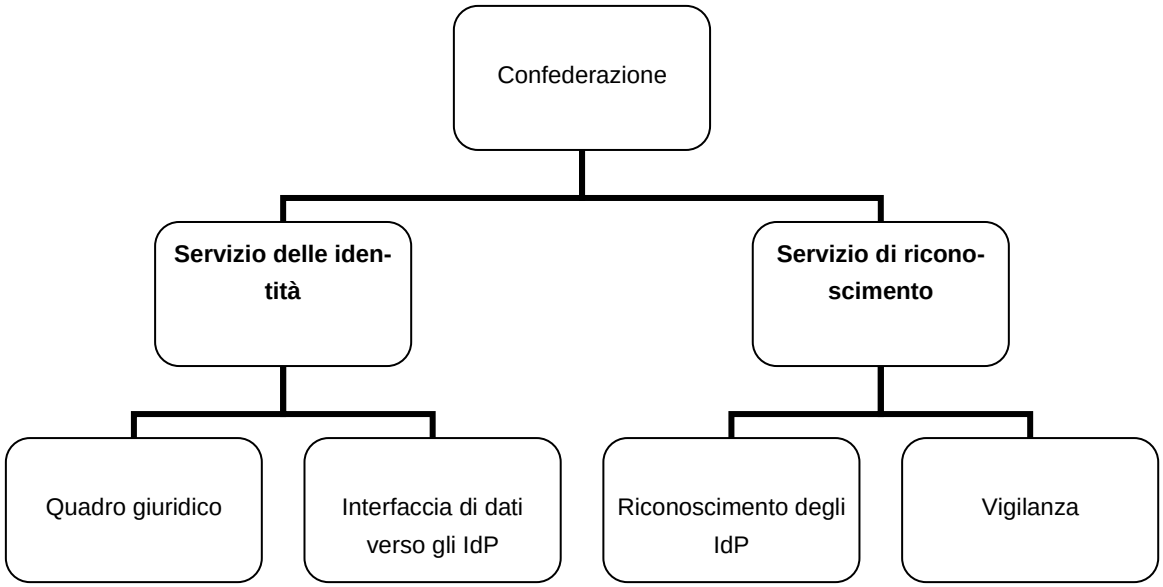
1.2.6 Contributo dello Stato ai sistemi di eID

Panoramica
Un'eID riconosciuta a livello statale 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. La conferma dell'identità di una persona da parte dello Stato è ritenuta particolarmente affidabile a tutti i livelli dell'organizzazione federale, grazie al fatto che l'identificazione viene effettuata regolarmente presso un servizio statale in occasione del rilascio di un documento.

La Confederazione garantisce che i sistemi di eID riconosciuti siano affidabili e assume numerosi compiti pertinenti:
1. elabora e aggiorna le basi legali creando trasparenza e sicurezza;

2. definisce gli standard nonché i requisiti di sicurezza e interoperabilità da rispettare per gestire un sistema di eID;
3. gestisce un'interfaccia elettronica tramite la quale gli IdP riconosciuti possono acquisire dati d'identificazione personale tenuti dallo Stato;
4. riconosce gli IdP e i loro sistemi di eID; e
5. esercita la vigilanza sugli IdP e sui loro sistemi di eID.

Sempre secondo l'AP, questi compiti andranno assunti da due unità amministrative della Confederazione: il Servizio svizzero delle identità elettroniche (Servizio delle identità) e il Servizio di riconoscimento dei fornitori di servizi identitari (Servizio di riconoscimento).

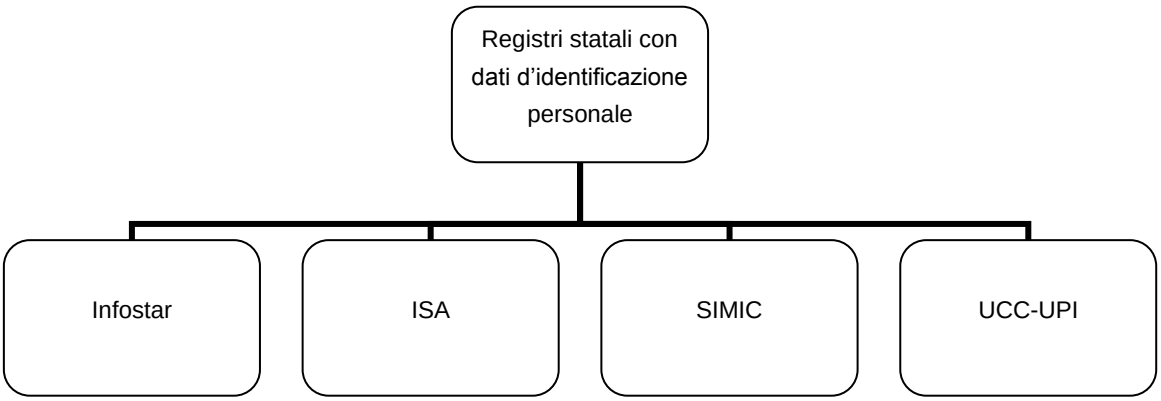


Registro con dati d'identificazione personale

Le autorità svizzere dei diversi livelli federali 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[5]). 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).

La legge del 23 giugno 2006 sull'armonizzazione dei registri (LArRa; RS 431.02) stabilisce che il NAVS13 è l'unico e univoco identificatore delle persone nei registri che raccolgono i dati dei censimenti della popolazione. Tali registri comprendono il registro delle persone della Confederazione nonché i registri cantonali e comunali degli abitanti. Non avendo accesso a questi ultimi, la Confederazione non può confermare i dati relativi al domicilio.

5 UPI è l'acronimo di «Unique Person Identification»



Relazione tra l'identificatore personale 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 particolari per i quali vi è una base legale formale. L'utilizzazione sistematica del NAVS13 cela il rischio del collegamento di gruppi 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[6] su l'assicurazione per la vecchiaia e per i superstiti (LAVS). L'articolo 50*a* 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[7] sulla parte generale del diritto delle assicurazioni sociali (LPGA). Secondo l'articolo 50*e* LAVS, l'utilizzazione sistematica del NAVS13 è ammessa soltanto se lo prevede una legge federale e se sono definiti lo scopo d'utilizzazione e gli aventi diritto.

Conformemente al decreto del Consiglio federale, le istituzioni senza carattere di autorità alle quali la legge ha conferito un compito pubblico dovrebbero essere autorizzate a utilizzare il NAVS13, a condizione che lo preveda una legge speciale. Il NAVS13 è sovente utilizzato nel quadro delle relazioni tra cittadini e servizi amministrativi. Se in futuro tale numero non dovesse poter essere rilevato e confermato dagli IdP, andrebbero previste onerose soluzioni di aggiramento, il che aumenterebbe notevolmente la complessità dei sistemi e ridurrebbe l'attrattiva dell'eID. Occorre pertanto autorizzare gli IdP a utilizzare sistematicamente il NAVS13 soltanto per questo scopo limitato. Gli IdP dovrebbero poter comunicare il NAVS13 unicamente ai gestori di servizi che utilizzano l'eID e sono a loro volta autorizzati a utilizzare sistematicamente il NAVS13 (art. 9).

Le restanti persone private devono per contro essere escluse dall'utilizzazione sistematica 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 numero di registrazione eID. Quest'ultimo serve anche a collegare la persona con l'eID rilasciata. La richiesta di un'eID è facoltativa e prevedibilmente connessa a spese. Inoltre, dato che soltanto i titolari di un documento svizzero o di una carta di soggiorno possono ottenere un'eID, il numero di registrazione eID non è complessivamente idoneo a fungere da identificatore personale generale.

6 RS **831.10**
7 RS **830.1**

Servizio svizzero delle identità elettroniche (Servizio delle identità)
Quadro giuridico
In collaborazione con il Servizio di riconoscimento, il Servizio delle identità cura 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 nel campo del riconoscimento degli IdP e dei sistemi di eID agli sviluppi tecnici e socioeconomici e alle attuali esigenze in materia di sicurezza.

Le condizioni quadro prescritte dal Consiglio federale esigono che il quadro giuridico sia elaborato in modo da consentire, in linea di principio, un riconoscimento successivo dell'eID presso l'UE o singoli Stati dell'UE. L'AP rispetta le prescrizioni del regolamento eIDAS e delle disposizioni esecutive[8] dell'UE.

Interfaccia
Il Servizio delle identità mette a disposizione degli IdP riconosciuti i dati d'identificazione personale tramite un'interfaccia elettronica (art. 20 AP). L'introduzione di un numero di registrazione eID consente di attribuire in modo univoco e duraturo i dati d'identificazione personale a una persona e alla sua eID senza che possa essere contestato. Questa interfaccia è accessibile esclusivamente agli IdP riconosciuti.

Il Servizio delle identità 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.

Il Servizio delle identità ottiene i diversi dati d'identificazione personale da diversi registri (art. 20 AP). Il cognome della persona è confermato sulla base dei dati di Infostar, mentre per esempio il numero del documento d'identità proviene da ISA e l'immagine del volto da SIMIC. I dati d'identificazione personale possono essere integrati con metadati supplementari come un riferimento alla fonte o la data del rilevamento (art. 7 cpv. 3 AP).
Gli IdP sono tenuti ad aggiornare periodicamente i dati d'identificazione personale attribuiti a un numero di registrazione eID: a dipendenza del livello di sicurezza annualmente (livello basso), trimestralmente (significativo) o settimanalmente (elevato) (art. 8 cpv. 1 AP).

Servizio di riconoscimento dei fornitori di servizi identitari (Servizi di riconoscimento)
Riconoscimento
Gli IdP (dell'economia privata o dell'ente pubblico) che soddisfano i presupposti possono farsi riconoscere assieme ai loro sistemi di eID da un Servizio di riconoscimento 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 solo alcuni di essi. A tal scopo il Consiglio federale stabilisce i requisiti giuridici, organizzativi e tecnici per gli IdP, il cui adempimento è verificato dal Servizio di riconoscimento.

Il Servizio di riconoscimento pubblica un elenco degli IdP e dei sistemi di eID riconosciuti, sulla cui base i gestori di servizi che utilizzano l'eID e le persone fisiche possono controllare lo statuto di un'eID o sistema di eID concreti (art. 22 AP).

Vigilanza

[8] Cfr. la sintesi nella bibliografia

Il Servizio di riconoscimento esercita la vigilanza sugli IdP e sui sistemi di eID riconosciuti e reagisce in caso di non adempimento delle prescrizioni o di eventi nell'ambito della sicurezza informatica. A tal scopo, a determinati intervalli esige le necessarie dimostrazioni di conformità dagli IdP riconosciuti e le verifica. Può imporre a un IdP o a un sistema di eID l'adozione di misure e a determinate condizioni revocare il riconoscimento (art. 12 AP).

1.3 Motivazione e valutazione della soluzione proposta

1.3.1 Soluzione sviluppata dal mercato

Già oggi sono in uso diverse eID. Per annunciarsi a un dispositivo mobile atto a navigare in Internet, ad esempio, occorre di norma allestire un profilo eID (p. es. AppleID, Google ID). Con quest'ultimo ci si può registrare in maniera semplice anche ad altri servizi in rete, che fanno affidamento su tale identificazione

Servizi statali in rete nell'ambito del governo elettronico richiedono un'identificazione univoca e affidabile che mediante procedure standardizzate garantisce che l'identità del titolare di un'eID è stata verificata. Diversi Stati rilasciano proprie eID secondo soluzioni gestite completamente dallo Stato o da privati riconosciuti. Le soluzioni puramente statali non garantiscono però una buona accoglienza da parte dei cittadini e sono connesse a un elevato onere di investimento e soprattutto di esercizio per l'ente pubblico. Sono in grado di tenere il passo con gli sviluppi tecnologici solo difficilmente e con adeguamenti costosi oppure essendo oggetto di nuovi concorsi. Sovente non conseguono la diffusione auspicata e in parte vengono impiegate in modo coattivo e solo una volta all'anno per la dichiarazione delle imposte. L'evoluzione delle eID rilasciate dallo Stato è illustrata ulteriormente al numero 1.5.

La soluzione proposta sgrava lo Stato da buona parte di questa dinamica del mercato e dagli elevati costi ad essa connessi.

Nel frattempo sono disponibili sul mercato anche diverse eID affidabili offerte da IdP svizzeri la cui accettazione è in continua crescita (p.es. la Mobile ID della telefonia mobile o la SuisseID della Posta). Questi sistemi di eID saranno rafforzati mediante il riconoscimento e impiegati nell'ambito del governo elettronico. Il fatto di stabilire regole chiare motiverà inoltre altri possibili IdP a lanciarsi in questo mercato (p. es. banche o offerenti di carte di credito).

I requisiti posti ai sistemi di eID svizzeri riconosciuti 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

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. L'accreditamento è rilasciato da un servizio a tal scopo designato dal Consiglio federale.

Nell'ambito delle piattaforme per la trasmissione sicura, per contro, è un'unità amministrativa del DFGP, ossia l'Ufficio federale della 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 sul riconoscimento di piattaforme di trasmissione (RS 272.11). 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 la considerazione tempestiva degli sviluppi tecnici nel campo della trasmissione sicura.

Questa procedura è più semplice e ha dimostrato la sua efficacia. La procedura di riconoscimento per gli IdP s'ispira pertanto a quella per le piattaforme di trasmissione: secondo l'AP, il Servizio di riconoscimento è competente per il ricevimento e l'esame delle domande di riconoscimento di IdP e 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 disposizioni saranno armonizzate con le regole vigenti nel settore della firma elettronica e delle piattaforme di trasmissione, cosicché gli IdP riconosciuti potranno beneficiare di sinergie nell'ambito delle certificazioni.

1.4 Compatibilità tra i compiti e le finanze

1.4.1 Nuovi compiti

La legge sull'eID comporta nuovi compiti per l'Amministrazione federale. Da un lato, il Servizio delle identità è incaricato di allestire un'interfaccia per la trasmissione di dati d'identificazione personale, dall'altro deve essere istituito il Servizio competente per il riconoscimento degli IdP e la relativa vigilanza (cfr. n. 1.2.6). Questi due servizi non sono necessariamente attribuiti alla medesima unità amministrativa della Confederazione.

Il Servizio delle identità assume i seguenti compiti:
a) gestisce e mantiene l'infrastruttura informatica che gli è necessaria (interfaccia verso gli IdP e collegamento delle banche dati interne all'Amministrazione come ISA, Infostar, ecc.);
b) fornisce supporto tecnico alle banche dati federali interessate;
c) fornisce supporto tecnico agli IdP riconosciuti;
d) elabora e cura le prescrizioni tecniche e organizzative per il riconoscimento di IdP e sistemi di eID;
e) acquisisce i servizi degli IdP necessari alla Confederazione;
f) si tiene informato sugli sviluppi tecnologici attuali nel settore dell'eID e sulle pertinenti questioni in materia di sicurezza informatica.

Secondo l'articolo 19 AP, il Servizio delle identità è un'unità amministrativa annessa al DFGP (fedpol). Quest'ultimo è competente per l'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 tenuta presso il DFGP. Se necessaria, una domanda di rettifica dei suddetti dati potrebbe essere indirizzata all'esistente servizio di clearing dell'UCC-UPI.

Il Servizio di riconoscimento assume i seguenti compiti:
a) riconosce gli IdP;
b) sorveglia gli IdP riconosciuti e i loro sistemi di eID; e
c) gestisce e pubblica l'elenco degli IdP riconosciuti.

Oltre alle funzioni di riconoscimento e vigilanza, il Servizio di riconoscimento assume pure quelle dell'organismo di vigilanza ai sensi del regolamento eIDAS. Altre funzioni di vigilanza corrispondenti sono assunte, in seno alla Confederazione, dal DFF (Organo direzione informatica della Confederazione, ODIC). All'articolo 21 l'AP insedia perciò il Servizio di riconoscimento presso il DFF.

1.4.2 Finanziamento

Prestazioni preliminari della Confederazione
L'introduzione di eID riconosciute richiede risorse finanziarie della Confederazione per un totale di 6,5 milioni di franchi. Dato che si tratta di un progetto strategico che va parimenti a beneficio delle amministrazioni pubbliche della Confederazione, dei Cantoni e dei Comuni nonché dell'economia privata e della popolazione, si propone un cofinanziamento sostenuto dal DFGP, da E-Government Svizzera e da risorse centrali della Confederazione destinate al settore informatico.

Attualmente si prevedono costi d'esercizio informatico di circa 1,5 milioni di franchi all'anno, a cui si aggiungono costi di personale per circa 0,7 milioni. Queste uscite saranno però a medio termine compensate dalle entrate degli emolumenti per la copertura delle spese. Il piano di finanziamento per i costi d'esercizio sarà presentato dopo la consultazione insieme al messaggio.

Finanziamento mediante emolumenti
Per le prestazioni che lo Stato fornisce all'IdP sono stati esaminati diversi modelli di finanziamento. Sono stati respinti sia il modello «prepaid» - secondo cui l'IdP versa allo Stato un emolumento che copra il più possibile i costi, senza però che si possa essere sicuri che la diffusione delle eID sia tanto 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 e non sarebbe pertanto opportuno a causa delle misure di risparmio dettate dalla politica. Si propone dunque un modello «pay-per-use» finanziato mediante emolumenti.

Secondo tale modello sarà emanata un'ordinanza sugli emolumenti. Per accelerare la diffusione delle 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 moderato emolumento dell'ordine delle decine di centesimi, che sarà stabilito in base a un'ordinanza del Consiglio federale ancora da emanare. A seconda della diffusione di eID riconosciute, in particolare dei livelli *significativo* ed *elevato*, questo modello permetterà di generare entrate sufficienti per coprire i costi.

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). Essi dovranno quindi essere disposti a indennizzare l'applicazione di sistemi di eID. Spetterà al mercato stabilire le modalità di fatturazione delle prestazioni.

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 il 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 tra i singoli sistemi dei diversi Paesi. Il progetto dei sistemi di eID riconosciuti svizzeri si orienta a queste prescrizioni europee cosicché le eID svizzere potrebbero essere usate anche nel contesto internazionale.

Con la presente legge si crea tra l’altro un quadro giuridico e di standardizzazione per il riconoscimento di sistemi di eID e di IdP. Tale quadro è strutturato in modo da consentire un successivo riconoscimento reciproco dei sistemi di eID tra la Svizzera e l’UE o singoli Stati membri. A tal scopo sarebbero necessari accordi bilaterali.

1.5.2 Sviluppi degli ultimi quindici anni

Gli Stati interessati si sono in un primo tempo concentrati sulle questioni di quando il loro documento d’identità verrebbe dotato di un’eID, di quali tecnologie utilizzare e di quali funzioni integrarvi.

I punti principali erano: quale tecnologia chip e quale sistema operativo su chip verrebbero usati nonché se il chip avrebbe comunicato con il suo ambiente con contatto o via radio (NFC). Un importante problema giuridico e politico era se l’eID sarebbe stata riferita a un identificatore personale esistente e, se del caso, di quale tipo questo sarebbe stato. Dal punto di vista funzionale andava deciso se il chip avrebbe contenuto pure una chiave per la firma elettronica e, successivamente, la funzione di passaporto elettronico con tecnologia radio nel frattempo standardizzata dall’Organizzazione dell’aviazione civile internazionale (International Civil Aviation Organization, ICAO).

Con queste considerazioni, negli ultimi anni la maggior parte degli Stati europei ha via via introdotto un’eID connessa con la carta d’identità come elemento centrale di un sistema di eID nazionale. Ha aperto la pista la Finlandia, nel 1999, seguita da Estonia, Belgio, Spagna e Portogallo. La Germania ha introdotto una carta d’identità elettronica nel 2010. Negli ultimi anni sono stati in particolare Paesi del Vicino Oriente e dell’Asia a rilasciare nuove carte d’identità statali con funzione di eID. Questa gara alla digitalizzazione ha forse avuto luogo anche perché nessuno Stato voleva restare indietro. Né gli Stati Uniti né il Regno Unito hanno invece introdotto un’eID statale, conformemente al loro generale scetticismo nei confronti delle carte d’identità, mentre diversi Stati federali americani hanno rilasciato patenti di guida elettroniche.

Una prima soluzione consisteva in smartcard con chip basati sul contatto, fondate essenzialmente sulla tecnologia delle carte per la firma elettronica. Esempi di questo tipo sono l’eID finlandese, quella estone, quella belga e sostanzialmente anche quella svizzera.

Un'altra soluzione diffusa risultò dagli sforzi profusi dall'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 edizione) e i Paesi Bassi hanno queste carte d'identità contenenti la funzione ePass secondo l'ICAO nonché una funzione, che si appoggia alla precedente, per l'identificazione elettronica in rete. Lo standard ECC non ha mai potuto stabilizzarsi completamente. Un suo utilizzo si è imposto però 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.

Questa fase dell'evoluzione dell'eID ha raggiunto una sorta di culmine con il 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 farsi registrare dallo Stato per acquisire determinati attribuiti e farsi pure autenticare per utilizzare il documento.

Con una strategia globale la Germania ha provveduto affinché i titoli di soggiorno per stranieri siano dotati di «funzioni d'identificazione in rete». Negli ultimi anni l'ePA tedesco è divenuto la misura per le nuove eID statali a livello mondiale. In Germania, nel frattempo, grosso modo la metà della popolazione dispone dell'ePA e ancora non è chiaro se la funzione eID sarà effettivamente e diffusamente impiegata. Si constata 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, inoltre, devono acquistare e impiegare componenti infrastrutturali come lettori e programmi. Lo Stato, infine, deve costantemente sviluppare e distribuire modifiche e aggiornamenti di queste componenti, il che rende la gestione molto più cara.

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 veramente riuscita a imporsi in nessuno Stato, ma si è constatato che diverse soluzioni flessibili sugli smartphone sono meglio accolte. Anche in Estonia, che ha un ruolo guida in materia, attualmente l'eID è impiegata principalmente usando uno smartphone come supporto.

1.5.3 Soluzioni alternative

Negli ultimi anni, le riflessioni relative alla promozione statale dell'eID hanno preso una nuova direzione, principalmente poiché il ciclo produttivo di una carta d'identità statale è troppo lungo rispetto alla rapidità dell'evoluzione del mondo digitale.

Ispirandosi al progetto statunitense dello sviluppo comune di un ecosistema d'identità elettronica (Identity Ecosystem[9]), in numerosi Paesi si iniziò 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 è limitato a organizzare

[9] National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem. Cfr. link nella bibliografia

e promuovere, senza fornire servizi ma influendo profondamente sul mercato in quanto rilascia eID per i suoi collaboratori e gestisce servizi che utilizzano l'eID nel quadro di offerte di governo elettronico. Negli Stati Uniti sono pure state elaborate importanti basi progettuali per una gestione delle identità interoperabile e affidabile.

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. Queste eID sono accettate da enti statali e possono essere impiegate per applicazioni di governo elettronico.

Nel suddetto regolamento eIDAS, l'UE ha infine seguito questa evoluzione e accettato per il reciproco riconoscimento non solo quelle rilasciate dallo Stato ma anche 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, alla Svizzera s'impone un'altra soluzione, che sgrava lo Stato da questa dinamica tecnologica e dai costi connessi. Al contempo offre all'economia privata il margine necessario per soluzioni flessibili e adeguate alle sue esigenze. Il ruolo dello Stato si limita al minimo necessario per creare una base di fiducia.

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

- La Svizzera ha tratto gli insegnamenti dalle esperienze degli ultimi quindici anni e con il suo piano di un'eID riconosciuta ha intrapreso un percorso nuovo, considerato paradigmatico da più parti.
- Il piano svizzero è fondamentalmente conforme con l'UE e il regolamento eIDAS.
- Il piano svizzero tiene conto delle più attuali basi teoriche e tecniche 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 incisivi.

1.5.5 Regolamento eIDAS e requisiti di compatibilità

Se è già importante poter utilizzare a livello internazionale il documento d'identità classico con dati visibili come documento di viaggio e d'identificazione, lo è ancor più per l'eID. Anche se al momento non viene utilizzata come documento di viaggio, l'eID è impiegata 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 degli offerenti delle firme elettroniche e di altri servizi fiduciari, nonché la loro certificazione, comprende, quale nuovo tema, la notifica e il riconoscimento reciproco di sistemi nazionali per l'identificazione elettronica. Tutti gli Stati membri sono obbligati ad accettare sempre, laddove richiedono un'eID per l'accesso a servizi pubblici, anche un'eID straniera provenien-

te da un sistema notificato (art. 6 del regolamento eIDAS). Questo obbligo vale anche per uno Stato membro che non dispone di un sistema di eID notificato.

Quali requisiti deve soddisfare un sistema di eID svizzero per essere conforme al regolamento eIDAS se del caso 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.

Con la presente legge si 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 dei rispettivi sistemi di eID tra la Svizzera e l'UE o i suoi Stati membri.

1.6 Attuazione

L'introduzione dell'eID riconosciuta contribuisce ad attuare la strategia «Svizzera digitale» e l'obiettivo strategico numero 5 delle linee guida della Strategia di e-government Svizzera (cfr. n. 3).

Nel quadro del mandato di rinnovare il passaporto svizzero, in seno al DFGP sono stati elaborati progetti e condotti lavori preliminari che possono tornare utili anche per l'attuazione dell'eID. Una serie di ordinanze del Consiglio federale e dipartimentali nonché istruzioni disciplinerà i dettagli organizzativi e tecnici dell'attuazione. La loro elaborazione sarà avviata non appena il progetto di legge sarà stato trattato dalle Camere.

Dovranno inoltre essere designate le unità amministrative presso le quali saranno insediati il Servizio delle identità e il Servizio di riconoscimento.

1.7 Struttura

La prima sezione dell'avamprogetto contiene le disposizioni generali e le definizioni. La seconda sezione disciplina il rilascio dell'eID: i presupposti personali per i richiedenti, il riconoscimento degli IdP, i livelli di sicurezza e la procedura di rilascio. La terza sezione disciplina gli obblighi dei titolari di un'eID. Le sezioni quarta e quinta sanciscono gli obblighi dei gestori di servizi che utilizzano l'eID e dei gestori di identità elettroniche. Nelle sezioni sesta e settima sono fissati l'organizzazione e i compiti del Servizio delle identità e del Servizio di riconoscimento. L'ottava sezione regola la competenza per stabilire gli emolumenti e la nona la responsabilità civile. Come ogni atto normativo, la legge termina con le disposizioni finali alla decima sezione. Un allegato riporta le modifiche di altri atti normativi.

1.8 Commento ai singoli articoli

1.8.1 Ingresso

La competenza per disciplinare i mezzi d'identificazione elettronica riconosciuti risulta indirettamente dalla Costituzione federale del 18 aprile 1999 (Cost.; RS 100). 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 delle eID spetta a fornitori di servizi identitari che per essere riconosciuti devono soddisfare diverse condizioni, il che limita l'esercizio dell'attività economica privata.

Nella misura in cui concerne i rapporti contrattuali tra i fornitori di servizi identitari, i titolari e i gestori di servizi che utilizzano l'eID, la presente legge federale disciplina aspetti di diritto civile e si fonda pertanto sull'articolo 122 capoverso 1 Cost., che conferisce alla Confederazione la competenza per legiferare nel campo del diritto civile.

1.8.2 Sezione 1: Disposizioni generali

Articolo 1 Oggetto e scopo

Capoverso 1

Oltre al riconoscimento dei fornitori di servizi identitari, la legge disciplina anche i diritti e gli obblighi dei titolari di un'eID e dei gestori di servizi che utilizzano l'eID, nonché il contenuto, il rilascio, la revoca e l'utilizzo di mezzi d'identificazione elettronica riconosciuti.

Capoverso 2 lettere a e b

L'eID contribuisce a creare sicurezza e fiducia nell'ambito delle comunicazioni elettroniche (e-business ed e-government). In futuro, i cittadini svizzeri e stranieri con corrispondenti documenti d'identità potranno dimostrare la loro 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 nel permettere di comunicare in rete in modo affidabile, ad esempio nel contesto del governo elettronico o del business elettronico, senza che le parti si debbano incontrare fisicamente. L'eID contribuisce al passaggio tempestivo e senza problemi della Svizzera a una sviluppata società dell'informazione.

Articolo 2 Definizioni

Per la scelta delle definizioni è stata per quanto possibile considerata la terminologia della FiEle da un lato e quella del regolamento eIDAS dall'altro. Sono state in particolare introdotte e usate nella legge le abbreviazioni internazionalmente usuali dei termini inglesi.

Lettere a e b

Nel contesto della presente legge, per eID s'intende sempre il mezzo d'identificazione elettronica riconosciuto. L'eID riconosciuta non costituisce però l'unico mezzo d'identificazione elettronica dato che, come menzionato nella prima parte del rapporto, già oggi esistono diverse offerte per l'identificazione elettronica a differenti livelli di sicurezza.

L'espressione «eID» è risultata dalla concezione originaria del mezzo d'identificazione elettronico (rilascio con la carta d'identità statale, cfr. n. 1.1). Malgrado la rinuncia ad apporre il mezzo d'identificazione elettronico sul documento d'identità o sulla carta di soggiorno, l'espressione «eID» è ampiamente diffusa. Essa segue inoltre una logica semplice: nell'ambito della comunicazione elettronica l'eID assume la medesima funzione di un docu-

mento d'identità convenzionale con l'immagine del volto combinata con un incontro personale, per dimostrare l'identità del titolare.

Per eID s'intende qui di seguito esclusivamente il mezzo d'identificazione elettronica rilasciato da un IdP secondo le prescrizioni della presente legge.

Lettera c
Il termine «Identity Provider – IdP» è usuale a livello sia nazionale che internazionale. Nella presente legge si utilizza pertanto l'abbreviazione IdP per designare i fornitori di servizi identitari.

Lettere d ed e
L'identificazione ha luogo al momento della registrazione presso un'IdP (acquisizione di un'eID) o un servizio che utilizza l'eID (applicazione informatica) e significa la registrazione dell'identità di una persona sotto forma di dati d'identificazione personale e di fattori di autenticazione nel quadro di una procedura controllata.

L'autenticazione ha luogo ogni volta che il titolare accede a un servizio che utilizza l'eID e significa che l'identità registrata e dichiarata dalla persona viene verificata sulla base dei fattori di autenticazione dell'eID nel quadro di una procedura controllata.

Lettera f
I dati d'identificazione personale sono gli attributi identitari di una persona rilevati dallo Stato quali il cognome o la data di nascita. Questa banca dati gestita dallo Stato comprende anche un numero di registrazione eID che funge da ancora per i dati d'identificazione personale.

Lettera g
La legge sull'eID introduce un numero d'identificazione per persone fisiche attribuito univocamente dallo Stato (numero di registrazione eID). Come accade con il numero d'identificazione delle imprese[10], un numero di registrazione eID va attribuito a ogni persona che acquisisce un'eID. Dato che in linea di massima è possibile, e in ogni caso non vietato, essere titolare di numerose eID (p. es. su diversi supporti), il numero di registrazione eID consente di attribuire i dati d'identificazione personale raccolti dai diversi registri delle persone alla medesima persona senza che insorgano contraddizioni e in maniera duratura. Ciò garantisce l'integrità dei dati d'identificazione personale utilizzati.

Lettera h
L'IdP gestisce almeno un sistema di eID. La distinzione tra IdP e sistema di eID è importante per il riconoscimento dell'IdP, nel cui ambito sono verificati soprattutto l'adempimento dei presupposti di cui all'articolo 4 AP nonché le procedure di rilascio e di gestione. Per il riconoscimento di un sistema di eID è invece prioritario il rispetto delle prescrizioni tecniche in materia di sicurezza. È d'altronde possibile che un IdP riconosciuto gestisca numerosi sistemi di eID a differenti livelli di sicurezza e magari non tutti riconosciuti. Il riconoscimento è disciplinato negli articoli 4 e seguenti AP.

[10] Cfr. art. 3 cpv. 1 lett. c della legge federale del 18 giu. 2010 sul numero d'identificazione delle imprese (LIDI; RS 431.03)

Lettere i e j
Si distingue tra la persona fisica o giuridica che gestisce l'applicazione tecnica e l'applicazione tecnica stessa anche nel caso dei gestori di servizi che utilizzano l'eID. La comunicazione ha luogo tra persone, ossia l'IdP e il gestore del servizio che utilizza l'eID (relying party), oppure tra applicazioni informatiche, ossia il sistema di eID e il servizio che utilizza l'eID (relying party application).

Le persone giuridiche che possono gestire un servizio che utilizza l'eID comprendono anche la Confederazione, i Cantoni e i Comuni, nonché le unità amministrative o le autorità che vi fanno capo e per i quali operano.

1.8.3 Sezione 2: Rilascio di un'eID

Articolo 3 Presupposti personali
Osservazione preliminare
Nessun IdP può essere obbligato ad avviare un rapporto contrattuale e a rilasciare un'eID soltanto perché qualcuno adempie i presupposti. La formulazione potestativa al capoverso 1 lo garantisce.

Acquisendo un'eID, il richiedente ne diventa il titolare.

Capoverso 1
Il documento d'identità come prova dell'identità
Per ottenere un'eID riconosciuta dallo Stato, l'identità del richiedente deve essere accertata. A tal scopo è sufficiente un documento d'identità valido (lett. a) o una carta di soggiorno per stranieri valida (lett. b).

Minorenni
L'eID può essere rilasciata anche a minorenni e a persone a cui è stato parzialmente o completamente revocato l'esercizio dei diritti civili. La persona in questione deve disporre di un corrispondente documento d'identità. La persona abilitata a rappresentarlo richiede l'eID in nome della persona rappresentata, che così diventa titolare dell'eID ma può utilizzarla solo sotto la sorveglianza del suo rappresentante.

Stranieri
Anche gli stranieri titolari di una carta di soggiorno valida secondo l'articolo 41 della legge federale del 16 dicembre 2005 sugli stranieri (LStr; RS 142.20) devono poter acquisire eID e utilizzare le applicazioni del governo elettronico.

Capoverso 2
La carta di soggiorno per stranieri indica il tipo di autorizzazione rilasciata (p. es. relativa al domicilio, al soggiorno o all'esercizio di un'attività lucrativa). Su di essa deve figurare l'immagine del volto e la firma della persona e contenere tutte le indicazioni relative al suo statuto secondo il diritto degli stranieri. Il DFGP (SEM) stabilisce la forma (biometrica o no) e il contenuto del documento.

In virtù dell'articolo 71 capoverso 1 dell'ordinanza del 24 ottobre 2007 sull'ammissione, il soggiorno e l'attività lucrativa (OASA; RS 142.201**)**, i seguenti permessi sono rilasciati a stranieri in Svizzera e consentono di acquisire senza problemi un'eID:

1. permesso di domicilio (permesso C);

2. permesso di dimora (permesso B);
3. permesso di soggiorno di breve durata e per l'esercizio a breve termine di un'attività lucrativa (permesso L).

A dipendenza del Paese di provenienza, questi permessi possono essere rilasciati come documenti biometrici o non biometrici (attualmente di carta, dal 2019 di policarbonato). Nel caso di cittadini di Stati terzi si tiene conto dei requisiti secondo l'accordo di associazione a Schengen. I titolari di questi documenti ottengono una carta di soggiorno ai sensi dell'articolo 41 capoverso 1 LStr.

In virtù dell'articolo 71*a* capoverso 1 OASA sono inoltre rilasciati i seguenti permessi per stranieri, con o senza limitazioni del soggiorno:

1. permesso per frontalieri (permesso G);
2. permesso per richiedenti l'asilo (permesso N);
3. permesso per persone ammesse provvisoriamente (art. 83 e 85 LStr) e rifugiati ammessi provvisoriamente (art. 59 LStr) (permesso F);
4. permesso per persone bisognose di protezione (permesso S);
5. permesso per coniugi professionalmente attivi e bambini di membri di rappresentanze straniere od organizzazioni intergovernative (permesso Ci);
6. carta di legittimazione non biometrica rilasciata dal DFAE in virtù dell'articolo 71° capoverso 2 alle persone beneficiarie di privilegi, immunità e facilitazioni.

Queste categorie di permessi per stranieri non autorizzano sistematicamente ad acquisire un'eID. Il Consiglio federale determina le categorie di carte di soggiorno che consentono di ottenere un'eID (cpv. 2).

Affinché il numero maggiore possibile di stranieri possa accedere alle applicazioni di governo elettronico con un'eID, al momento è previsto che tutti gli stranieri che dispongono di un permesso di soggiorno (art. 41 cpv. 1 LStr in combinato disposto con art. 71 cpv. 1 OASA; permessi L, B e C) e i frontalieri (art. 71*a* OASA; permesso G) possano richiedere un'eID. Nel settore del diritto in materia di stranieri è ipotizzabile l'utilizzo di applicazioni di governo elettronico, malgrado nella maggior parte dei casi siano i Cantoni a essere competenti per i contatti. Il Consiglio federale può prevedere procedure alternative per l'identificazione elettronica.

Per quanto riguarda i restanti stranieri, in particolare i titolari di permessi N, F ed S, si rinuncia per il momento a concedere loro l'accesso a funzioni eID. Molti richiedenti l'asilo non possono presentare documenti d'identità nell'ambito della procedura d'asilo, il che rende impossibile un'identificazione sicura. Pure nel caso delle persone ammesse provvisoriamente sono presentate al DFGP (SEM) numerose domande di modifica o rettifica di dati personali che non di rado si basano su documenti non validi. Attualmente, nel settore dell'asilo non sono previsti servizi elettronici a cui titolari di permessi N, F o S debbano accedere direttamente. Il rilascio di un'eID per queste categorie di persone non è pertanto prioritario.

Capoverso 3

L'evoluzione tecnica nel settore dell'eID è rapida. I processi d'identificazione possono eventualmente essere strutturati ispirandosi ai metodi d'identificazione ammessi nel settore bancario, in cui l'Autorità federale di vigilanza sui mercati finanziari (FINMA) definisce esattamente i metodi ammessi per l'identificazione dei nuovi clienti. Per poter reagire in modo

flessibile ai più recenti sviluppi tecnologici, i dettagli relativi ai presupposti per il rilascio, alla procedura e al blocco o alla revoca sono disciplinati a livello di ordinanza.

Il numero 4.4 fornisce una panoramica sulla delega di competenze legislative.

Articolo 4 Riconoscimento degli IdP

Osservazione preliminare

Nell'ambito del riconoscimento dei fornitori di servizi identitari vengono verificati e riconosciuti anche i loro sistemi di eID. I requisiti tecnici posti ai servizi che utilizzano l'eID (relying party application) sono invece disciplinati soltanto indirettamente tramite i requisiti 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[11].

Capoversi 1 e 2

L'IdP che intende rilasciare eID riconosciute deve soddisfare diversi presupposti organizzativi e tecnici. Il rispetto dei presupposti, regolarmente verificato dal Servizio di riconoscimento, garantisce un controllo sufficiente sugli IdP e sui dati da questi eventualmente registrati.

Lettere a e b

Gli IdP devono avere la loro sede in Svizzera e disporre di un numero d'identificazione delle imprese. Possono gestire sistemi di eID servizi sia privati che pubblici. L'articolo stabilisce indirettamente che persone fisiche o giuridiche non iscritte nel registro di commercio non possono essere riconosciute e quindi non possono gestire sistemi di eID riconosciuti.

Lettere c e d

Un presupposto organizzativo concerne le persone che eseguono la verifica dei documenti d'identità presentati nell'ambito della procedura di rilascio e che possono influire sulla trasmissione dei dati: 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.

Per rischio per la sicurezza s'intende ad esempio l'assunzione di una persona oggetto di una condanna passata in giudicato per determinati reati (cfr. i commenti all'art. 12 cpv. 2 lett. d) 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 i registri delle esecuzioni.

Lettera e

L'affidabilità è comprovata dal rispetto degli standard di sicurezza validi al momento e dalla certificazione delle procedure.

Lettera f

L'IdP deve garantire che il trattamento e la gestione dei dati hanno luogo esclusivamente in Svizzera. Qualsiasi accesso non autorizzato ai dati da parte di terzi all'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 presente legge, in particolare anche dati provvisori, dati provenienti da memorizzazioni temporanee e dati marginali.

[11] Cfr. link nella bibliografia

Lettera g
L'IdP deve stipulare un'assicurazione di responsabilità civile retta dal codice delle obbligazioni (cfr. sez. 9 art. 24).

Capoverso 3
Poiché l'evoluzione tecnica nel settore dell'identificazione e dell'autenticazione elettroniche è difficilmente prevedibile, il riconoscimento va rinnovato a intervalli regolari. L'IdP allestisce annualmente un rapporto sulla sicurezza relativo a tutti i sistemi di eID riconosciuti da esso gestiti e lo trasmette al Servizio di riconoscimento. Il Consiglio federale stabilisce la forma e il contenuto di tale rapporto.

Capoverso 4
Come in altri punti, anche qui il disciplinamento della procedura e dei dettagli tecnici è delegato al Consiglio federale, competente per legiferare a livello di ordinanza.

Vengono disciplinati a livello di ordinanza e di istruzione soprattutto gli standard applicabili e i protocolli tecnici per i sistemi di eID. L'applicazione degli standard e dei protocolli è regolarmente verificata dal Servizio di riconoscimento. In tal modo vengono riconosciuti anche i sistemi di eID.

Articolo 5 Livelli di sicurezza
Capoverso 1
Non tutte le transazioni richiedono il medesimo livello di sicurezza. Sovente, un livello di sicurezza superiore comporta un onere maggiore per l'acquisizione nonché maggiori difficoltà d'utilizzo e maggiori costi. Al fine di andare incontro alle esigenze del mercato, gli IdP devono dunque poter offrire tre diversi livelli di sicurezza, come prescritto anche dall'UE e dalla NIST. I gestori di servizi che utilizzano l'eID possono decidere autonomamente quale livello di sicurezza intendono applicare (cfr. art. 15 AP).

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.

A dipendenza del livello di sicurezza del sistema, l'eID offre un differente grado di affidabilità. I livelli *basso* e *significativo* mirano a ridurre il rischio di un uso abusivo dell'identità, mentre il livello *elevato* mira a prevenire tale rischio.

Capoverso 2
I dettagli relativi ai diversi livelli di sicurezza saranno fissati a livello di ordinanza. I livelli si distinguono per la procedura di rilascio, la gestione e l'applicazione nonché eventualmente per altre misure di sicurezza tecniche od organizzative. I requisiti sono descritti nella legge nel modo più approfondito possibile per non dipendere dallo stato della tecnologia e saranno determinati in dettaglio e per i diversi supporti eID a livello di ordinanza o di istruzione.

Capoverso 3
Un'eID di un livello di sicurezza superiore deve poter essere impiegato anche presso un servizio che utilizza l'eID e richiede un livello inferiore. I titolari possono dunque utilizzare la 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.

Articolo 6 Procedura di rilascio

Osservazione preliminare

La procedura di rilascio ha luogo tra il richiedente, l'IdP e il Servizio delle identità. A dipendenza del livello di sicurezza, il rilascio presuppone che il richiedente si presenti personalmente o si identifichi in modo equivalente. Il Consiglio federale disciplina la procedura di rilascio a seconda del livello di sicurezza; le pertinenti deleghe figurano in diverse disposizioni dell'AP (in particolare art. 3 cpv. 3 e art. 5 cpv. 4).

Capoverso 1

L'IdP non può rilasciare un'eID di sua spontanea volontà anche se conosce la persona in questione poiché è già sua cliente. La richiesta deve provenire dal futuro titolare dell'eID (richiedente), che a sua volta non è obbligato ad acquisire un'eID.

Capoversi 2 e 3

L'IdP verifica se il richiedente soddisfa i presupposti personali di cui all'articolo 3 e successivamente chiede al Servizio delle identità di trasmettergli i dati d'identificazione personale in forma elettronica. Se l'IdP intende rilasciare l'eID soltanto a una cerchia limitata di persone (clienti), i presupposti personali comprendono anche la relazione clientelare. Il richiedente deve dare il suo consenso esplicito alla trasmissione dei dati d'identificazione personale. Mediante misure tecniche e organizzative il Servizio delle identità garantisce che i dati d'identificazione personale non possano essere consultati in modo abusivo. L'IdP non deve ad esempio poter consultare dati d'identificazione personale unicamente indicando il numero del documento d'identità e senza il consenso esplicito del titolare. Per questa dichiarazione di consenso deve eventualmente avere luogo un contatto diretto tra il Servizio delle identità e il richiedente.

Capoverso 4

L'IdP attribuisce i dati d'identificazione personale all'eID e si assicura che l'eID sia attribuita 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 utilizzata 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.

Capoverso 5

La trasmissione dei dati d'identificazione personale è richiesta elettronicamente presso il sistema d'informazione del Servizio delle identità, che mette a verbale la richiesta.

Articolo 7 Dati d'identificazione personale

Capoversi 1 e 2

La trasmissione di dati d'identificazione personale ai sensi del capoverso 2 presuppone che la procedura di registrazione, il sistema di eID e l'autenticazione soddisfino requisiti tecnici e organizzativi elevati.

Alcuni dei dati d'identificazione personale menzionati sono dati biometrici (immagine del volto, immagine della firma). Dato che possono essere confermati unicamente dati tenuti nei sistemi d'informazione della Confederazione (cfr. art. 20 AP), l'elenco è esaustivo. Il titolare può limitare i dati d'identificazione personale che nel caso concreto sono trasmessi dall'IdP a un gestore di servizi che utilizzano l'eID (cfr. art. 17 cpv. 1 lett. f AP). La denominazione dei

dati d'identificazione personale si fonda nella misura del possibile sulla terminologia della LArRa.

Capoverso 3
Il Servizio delle identità può integrare i dati d'identificazione personale con informazioni supplementari che possono aiutare l'IdP nella gestione dell'eID, ad esempio relative al sistema d'informazione da cui provengono e al loro più recente aggiornamento in tale sistema.

Capoverso 4
Oltre ai dati d'identificazione personale, l'IdP può attribuire a un'eID (o al numero di registrazione eID) dati supplementari quali un indirizzo, un numero di telefono o di cliente. Sarebbe pure ipotizzabile che una banca funga da IdP e aggiunga un'eID riconosciuta a una carta di credito o a una carta di conto.

Articolo 8 Aggiornamento dei dati d'identificazione personale
Capoverso 1
Alcuni degli attributi dell'identità sono modificabili. Dall'esecuzione del riveduto diritto in materia di nomi del Codice civile (CC, RS 210, in part. art. 29 segg. e art. 160) è emerso che sempre più sovente viene modificato il cognome ufficiale, che non rimane dunque più lo stesso dalla nascita al decesso. Anche gli adeguamenti dello stato civile e del sesso sono più frequenti rispetto al secolo precedente. L'obbligo di aggiornamento regolare si fonda su questa constatazione.

L'affidabilità dell'eID è incrementata mediante regolari aggiornamenti dei dati d'identificazione personale sulla base dei sistemi d'informazione statali. Gli intervalli massimi di questi adeguamenti sono prescritti per ogni livello di sicurezza. La relativa competenza spetta all'IdP. Per gli aggiornamenti regolari sono riscossi emolumenti.

Capoverso 2
Il Servizio delle identità garantisce che l'IdP possa sistematicamente verificare la validità del numero di registrazione eID mediante una procedura usuale (cfr. art. 20 cpv. 4 AP), attualmente la tenuta di un elenco elettronico. Gli IdP devono consultare periodicamente questi elenchi e bloccare o revocare immediatamente le eID attribuite a un numero di registrazione eID indicatovi come non valido. Questo obbligo aumenta l'affidabilità delle eID riconosciute e la consultazione è pertanto gratuita. Gli IdP sono pure tenuti ad allestire un sistema gratuito che consenta tale consultazione per le sole eID da essi rilasciate (art. 17 cpv. 1 lett. c AP).

A seconda dell'esito della consultazione, l'eID va bloccata o revocata. È necessario distinguere tra blocco o revoca di un'eID e blocco o revoca di un numero di registrazione eID. Se ad esempio viene notificata la perdita del supporto e quindi dell'eID, che potrebbe pertanto essere accessibile a terzi, l'eID in questione è temporaneamente non valida, ma lo stato del numero di registrazione eID non è interessato dato che questo è collegato all'identità della persona a livello statale, indipendente dall'eID. Quest'ultima può poi essere riattivata e nuovamente utilizzata non appena il motivo del blocco viene a cadere. La revoca di tutte le eID attribuite a un numero di registrazione eID ha tuttavia luogo quando quest'ultimo numero non può più essere utilizzato, ad esempio in caso di decesso del titolare. Un numero di registrazione eID revocato non può più essere riattivato, mentre uno temporaneamente bloccato sì.

L'aggiornamento dei dati d'identificazione personale richiede il versamento di un emolumento. Il Consiglio federale emanerà una pertinente ordinanza. L'emolumento deve coprire i costi e ammonterà presumibilmente a qualche decina di centesimi per aggiornamento.

Articolo 9 Utilizzo sistematico del numero di assicurato per lo scambio di dati

Osservazione preliminare

Il numero di assicurato (NAVS13) ai sensi della 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 9 AP contiene la base legale e i principi di trattamento relativi all'utilizzo sistematico del NAVS13 per l'eID. Qui di seguito i dettagli del disciplinamento.

Capoverso 1

Il NAVS13 è utilizzato dal Servizio delle identità durante la procedura di rilascio e l'aggiornamento dei dati (art. 8 AP) per identificare le persone e funge da identificatore univoco nel quadro della consultazione di altre banche dati che pure lo utilizzano sistematicamente. Il NAVS13 è imprescindibile per confrontare automaticamente o inoltrare i dati tra diverse banche dati. Solo esso può garantire che una persona sia identificabile in modo univoco nei diversi registri anche dopo che ha modificato il cognome. Le modifiche del diritto in materia di nomi introdotte negli ultimi anni rendono alle persone più facile oscurare la loro precedente identità e costruirsene legalmente una nuova. Con la modifica del nome, infatti, vengono rilasciati nuovi documenti d'identità, che non consentono di risalire alla precedente identità. Il NAVS13 permette per contro un'attribuzione univoca.

Capoverso 2

Gli IdP sono autorizzati a registrare il NAVS13 nei loro sistemi. Il NAVS13 è comunicato ai servizi che utilizzano l'eID soltanto se questi sono a loro volta autorizzati a farne uso sistematicamente secondo le menzionate disposizioni della LAVS. La trasmissione di questo attributo a terzi non autorizzati a utilizzarlo sistematicamente deve pertanto essere impedita mediante misure tecniche. Sul rapporto relativo alla trasmissione dei dati il NAVS13 è reso invisibile. Il numero di registrazione eID è il numero d'identificazione univoco per l'IdP.

Articolo 10 Trattamento e trasmissione di dati

Osservazione preliminare

Il trattamento e la trasmissione di dati è l'effettiva attività degli IdP. L'identificazione e l'autenticazione sono prestazioni fornite sia ai gestori di servizi che utilizzano l'eID che ai titolari di eID. Gli IdP fungono da intermediari tra di loro. Il disciplinamento della protezione dei dati ne risulta pertanto particolarmente importante.

Capoversi 1 e 2

Le disposizioni di protezione dei dati formulate ai capoversi 1 e 2 non sono più restrittive di quelle della pertinente legislazione. Nell'ambito dell'utilizzo dell'eID il titolare può scegliere i dati d'identificazione personale che vanno trasmessi al servizio che utilizza l'eID. Possono tuttavia essere trasmessi unicamente quelli corrispondenti al livello di sicurezza richiesto dal servizio in questione.

Capoverso 3

La trasmissione di dati d'identificazione personali confermati a livello statale dei livelli di sicurezza *significativo* ed *elevato* e in particolare la loro commercializzazione sono vietate sia all'IdP che al gestore di servizi che utilizzano l'eID. Il modello aziendale degli IdP e dei gestori di servizi che utilizzano l'eID non può fondarsi sulla vendita di dati o profili d'utilizzo confermati dallo Stato e dunque particolarmente informativi. Questi dati non devono però poter essere comunicati neppure gratuitamente, ad esempio ai fini dell'utilizzo commerciale da parte di un'altra impresa del medesimo gruppo. Il divieto di commercializzazione non è riferi-

to esplicitamente ai dati supplementari attribuiti all'eID conformemente all'articolo 7 capoverso 4 AP.

Capoverso 4
Il riferimento alla legislazione sulla protezione dei dati comprende sia la legge del 19 giugno 1992 sulla protezione dei dati (LPD; RS 235.1) che gli atti normativi subordinati. Gli IdP e i gestori di servizi che utilizzano l'eID sottostanno in particolare agli articoli 16-25bis LPD e alla sorveglianza di cui all'articolo 27 LPD.

Articolo 11 Estinzione del riconoscimento
Capoverso 1
Per poter gestire un sistema di eID, l'IdP deve essere in grado di esercitare la sua attività. In caso di avvio di una procedura di fallimento, questa capacità viene a mancare e il riconoscimento si estingue per legge. I sistemi di eID non sono pignorabili e non rientrano nella massa fallimentare. I dati confermati tramite i sistemi di eID non sono commerciabili e sono dunque privi di valore economico.

Capoversi 2 e 3
I sistemi di eID sono interconnessi tramite l'interoperabilità (art. 18 AP) e costituiscono i nodi delle reti che collegano tra loro i servizi che utilizzano l'eID. Il capoverso 3 è inteso garantire la preservazione delle reti eID costituite. Dato che il ricavo della ripresa può rientrare nella massa fallimentare, i sistemi di eID nel complesso hanno un valore economico, anche se i singoli dati non sono commerciabili.

Articolo 12 Misure di vigilanza e revoca del riconoscimento
Capoversi 1 e 2
Il Servizio di riconoscimento 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. 4 AP). Le misure necessarie possono consistere in particolare in prescrizioni tecniche, ad esempio relative al rispetto dei più recenti standard, o misure organizzative come oneri per la formazione dei collaboratori. Il Servizio di riconoscimento stabilisce un termine affinché l'IdP colmi le lacune constatate. Se le lacune non vengono colmate può revocare il riconoscimento.

Capoverso 4
Lettere a - c
La revoca del riconoscimento costituisce una sanzione amministrativa. Il riconoscimento può essere revocato se l'IdP viola le disposizioni della presente legge, non adempie più i pertinenti presupposti o non attua entro i termini gli oneri imposti nell'ambito della procedura di riconoscimento. La formulazione potestativa garantisce che questa sanzione, dalle ripercussioni pesanti, sia pronunciata soltanto nel rispetto del principio della proporzionalità.
Lettera d
Entrano in considerazione reati connessi alla criminalità su Internet, in particolare quelli che possono comportare un abuso dell'identità, ossia un utilizzo abusivo dei dati personali (dell'identità) di un'altra persona. L'abuso d'identità è sovente commesso con lo scopo di danneggiare la reputazione di qualcuno o di procacciarsi un indebito profitto. Se l'autore mira a procacciare a sé stesso o a un terzo un indebito profitto si rende colpevole di truffa (art. 146 Codice penale, CP; RS 311.0) o tentata truffa e può essere condannato a una pena detentiva di fino a cinque anni. Si ricorre in parte a un'altra identità al fine di procacciarsi un profitto anche nel quadro del phishing perseguibile. Se l'autore penetra in un sistema informatico con dati personali si rende colpevole di accesso indebito a un sistema per

l'elaborazione di dati (hacking, art. 143bis CP), se invece ottiene indebitamente dati altrui non a lui destinati si macchia di acquisizione illecita di dati (art. 143 CP). A dipendenza dell'intenzione dell'autore e del caso concreto possono essere applicate pure fattispecie quali il danneggiamento di dati, il danno patrimoniale procurato con astuzia, la minaccia o la coazione (art. 144bis, 151, 180 o 181 CP). Se, infine, mediante l'abuso di un'identità altrui l'autore compie un delitto contro l'onore o la sfera personale privata sono applicate le disposizioni penali degli articoli 173 e seguenti. Per il raro caso dell'abuso d'identità senza uno degli scopi descritti, diversi Cantoni prevedono disposizioni del diritto sulle contravvenzioni che sanzionano con la multa i comportamenti gravemente sconvenienti o le molestie.

Articolo 13 Sistema di eID sussidiario della Confederazione
Come già menzionato in precedenza, la presente legge presuppone un mercato funzionante. Se per contro nessun IdP privato ha interesse a far riconoscere sistemi di eID dei livelli di sicurezza *significativo* o *elevato*, la Confederazione si riserva il diritto di gestire un proprio sistema di eID, in particolare per l'identificazione e l'autenticazione nel quadro di prestazioni e contatti elettronici nel settore amministrativo (applicazioni del governo elettronico). Al capoverso 2 vengono al contempo create le basi legali per allestire e gestire un sistema di eID statale, eventualmente in collaborazione con privati.

1.8.4 Sezione 3: Titolari di un'eID

Articolo 14 Obblighi
Capoversi 1 e 2
Oggigiorno quasi tutti sono abituati a utilizzare i mezzi digitali. Gli obblighi che la presente legge impone ai titolari di un'eID non superano gli usuali obblighi di diligenza che devono essere osservati utilizzando una carta di credito o di conto bancario. È per esempio imprescindibile (e ragionevolmente esigibile) non rendere pubblico e non conservare insieme al supporto eID l'eventualmente necessario PIN, 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 eID.

Capoverso 3
Nel quadro della responsabilità delittuale, l'articolo 14 AP costituisce una norma di protezione nel senso del diritto in materia di responsabilità civile. Il Consiglio federale può in particolare disciplinare in un'ordinanza gli obblighi di diligenza supplementari da rispettare, la cui chiara definizione consente lo sgravio in caso di responsabilità extracontrattuale (delittuale). A livello di ordinanza è per esempio prescritto 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.

1.8.5 Sezione 4: Gestori di servizi che utilizzano l'eID

Articolo 15 Accordo con un IdP
Ogni gestore di un servizio che utilizza l'eID ha stipulato un accordo con almeno un IdP. Tale accordo disciplina perlomeno il livello di sicurezza e le procedure tecniche e organizzative applicabili.

Articolo 16 Autorità in veste di gestori di servizi che utilizzano l'eID
Per l'utilizzo delle loro prestazioni, le autorità in veste di gestori di servizi che utilizzano l'eID possono richiedere un'identificazione elettronica soltanto se ciò è necessario nel caso con-

creto. Se però l'identificazione elettronica è prescritta, anche le autorità cantonali e comunali che eseguono il diritto federale devono accettare tutte le eID riconosciute del livello di sicurezza richiesto. Ciò non esclude che possano continuare a essere utilizzati i mezzi d'identificazione elettronici attualmente in uso.

Questa disposizione sottolinea l'importanza e il grado di accettazione interno alla Confederazione di un'eID riconosciuta a livello statale come definita nella strategia «Svizzera digitale» e nella Strategia di e-government del Consiglio federale (cfr. n. 3). Non per ultimo si intende in tal modo proteggere gli investimenti effettuati dalla Confederazione nell'ambito dell'eID e creare un'ampia base di consenso per l'utilizzo della stessa nelle procedure di governo elettronico. Ciò va a beneficio non soltanto della Confederazione, dei Cantoni e dei Comuni, che grazie all'eID riconosciuta a livello statale possono risparmiare i costi, ma anche di tutti gli abitanti della Svizzera.

1.8.6 Sezione 5: Fornitori di servizi identitari (IdP)

Articolo 17 Obblighi

Capoverso 1

Lettera a

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

Lettera 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 procedura è suddivisa nelle tre fasi seguenti e può essere strutturata diversamente a seconda del livello di sicurezza.

1. L'IdP attribuisce in modo univoco all'eID i dati d'identificazione personale trasmessi dal Servizio delle identità (art. 7 AP) con il numero di registrazione eID e il pertinente mezzo di autenticazione che autentifica il titolare. Perlomeno 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. Garantisce che l'eID sia attribuita 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 consegnata 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).

Lettera c

Dato che l'evoluzione tecnica nel settore della trasmissione sicura di dati è rapida, la verifica della validità di tutte le eID mediante una procedura usuale è prescritta nelle legge con una formulazione che corrisponde a quella della FiEle riveduta. Attualmente sono considerati procedure usuali gli elenchi elettronici: il Servizio delle identità può ad esempio tenere e pubblicare un elenco dei numero 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 e ad aggiornarlo con la sua procedura usuale.

Lettera d
L‘IdP è obbligato a consultare i più recenti requisiti di sicurezza e a verificare che i sistemi da esso gestiti li rispettano.

Lettera e
L’aggiornamento dei dati d’identificazione personale genera maggiore sicurezza. Gli intervalli tra un aggiornamento e l’altro si differenziano a seconda dei livelli di sicurezza e sono stabiliti all’articolo 8 capoverso 1.

Lettera f
Se nell’ambito dell’utilizzo di un’eID devono essere trasmessi dati d’identificazione personale (tipicamente durante la registrazione presso un servizio che utilizza l’eID), l’IdP deve ottenere il consenso del titolare.

Se ad esempio un titolare desidera giocare in un casinò in rete deve dimostrare di aver compiuto diciotto anni. Il casinò ha stipulato un accordo con un IdP. Il titolare dispone di un’eID implementata sullo smartphone e lo comunica al casinò. Quest’ultimo contatta in rete l’IdP, che chiede al titolare se desidera trasmettere il cognome, il nome e la data di nascita al casinò. Il titolare conferma il suo consenso e i dati liberati vengono trasmessi al casinò, che in tal modo dispone di una prova dell’età confermata a livello statale e può ammettere il titolare al gioco in rete, a condizione che non vi siano altri motivi di esclusione. Per ogni ulteriore visita è sufficiente accedere con l’eID.

Lettera g
I dati del protocollo dell’IdP sull’utilizzo dell’eID vanno cancellati dopo sei mesi. Questa disposizione non concerne i dati di protocollo, registrazione e transazione del servizio che utilizza l’eID.

Capoversi 2, 3 e 4
L’IdP garantisce che i problemi di utilizzo dell’eID 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 o altri canali.

È possibile che i gestori di servizi che utilizzano l’eID o gli IdP si accorgano del rischio d’abuso dell’eID prima del titolare (p. es. perché l’eID è utilizzata in un luogo inusuale) come pure che un terzo cerchi abusivamente di bloccare l’eID. Prima di bloccarla l’IdP deve dunque assicurarsi che la persona che richiede il blocco dell’eID vi sia autorizzata.

Articolo 18 Interoperabilità
L’interoperabilità tra i sistemi di eID costituisce un presupposto importante per la diffusione delle eID. L’articolo 18 dispone pertanto che gli IdP debbano riconoscere reciprocamente i loro sistemi di eID mediante standard tecnici e interfacce definite stabiliti a livello di ordinanza o istruzione.

I titolari dovrebbero poter utilizzare le loro eID presso tutti i servizi che utilizzano l’eID, a condizione che l’eID offra perlomeno il livello di sicurezza richiesto. Ciò deve essere possibile indipendentemente dall’esistenza di un accordo tra il gestore del servizio che utilizza l’eID e l’IdP che ha rilasciato l’eID. A tal fine gli IdP devono federare reciprocamente i loro servizi d’identificazione, analogamente a una rete di carte di credito o al roaming nel settore della telefonia mobile, mediante standard e regole d’interoperabilità che devono essere rispettate

da tutti gli IdP oppure mediante una piattaforma a cui devono aderire tutti gli IdP. In questo secondo caso occorre un'organizzazione che potrebbe essere istituita da Confederazione e Cantoni nel quadro della Federazione svizzera d'identità. A tempo debito verrà trovata la soluzione più adeguata ed economica, considerando che deve essere accordato un diritto di consultazione agli attori interessati dell'economia e dell'amministrazione.

1.8.7 Sezione 6: Servizio svizzero delle identità elettroniche

Articolo 19 Organizzazione

Il Servizio svizzero delle identità elettroniche (Servizio delle identità) è insediato presso il DFGP. Il Consiglio federale ne disciplina l'organizzazione. Si confrontino in merito i commenti al numero 1.4.1.

Articolo 20 Compiti e obblighi

Capoverso 1

Il Servizio delle identità attribuisce i dati d'identificazione personale a un numero di registrazione eID e li trasmette all'IdP. La quantità di dati d'identificazione personale trasmessi varia a seconda del livello di sicurezza (cfr. art. 7 AP).

Capoversi 2 e 3

Il Servizio delle identità gestisce un sistema d'informazione che ha accesso ai registri di persone tenuti a livello di Confederazione ed effettua un confronto con tali registri. Al momento dell'elaborazione della presente legge questi registri sono i seguenti:

a. il sistema d'informazione sui documenti d'identità (ISA) di cui all'articolo 11 della legge federale del 22 giugno 2001 sui documenti d'identità (LDI; RS 143.1) e all'articolo 10 dell'ordinanza del 20 settembre 2002 sui documenti d'identità (ODI; RS 143.11);
b. il sistema d'informazione centrale sulla migrazione (SIMIC) di cui all'articolo 101 e seguenti LStr (RS 142.20) e all'ordinanza SIMIC del 12 aprile 2006 (RS 142.513);
c. il registro informatizzato dello stato civile (Infostar) di cui all'articolo 39 CC (RS 201) e all'articolo 6*a* dell'ordinanza del 28 aprile 2004 sullo stato civile (OSC; RS 211.112.2);
d. il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI) di cui all'articolo 71 LAVS (RS 831.10).

Capoverso 4

Si confrontino i commenti all'articolo 8 capoverso 2.

Capoverso 5

I diversi sistemi d'informazione sono alimentati con dati da differenti fonti. Infostar è il registro centrale dello stato civile ed è alimentato con dati provenienti dagli uffici di stato civile regionali di tutta la Svizzera. L'ISA riprende dati da Infostar o dai registri di controllo degli abitanti, nella misura in cui questi ultimi sono tenuti sulla base degli atti di famiglia o del registro delle famiglie. SIMIC è gestito dalla SEM e contiene dati personali su stranieri che hanno diritto di soggiorno in Svizzera in base ad accordi internazionali.

Se dunque, per esempio, una persona che figura in SIMIC intende far registrare un evento inerente allo stato civile (matrimonio, divorzio, nascita, ecc.), la registrazione può differire (p. es. nell'ortografia del nome). Il Consiglio federale disciplina la procedura in questi casi. Gli accertamenti in caso di presunte o effettive contraddizioni nei dati d'identificazione personale nell'ambito del NAVS13 son già oggi condotti dal servizio di clearing dell'UCC-UPI. I corri-

spondenti accertamenti nell'ambito dell'eID potrebbero parimenti essere affidati a questo servizio.

1.8.8 Sezione 7: Servizio di riconoscimento dei fornitori di servizi identitari

Articolo 21 Competenza

Il Servizio di riconoscimento dei fornitori di servizi identitari (Servizio di riconoscimento) è insediato presso il DFF. La procedura di riconoscimento degli IdP s'ispira a quella per il riconoscimento delle piattaforme di trasmissione (cfr. n. 1.3.2). Un'unità amministrativa è responsabile per l'esecuzione della procedura di riconoscimento. Nel regolamento eIDAS questa funzione è conferita all'organismo nazionale di vigilanza. Dato che il DFF (ODIC) assume altre funzioni dell'organismo nazionale di vigilanza ai sensi del regolamento eIDAS, si propone di insediarvi anche il Servizio di riconoscimento. Si confrontino in merito i commenti al numero 1.4.1.

Articolo 22 Elenco degli IdP riconosciuti

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.

1.8.9 Sezione 8 Emolumenti

Articolo 23

Sono ipotizzabili diverse possibilità per determinare gli emolumenti che il Servizio delle identità e il Servizio di riconoscimento riscuotono dagli IdP. Sarà il Consiglio federale a decidere, in considerazione delle circostanze concrete dell'esecuzione della legge, ad esempio se occorra rinunciare, nei primi cinque anni, a una copertura totale delle spese amministrative, in particolare del Servizio delle identità. Riduzioni degli emolumenti per gli IdP che rilasciano gratuitamente l'eID potrebbero incentivare la diffusione rapida dell'eID, con conseguenti benefici per l'efficienza del traffico elettronico a medio e lungo termine, sia tra privati che con le autorità.

Si presuppone inoltre che il mezzo d'identificazione riconosciuto sia applicato su un supporto che ha a sua volta una funzione, ad esempio una carta bancaria, un settore securizzato di uno smartphone o il supporto per la firma elettronica (p. es. SuisseID) oppure anche una tessera munita di fotografia per collaboratori di un'impresa (p. es. ospedale). Quest'ultima potrebbe in tal caso delegare l'identificazione dei suoi collaboratori a un IdP riconosciuto e usarne il sistema eID per l'autenticazione nel suo sistema informatico. Spetta al mercato determinare se e come fatturare i costi generati dall'utilizzo dell'eID. Il piano ipotizza un modello pay-per-use ma non esclude altri modelli.

1.8.10 Sezione 9: Responsabilità

Articolo 24

Osservazione preliminare

Le responsabilità per danni cagionati utilizzando l'eID sono rette dalle pertinenti disposizioni, note e consolidate, del Codice delle obbligazioni (CO; RS 220) o della legge sulla responsabilità (RS 170.32).

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 presente legge tratta esclusivamente l'identificazione sicura dei partecipanti alle comunicazioni elettroniche.

Al momento si rinuncia pure a introdurre una responsabilità causale dell'IdP analogamente a quella prevista dalla FiEle riveduta. Di conseguenza, anche le regole relative alla prescrizione sono rette dal CO. Al momento della negoziazione di un accordo bilaterale per la notifica degli IdP svizzeri riconosciuti all'UE occorrerà apportare alla presente legge i necessari adeguamenti, prestando particolare attenzione alle disposizioni sulla responsabilità transnazionale.

Capoverso 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 CO. La questione se si tratti di una responsabilità contrattuale o extracontrattuale (delittuale) (art. 41 segg. CO) va valutata nel singolo caso.

Capoverso 2
Il Servizio delle identità e il Servizio di riconoscimento sono attribuiti a unità amministrative della Confederazione e sottostanno alla legge sulla responsabilità (RS 170.32).

1.8.11 Sezione 10: Disposizioni finali

Articolo 25 Modifica di altri atti normativi
In allegato alla legge figurano le modifiche di altri atti normativi proposte. In particolare, il servizio delle identità è autorizzato ad accedere ai menzionati sistemi d'informazione ISA, SIMIC e Infostar. Il sistema d'informazione UCC-UPI non deve essere accessibile mediante procedura di richiamo.

Articolo 26 Referendum ed entrata in vigore
Come ogni legge federale, anche la nuova legge sull'eID sottostà al referendum facoltativo; il Consiglio federale ne determina l'entrata in vigore.

1.8.12 Allegato: Modifica di altri atti normativi

Osservazioni preliminari
Identificazione e autenticazione per servizi della Confederazione che utilizzano l'eID
Dagli accertamenti condotti finora è emerso che i requisiti per l'identificazione e l'autenticazione nell'ambito delle applicazioni di governo elettronico vanno, se del caso, disciplinati a livello di ordinanza o istruzione.

Nel settore agricolo, ad esempio, i diritti materiali d'accesso al sistema d'informazione per il servizio veterinario pubblico sono disciplinati nell'ordinanza del 6 giugno 2014 concernente i sistemi d'informazione per il servizio veterinario pubblico (O-SISVet; RS 916.408). Per il sistema d'informazione Agate, le informazioni concernenti i diritti d'accesso sono elencate nell'allegato all'ordinanza del 23 ottobre 2013 sui sistemi d'informazione nel campo dell'agricoltura (OSIAgr; RS 916.117.71). Sul portale stesso sono descritte le modalità

d'accesso al sistema con una SuisseID o un certificato AdminPKI, richieste per determinate applicazioni.

StartBiz, un servizio in rete della SECO per le piccole e medie imprese, può essere utilizzato dopo essersi registrati con una SuisseID. L'ordinazione in rete di un estratto del casellario giudiziale presso l'UFG è pure possibile con un'eID.

eID in funzione di documento
Un'eID ai sensi della presente legge è intesa fungere da documento d'identificazione. Gli istituti finanziari e i casinò in particolare, che sottostanno alla legge del 10 ottobre 1997 sul riciclaggio di denaro (LRD; RS 955.0), devono poter effettuare un'identificazione elettronica sicura con un'eID. L'eID è un documento probante ai sensi dell'articolo 3 LRD. La definizione esaustiva di documento probante non è però contenuta nella LRD bensì nell'ordinanza FINMA del 3 giugno 2015 sul riciclaggio di denaro (ORD-FINMA; RS 955.033.0). Questa ordinanza andrà se del caso adeguata affinché sia possibile impiegare un'eID nell'ambito delle comunicazioni elettroniche con istituti finanziari e casinò.

1. Legge federale del 22 giugno 2001 sui documenti d'identità (LDI; RS 143.1)

Articolo 1 capoverso 3 secondo periodo
In linea di massima, i passaporti diplomatici e di servizio sono rilasciato unicamente a cittadini svizzeri. Per determinati Stati accreditatari o per assumere certi compiti nell'interesse e su incarico della Svizzera è necessario, per motivi di sicurezza, rilasciare tali documenti anche a persone prive della cittadinanza svizzera, al fine di impedire che accompagnatori stranieri di diplomatici svizzeri o altri impiegati di una rappresentanza svizzera siano confrontati con gravi svantaggi. In parte, anche l'annuncio nello Stato accreditatario ed eventualmente il rilascio di un visto sono possibili soltanto con un passaporto diplomatico o di servizio svizzero. Gli sviluppi sociali nel campo delle unioni personali e, in questo ambito, in particolare il fatto che un numero sempre maggiore di diplomatici ha coniugi o conviventi stranieri ha acuito ulteriormente la suddetta problematica. Si tratta inoltre di agevolare a collaboratori stranieri l'adempimento della propria funzione in singoli casi. Per determinati impieghi in regioni di crisi o di conflitto comportanti elevati rischi per la vita e l'integrità fisica, l'EDA è costretto a reclutare degli specialisti che potrebbero non avere la cittadinanza svizzera, dato che tale impiego non interessa alcun cittadino svizzero. Anche se le viene rilasciato un simile documento svizzero, la persona in questione non acquisisce la cittadinanza svizzera e nel suo passaporto, sulla pagina dei dati personali, alla rubrica Cittadinanza figurerà la sua patria e il luogo d'origine recherà il simbolo ***.

Articolo 11 capoverso 1 lettera k
I dati personali registrati in ISA vanno integrati con il NAVS13 ed eventualmente il numero di registrazione eID. Ciò è imprescindibile per poter attribuire in modo univoco i dati richiesti per l'eID e provenienti da diversi registri della Confederazione. Nella misura in cui il NAVS13 può essere utilizzato come identificatore personale universale in seno all'Amministrazione federale (lett. k), non è necessario riprendere anche un numero di registrazione eID supplementare.

Articolo 12 capoverso 2 lettere g e h
Il Servizio delle identità deve poter richiamare dall'ISA i dati necessari per un'eID, in particolare quelli che non sono registrati in Infostar come i numeri dei documenti, l'immagine del volto 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.

Articolo 14
Dato che con l'introduzione dell'eID riconosciuta i dati provenienti dall'ISA sono registrati anche nei sistemi d'informazione degli IdP riconosciuti e dei Servizi delle identità, questi servizi devono essere esclusi dal divieto di gestire banche dati parallele.

2. Codice civile svizzero (CC, RS 210)

Articolo 43*a* capoverso 4 numero 5
L'articolo 43*a* CC disciplina l'accesso mediante procedura di richiamo ai registri elettronici al fine di gestire lo stato civile della persona. Il Servizio delle identità è aggiunto all'elenco dei servizi aventi accesso a Infostar.

3. Legge federale del 20 dicembre 1946 su l'assicurazione per la vecchiaia e per i superstiti (LAVS, RS 831.10)

Articolo 50*a* capoverso 1 lettera b^{quater}
L'articolo 50*a* LAVS determina i servizi a cui possono essere comunicati dati, in particolare il NAVS13, in deroga all'articolo 33 della legge federale del 6 ottobre 2000 sulla parte generale del diritto delle assicurazioni sociali (LPGA; RS 830.1). L'AP aggiunge a questo elenco il Servizio delle identità. Il presupposto legale formale per l'utilizzo sistematico del NAVS13 da parte del Servizio delle identità e degli IdP è creato all'articolo 9 AP.

4. Legge del 18 marzo 2016 sulla firma elettronica (FiEle; RS 943.03)

Articolo 9 capoverso 1bis
Chiunque richieda il rilascio di una firma elettronica deve presentarsi personalmente. Quest'obbligo viene a cadere se l'identità è dimostrata mediante un'eID.

2 Ripercussioni

2.1 Ripercussioni per la Confederazione

2.1.1 Identificazione sicura in rete

Diversi servizi della Confederazione potranno presumibilmente fare buon uso dell'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 impiegata 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 al numero 1.4.2. L'onere supplementare si limiterà ad adeguamenti delle soluzioni informatiche e all'acquisizione dei servizi degli IdP, ma anche in questo ambito sarà possibile realizzare risparmi semplificando i processi.

Considerando le diverse soluzioni messe in atto all'estero e il loro attuale utilizzo, vi è anche un certo rischio che, per diversi motivi, la soluzione proposta non riesca a imporsi sul mercato malgrado tutti gli accertamenti e i riscontri positivi. Per il presente progetto sono state considerate le esperienze maturate all'estero e si è cercato di trarre le corrette conclusioni dagli errori constatati negli altri Paesi. In fin dei conti, però, saranno gli utenti e il mercato a decidere se la proposta avrà successo.

2.1.2 Osservazione in merito agli acquisti pubblici

Le autorità in veste di gestori di servizi che utilizzano l'eID
Le autorità che offrono un tale servizio gestiscono un servizio che utilizza l'eID ai sensi della presente legge e devono concludere con almeno un IdP un accordo sull'utilizzo di un sistema di eID.

Le prestazioni d'identificazione sono richieste per un'applicazione di governo elettronico gestita in esecuzione di un compito d'interesse pubblico. L'autorità sottostà al diritto in materia di acquisti pubblici. Le prestazioni d'identificazione costituiscono prestazioni informatiche che sottostanno dunque al diritto in materia di acquisti pubblici. Con la presente legge si crea un mercato per questo tipo di prestazioni, che vengono fornite dietro compenso (entrate fiscali).

Per le prestazioni dell'IdP occorre quindi eseguire una procedura d'acquisto pubblico conformemente alle disposizioni applicabili in materia (legge federale del 16 dicembre 1994 sugli acquisti pubblici, LAPub; RS 712.056.1, oppure diritto cantonale) a meno che il Consiglio federale non designi un'unità amministrativa che gestisca un sistema di eID per le esigenze della Confederazione (art. 13 AP).

Fornitori di servizi d'identificazione
Il riconoscimento degli IdP non costituisce per contro una procedura d'acquisto ma un atto di polizia economica a protezione dei clienti che si fonda sull'articolo 95 capoverso 1 Cost. (cfr. n. 4.1).
Il riconoscimento non dipende da una politica 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 ai sensi della presente legge. Un riconoscimento viene rilasciato e rinnovato a condizione che i relativi presupposti (art. 4 AP) siano soddisfatti e le prescrizioni tecniche e organizzative siano rispettate.

2.2 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 governo elettronico. L'utilizzo dell'eID semplifica notevolmente le procedure di identificazione e autenticazione per accedere a questi sistemi. Nel Cantone di Berna, ad esempio, attualmente per compilare elettronicamente la dichiarazione delle imposte occorre inserire una password comunicata per via postale dopo

che il richiedente ha inviato un modulo firmato a mano. Il possesso di un'eID eviterebbe questo scambio postale.

Un'identificazione semplice e sicura favorisce l'utilizzo delle prestazioni di governo elettronico offerte dalle città e dai Comuni. Con l'adeguamento delle procedure, i privati potrebbero evitare di presentarsi personalmente e curare i contatti con le autorità cantonali e comunali indipendentemente da dove si trovano, semplicemente utilizzando dispositivi in grado di connettersi a Internet.

2.3 Ripercussioni per l'economia

Condizioni sicure e disciplinate anche nello spazio digitale contribuiscono in maniera sostanziale a rendere attrattiva e concorrenziale la piazza economica svizzera. Il Consiglio federale vuole che lo Stato contribuisca a un passaggio riuscito della Svizzera a una società dell'informazione. A tal scopo ha deciso numerose misure, per lo più concernenti l'adeguamento del quadro giuridico o l'allestimento di elementi infrastrutturali, tra cui la FiEle o la creazione di numeri d'identificazione delle persone e delle imprese univoci e dei relativi registri.

Mezzi d'identificazione elettronici riconosciuti costituiscono un elemento fondamentale di un ecosistema di eID globale in grado di produrre sicurezza e fiducia nello scambio elettronico di dati e consentono di sbrigare elettronicamente e quindi più efficacemente pratiche complesse con le autorità o tra privati. Generano inoltre nuove e importanti aree d'attività.

2.4 Ripercussioni per la società

L'identificazione sicura dei partner delle comunicazioni elettroniche rende più difficile o impedisce gli abusi e crea fiducia nello spazio digitale.

Sovente in Internet gli abusi si fondano sull'impossibilità di identificare con sicurezza i partner della comunicazione. La posta spam si basa sull'impossibilità di distinguere i mittenti affidabili dagli altri e di perseguire questi ultimi. Nel caso del phishing, spacciandosi per qualcun altro, ad esempio la banca del destinatario, i mittenti dell'email possono provocare danni ingenti. Mezzi d'identificazione riconosciuti aiutano a proteggere l'identità dei titolari nell'attuale mondo globalizzato e altamente interconnesso e rendono notevolmente più difficile il furto d'identità, potenzialmente molto pericoloso. L'introduzione di un numero di registrazione eID evita in tanti casi di dover comunicare il cognome, il nome e la data di nascita. Il numero di registrazione eID è dunque uno pseudonimo univoco che non consente a terzi di risalire ad altri dati personali. In tal modo la sfera privata risulta maggiormente protetta rispetto alla situazione in cui bisogna comunicare i nomi, che terzi possono attribuirsi facilmente.

2.5 Ripercussioni per l'ambiente

L'avamprogetto non ha ripercussioni dirette per l'ambiente. In linea di massima, il crescente passaggio dallo svolgimento fisico delle pratiche a quello elettronico dovrebbe permettere di risparmiare risorse al saldo, con i conseguenti benefici per l'ambiente derivanti dalla possibilità di evitare di presentarsi personalmente presso le autorità, alleggerendo in tal modo l'infrastruttura del traffico e le emissioni.

2.6 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.

3 Rapporto con il programma di legislatura e le strategie nazionali del Consiglio federale

L'avamprogetto di legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge eID) è annunciato nel messaggio del 27 gennaio 2016[12] sul programma di legislatura 2015-2019 e nel decreto federale del 14 giugno 2016[13] sul programma di legislatura 2015-2019.

Il presente avamprogetto mira in particolare a conseguire gli obiettivi di diverse strategie del Consiglio federale, pure incluse nelle grandi linee del programma di legislatura 2015-2019. Nell'aprile 2016, ad esempio, il Consiglio federale ha aggiornato la Strategia Svizzera digitale[14] definendo i campi d'intervento in cui il potenziale d'innovazione delle TIC possa esplicare effetti particolarmente importanti. In diversi campi d'intervento della suddetta strategia, i mezzi d'identificazione elettronica sicuri costituiscono i presupposti per l'attuazione ed elementi dell'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[15] è definire un'identità elettronica valida sul territorio nazionale e all'estero. Ai fini della promozione dell'innovazione e della piazza economica, la Svizzera deve disporre di un piano d'attuazione affidabile per un'identità durevole nello spazio virtuale e in tal modo creare prospettive a lungo termine per l'economia e la società digitale.

4 Aspetti giuridici

4.1 Costituzionalità

La competenza per disciplinare l'eID risulta indirettamente dalla Costituzione federale (Cost., RS 101). Il rilascio di eID è delegato a gestori dell'identità privati, che per essere riconosciuti 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.

Nella misura in cui i presupposti concernono i rapporti contrattuali tra fornitori dell'identità e utenti, l'AP disciplina aspetti di diritto civile e si fonda dunque anche sull'articolo 122 capoverso 1 Cost., che attribuisce alla Confederazione la competenza per legiferare nel campo del diritto civile.

12 FF 2016 909, 966 e 1026

13 FF 2016 4605, 4607

14 Strategia Svizzera Digitale: cfr. link nella bibliografia

15 Strategia di e-government Svizzera: cfr. link nella bibliografia

4.2 Compatibilità con gli impegni internazionali della Svizzera

L'AP è compatibile con gli impegni internazionali vigenti. Nel quadro della sua elaborazione si è provveduto a preservare in linea di massima la possibilità della notifica ai sensi del regolamento eIDAS. Se successivamente auspicato, l'eID svizzera potrà anche essere riconosciuta in tutta l'Europa mediante un accordo bilaterale con l'UE o con singoli Stati membri.

4.3 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 concernenti i mezzi d'identificazione elettronica riconosciuti sotto forma di legge federale.

4.4 Delega di competenze legislative

Acquisizione di un'eID da parte di stranieri
Emanando un'ordinanza il Consiglio federale può escludere dall'acquisizione di un'eID gli stranieri che non possono essere identificati con sicurezza sulla base di documenti d'identità esteri e che non ottengono un permesso di dimora. Se tuttavia risulta necessario l'accesso a servizi che utilizzano l'eID, in particolare nel settore dell'asilo, possono essere previste altre procedure per l'identificazione e l'autenticazione, ad esempio mediante codici d'accesso cartacei. La relativa competenza è conferita all'articolo 3 capoverso 2 AP.

Prescrizioni tecniche e organizzative
Per poter reagire il più possibile tempestivamente agli sviluppi tecnici, i presupposti per le procedure, le prescrizioni tecniche e gli standard sono disciplinati a livello di ordinanza.

L'articolo 3 capoverso 3 AP conferisce al Consiglio federale la competenza di disciplinare l'acquisizione, la procedura di rilascio nonché il blocco e la revoca dell'eID.

In virtù dell'articolo 4 capoverso 4, il Consiglio federale può emanare prescrizioni sui presupposti per il riconoscimento degli IdP, in particolare sui requisiti tecnici e di sicurezza, la copertura assicurativa nonché gli standard applicabili e i protocolli tecnici per i sistemi di eID. Gli standard internazionali e nazionali da applicare vengono rielaborati e ripubblicati a brevi intervalli. Con l'emanazione di un'ordinanza il Consiglio federale può reagire più rapidamente rispetto al Parlamento.

In virtù dell'articolo 5 capoverso 4 AP, i requisiti minimi per le procedure d'identificazione e autenticazione dei diversi livelli di sicurezza possono essere disciplinati a livello di ordinanza. Anche in questo campo è necessaria una certa flessibilità per rimanere al passo con l'evoluzione tecnica.

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 a livello di ordinanza (art. 18 cpv. 2 AP).

Destinatario di un'ordinanza sui più recenti standard applicabili e sui protocolli tecnici per la trasmissione di dati d'identificazione personale è il Servizio delle identità. Il Consiglio federa-

le disciplina la procedura per il caso in cui differenti registri di persone forniscano dati contradditori (art. 20 cpv. 5 AP).

Sistema di eID sussidiario della Confederazione
Se nessun IdP rilascia un'eID per l'identificazione e l'autenticazione adeguata per i servizi che utilizzano l'eID delle autorità, il Consiglio federale può designare un'unità amministrativa che gestisca un tale sistema di eID. Questa unità amministrativa può eventualmente collaborare con privati per l'installazione e la gestione del sistema (art. 13 AP).

Norme di protezione di responsabilità civile per titolari
In virtù dell'articolo 14 capoverso 3 AP, il Consiglio federale può stabilire in un'ordinanza gli obblighi di diligenza che devono essere rispettati dai titolari di un'eID. Tali obblighi possono modificarsi con relativa rapidità conformemente all'evoluzione tecnica. È pertanto opportuno disciplinare la questione in un'ordinanza.

Riscossione di emolumenti
Si confrontino i commenti all'articolo 23.

4.5 Protezione dei dati

4.5.1 Il diritto in materia di protezione dei dati è sufficiente

Le disposizioni del diritto in materia di protezione dei dati (Legge federale del 19 luglio 1992 sulla protezione dei dati, LPD, RS 235.1, e le pertinenti ordinanze) sono sufficienti per garantire la protezione dei dati nel settore dell'eID. Ciononostante, per quanto riguarda la necessità di ottenere il consenso del titolare è stata introdotta nell'AP una disposizione esplicita che limita il trattamento dei dati d'identificazione personale confermati a livello statale: gli IdP possono trattarli unicamente per effettuare identificazioni e autenticazioni (art. 10 cpv. 1 AP).

L'AP limita inoltre la trasmissione di determinati dati d'identificazione personale e i relativi profili d'utilizzo (art. 10 cpv. 3 AP).

4.5.2 Consenso alla trasmissione

Sempre laddove sono in gioco dati d'identificazione personale è importante che siano rispettate le prescrizioni della protezione dei dati e adottati i necessari provvedimenti di sicurezza. I titolari dell'eID danno il loro consenso esplicito alla trasmissione di determinati dati d'identificazione personale. Per il rilascio dell'eID l'IdP è autorizzato a richiamare i dati presso il Servizio delle identità (art. 6 cpv. 3 AP); per l'utilizzo dell'eID presso un servizio che utilizza l'eID l'IdP ha inoltre l'obbligo di chiedere al titolare il consenso per la trasmissione dei dati al suddetto servizio (art. 17 cpv. 1 lett. f AP).

4.5.3 Limitazione della commerciabilità dei dati

Particolare attenzione è prestata alla commercializzazione dei dati. L'articolo 10 capoverso 3 vieta la trasmissione a terzi di dati confermati a livello statale e dei profili su di essi fondati. Si distingue però tra dati di base, trasmessi al livello di sicurezza *basso*, e dati complementari dei livelli di sicurezza *significativo* ed *elevato*. I dati di base numero di registrazione eID, cognome e data di nascita nonché i dati attribuiti dall'IdP (p. es. indirizzo o numero del cliente) non sono compresi nel divieto di commercializzazione. Per contro non possono essere

commercializzati i profili di utilizzo, che si fondano sui dati complementari confermati (p. es. il sesso o lo stato civile).

Da questa limitazione della commerciabilità risulta la diminuzione del valore economico dei dati d'identificazione personale confermati a livello statale, che sono esplicitamente dichiarati non pignorabili e non rientranti nella massa fallimentare (art. 11 cpv. 1 AP). Al fine di garantire la continuità di un sistema di eID e della corrispondente eID in caso di crisi finanziaria di un IdP, i sistemi di eID riconosciuti possono essere venduti nella loro interezza ad altri IdP riconosciuti. Il risultante ricavo rientra nella massa fallimentare (art. 11 cpv. 3 AP).

5 Documentazione supplementare

- Mezzi d'identificazione elettronica riconosciuti a livello statale (eID), Piano 2016
- Riferimenti bibliografici
- Tabella delle concordanze terminologiche

5.1 Riferimenti bibliografici dei documenti citati nel presente rapporto esplicativo

Pag.	Documento	Link (stato al 14 novembre 2016
3	Regolamento eIDAS	Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE GU L 257 del 28.8.2014, pag. 73, rettificato in GU L 272 del 7.10.2016, pag. 96 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:02014R0910-20140917&from=DE
5 9	Decisioni e regolamento d'esecuzione dell'eIDAS	Decisione d'esecuzione (UE) 2015/296 della Commissione del 24 febbraio 2015 che stabilisce modalità procedurali per la cooperazione tra Stati membri in materia di identificazione elettronica a norma dell'articolo 12, paragrafo 7, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 53 del 25.2.2015, pag. 14 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D0296&from=DE
		Decisione di esecuzione (UE) 2015/1505 della Commissione dell'8 settembre 2015 che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 235 del 9.9.2015, pag. 26 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D1505&from=DE

		Decisione di esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 235 del 9.9.2015, pag. 37 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D1506&from=DE
		Decisione di esecuzione (UE) 2015/1984 della Commissione del 3 novembre 2015 che definisce le circostanze, i formati e le procedure della notifica di cui all'articolo 9, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 289 del 5.11.2015, pag. 18 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015D1984&from=DE
		Decisione di esecuzione (UE) 2016/650 della Commissione del 25 aprile 2016 che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 109 del 26.4.2016, pag. 40 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016D0650&from=DE
		Regolamento di esecuzione (UE) 2015/1501 della Commissione dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 235 del 9.9.2015, pag. 1–6 rettificato in GU L 28 del 4.2.2016, pagg. 1-6

		http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015R1501R(01)&from=DE
		Regolamento di esecuzione (UE) 2015/1502 della Commissione dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno GU L 235 del 9.9.2015, pag. 7 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015R1502&from=DE
		Regolamento di esecuzione (UE) 2015/806 della Commissione del 22 maggio 2015 che stabilisce le specifiche relative alla forma del marchio di fiducia UE per i servizi fiduciari qualificati GU L 128 del 23.5.2015, pag. 13 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015R0806&from=DE
		Regolamento (UE) 2015/1017 del Parlamento europeo e del Consiglio del 25 giugno 2015 relativo al Fondo europeo per gli investimenti strategici, al polo europeo di consulenza sugli investimenti e al portale dei progetti di investimento europei e che modifica i regolamenti (UE) n. 1291/2013 e (UE) n. 1316/2013 – il Fondo europeo per gli investimenti strategici GU L 348 del 20.12.2013, pag. 129, modificato dall'ordinanza (UE) 2015/1017, GU L 169 del 1.7.2015, pag. 16 http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015R1017&from=DE
14	Strategia USA NSTIC	National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem https://www.nist.gov/itl/nstic
21	Requisiti NIST di sicurezza	Cybersecurity Framework https://www.nist.gov/cyberframework

38	Strategie del Consiglio fede-rale	Strategia "Svizzera digitale" https://www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/strategia-svizzera-digitale/strategia.html
		Strategia di e-government Svizzera https://www.egovernment.ch/it/umsetzung/e-government-strategie/

5.2 Tabella delle concordanze terminologiche

Piano eID	**Legge eID**	**eIDAS Italiano**	**English**
Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)	Servizio di riconoscimento dei fornitori di servizi identitari (Servizio di riconoscimento)	-	Accreditation Authority
Richiedente	Richiedente	Richiedente	Applicant
Autenticazione	Autenticazione	Autenticazione	Authentication
Identificatore personale univoco (IPU)	Numero di registrazione eID	Identificazione univoca	Unique Personal Identification Number
Mezzi d'identificazione riconosciuti dallo Stato (eID)	Mezzi d'identificazione elettronica riconosciuti a livello statale (eID)	Mezzi di identificazione elettronica	Credential
Sistema di identificazione elettronica (sistema di eID)	Sistema di identificazione elettronica (sistema di eID)	Sistema di identificazione elettronica	Identity System
Identificazione elettronica	Identificazione elettronica	Identificazione elettronica	Identification
Gestore dell'identità elettronica (Identity Provider, IdP), emettitore, rilasciante, riconosciuto a livello statale	Fornitore di servizi identitari (Identity Provider, IdP) riconosciuto a livello statale	Rilasciante	Identity Provider (IdP), Credential Service Provider (CSP)
Prova elettronica dell'identità	Documento d'identità elettronico	Prova elettronica dell'identità	Identity Proofing
Titolare	Titolare	Persona fisica	Claimant/Subscriber
Interoperabilità	Interoperabilità	Interoperabilità	Interoperability
Servizi online	Servizi in rete	Servizi online	Online Services
Dati di identificazione personale (DIP)	Dati d'identificazione personale	Dati di identificazione personale	Identity Attribute
Registrazione	Registrazione	Registrazione	Registration
Servizio svizzero per l'identità elettronica (SIE)	Servizio svizzero delle identità elettroniche (Servizio delle identità)	Fonte affidabile	Steering Group and Attribute Authority, Root Attribute Authority
Parte facente affidamento sulla certificazione (pfac)	Gestore di servizi che utilizzano l'eID	Parte facente affidamento sulla certificazione	Relying Party (RP)
Servizio che fa affidamento sulla certificazione	Servizio che utilizza l'eID	-	Relying Service
Livello di garanzia	Livello di sicurezza	Livello di garanzia	Level of Assurance / Assurance Level