*Avamprogetto*

# Legge federale sui mezzi d'identificazione elettronica riconosciuti

## Legge sull'eID

del …

---

*L'Assemblea federale della Confederazione Svizzera,*
visti gli articoli 95 capoverso 1 e 122 capoverso 1 della Costituzione federale[1],
visto il messaggio del Consiglio federale del …[2],
*decreta:*

## Sezione 1: Disposizioni generali

### Art. 1 Oggetto e scopo

[1] La presente legge disciplina:

a. il contenuto, il rilascio, l'utilizzo, il blocco e la revoca di mezzi d'identificazione elettronica riconosciuti (eID);
b. il riconoscimento dei fornitori di servizi identitari e dei loro sistemi di eID nonché la vigilanza su di essi;
c. i diritti e gli obblighi dei titolari di un'eID;
d. i diritti e gli obblighi dei gestori di servizi che utilizzano l'eID.

[2] Persegue lo scopo di:

a. promuovere comunicazioni elettroniche sicure tra privati e con le autorità; e
b. garantire la standardizzazione e l'interoperabilità delle eID.

### Art. 2 Definizioni

Nella presente legge s'intende per:

RS .....
1 RS **101**
2 FF **…**

a. *mezzo d'identificazione elettronica:* un mezzo elettronico utilizzato per l'identificazione e l'autenticazione di una persona fisica;

*b.* *mezzo d'identificazione elettronica riconosciuto (eID):* un mezzo d'identificazione elettronica rilasciato da un identity Provider (IdP) secondo le prescrizioni della presente legge;

*c.* *identity Provider (IdP):* un fornitore di servizi identitari riconosciuto secondo la presente legge;

d. *identificazione:* utilizzo di dati d'identificazione personale che rappresentano una persona in modo univoco;

e. *autenticazione*: verifica di un'identità dichiarata;

f. *dati d'identificazione personale:* insieme di dati gestito dallo Stato che consente di stabilire l'identità di una persona;

g. *numero di registrazione eID:* un numero d'identificazione attribuito in modo univoco a una persona;

h. *sistema di eID*: sistema elettronico per il rilascio, la gestione e l'utilizzazione di eID;

i. *gestore di un servizio che utilizza l'eID*: persona fisica o giuridica che nel quadro della sua attività gestisce servizi in rete i cui utenti devono disporre di un'identità affidabile e autentica.;

j. *servizio che utilizza l'eID*: un'applicazione informatica che si serve di un sistema di eID.

## Sezione 2: Rilascio di un'eID

### Art. 3 Presupposti personali

[1] Gli IdP possono rilasciare un'eID alle seguenti persone:

a. cittadini svizzeri che al momento del rilascio sono titolari di un documento d'identità svizzero valido conformemente alla legge federale del 22 giugno 2001[3] sui documenti d'identità;

b. cittadini stranieri che al momento del rilascio sono titolari di una carta di soggiorno valida conformemente alla legge federale del 16 dicembre 2005[4] sugli stranieri.

[2] Il Consiglio federale può definire categorie di carte di soggiorno che non consentono di ottenere un'eID. Per l'identificazione e l'autenticazione elettroniche delle persone in questione può prevedere procedure alternative.

3 RS **143.1**
4 RS **142.20**

[3] Il Consiglio federale disciplina i presupposti per l'acquisizione, il rilascio, il blocco e la revoca di un'eID.

**Art. 4** Riconoscimento degli IdP

[1] Gli IdP che intendono rilasciare eID necessitano un riconoscimento del Servizio di riconoscimento dei fornitori di servizi identitari (Servizio di riconoscimento) (art. 21).

[2] Sono riconosciuti gli IdP che:

a. hanno sede in Svizzera;

b. dispongono di un numero IDI conformemente alla legge federale del 18 giugno 2010[5] sul numero d'identificazione delle imprese (LIDI);

c. dimostrano che i responsabili dei sistemi di eID non rappresentano un rischio per la sicurezza;

d. impiegano persone che dispongono delle conoscenze tecniche, dell'esperienza e delle qualifiche necessarie;

e. garantiscono che i sistemi di eID da loro gestiti adempiono i requisiti di sicurezza previsti per il corrispondente livello di sicurezza;

f. detengono e trattano i dati del sistema di eID in Svizzera secondo il diritto svizzero;

g. dimostrano di avere un'assicurazione sufficiente a coprire la responsabilità civile secondo l'articolo 24 o garanzie finanziarie equivalenti;

h. garantiscono il rispetto del diritto applicabile, segnatamente della presente legge e delle sue disposizioni d'esecuzione.

[3] Il riconoscimento deve essere rinnovato al più tardi dopo tre anni.

[4] Il Consiglio federale emana prescrizioni più dettagliate sui presupposti del riconoscimento, in particolare su:

a. i requisiti tecnici e di sicurezza e la loro verifica;

b. la copertura assicurativa necessaria o le garanzie finanziarie equivalenti;

c. gli standard e i protocolli tecnici applicabili ai sistemi di eID nonché la loro verifica regolare.

**Art. 5** Livelli di sicurezza

[1] Gli IdP possono gestire sistemi di eID con differenti livelli di sicurezza correlati fra loro e rilasciare di conseguenza eID che offrono i seguenti gradi di affidabilità:

a. basso: riduzione del rischio di uso abusivo o alterazione dell'identità;

5 RS **431.03**

b. significativo: riduzione significativa del rischio di uso abusivo o alterazione dell'identità;

c. elevato: impedimento dell'uso abusivo o dell'alterazione dell'identità.

[2] I diversi livelli di sicurezza si distinguono per:

a. il processo di rilascio, in particolare per quanto riguarda l'identificazione e l'autenticazione del titolare al momento della registrazione;

b. la gestione del sistema, in particolare per quanto riguarda l'aggiornamento dei dati d'identificazione personale;

c. l'utilizzo, in particolare per quanto riguarda l'identificazione e l'autenticazione; e

d. misure di sicurezza tecniche od organizzative supplementari secondo il corrispondente stato della tecnica.

[3] Un'eID rilasciata per un determinato livello di sicurezza può essere utilizzata anche per un livello di sicurezza inferiore.

[4] Il Consiglio federale disciplina i diversi livelli di sicurezza, in particolare i requisiti minimi per l'identificazione e l'autenticazione.

**Art. 6** Processo di rilascio

[1] Chi desidera un'eID ne richiede il rilascio a un IdP.

[2] L'IdP verifica i presupposti personali.

[3] Con il consenso del richiedente, l'IdP chiede al Servizio svizzero delle identità elettroniche (Servizio delle identità) la trasmissione dei dati d'identificazione personale secondo l'articolo 7 capoversi 1 e 2.

[4] L'IdP attribuisce i dati d'identificazione personale all'eID e l'eID alla persona fisica.

[5] Il Servizio delle identità mette a verbale la trasmissione dei dati.

**Art. 7** Dati d'identificazione personale

[1] Il Servizio delle identità attribuisce i seguenti dati d'identificazione personale a un'eID:

a. numero di registrazione eID;

b. cognome ufficiale;

c. nomi;

d. data di nascita.

[2] Per i livelli di sicurezza significativo ed elevato può inoltre attribuire all'eID i seguenti dati d'identificazione personale:

a. il numero d'assicurato di cui all'articolo 50*c* della legge federale del 20 dicembre 1946[6] su l'assicurazione per la vecchiaia e per i superstiti (numero d'assicurato);

b. il sesso;

c. il luogo di nascita;

d. lo stato civile;

e. la cittadinanza e se del caso lo statuto di soggiorno;

f. l'immagine del viso;

g. il numero e il tipo del documento d'identità o della carta di soggiorno rilasciati dalla Svizzera;

h. l'immagine della firma.

[3] Può integrare i dati d'identificazione personale con informazioni supplementari, in particolare il momento del più recente aggiornamento dei dati nei sistemi d'informazione secondo l'articolo 20.

[4] L'IdP può attribuire dati supplementari a un'eID.

**Art. 8** Aggiornamento dei dati d'identificazione personale

[1] L'IdP aggiorna i dati d'identificazione personale da esso gestiti, ottenendoli automaticamente presso il Servizio delle identità in base al numero di registrazione eID, almeno con le scadenze seguenti:

a. per eID del livello di sicurezza basso: annualmente;

b. per eID del livello di sicurezza significativo: trimestralmente;

c. per eID del livello di sicurezza elevato: settimanalmente.

[2] È responsabile per il blocco o la revoca immediati delle eID da esso rilasciate nel caso in cui il numero di registrazione eID non debba più essere utilizzato.

**Art. 9** Utilizzo sistematico del numero d'assicurato per lo scambio di dati

[1] Il Servizio delle identità è autorizzato a utilizzare sistematicamente il numero d'assicurato per identificare le persone nell'ambito dello scambio elettronico di dati con i registri di persone secondo l'articolo 20 capoverso 2.

[2] L'IdP non può utilizzare il numero d'assicurato per l'identificazione di persone; può però registrarlo nel suo sistema di eID e comunicarlo ai gestori di servizi che utilizzano l'eID e sono autorizzati a usare il numero d'assicurato.

6 RS **831.10**

**Art. 10** Trattamento e trasmissione di dati

[1] Gli IdP possono trattare i dati d'identificazione personale trasmessi dal Servizio delle identità unicamente per effettuare identificazioni e autenticazioni secondo la presente legge.

[2] Possono trasmettere ai gestori di servizi che utilizzano l'eID unicamente i dati d'identificazione personale corrispondenti al livello di sicurezza richiesto e a condizione che il titolare dell'eID vi acconsenta.

[3] Né IdP riconosciuti né gestori di servizi che utilizzano l'eID possono comunicare a terzi i dati d'identificazione personale secondo l'articolo 7 capoverso 2 o i profili di utilizzo su di essi fondati.

[4] Per il resto si applica la legislazione sulla protezione dei dati.

**Art. 11** Scadenza del riconoscimento

[1] Il riconoscimento scade con l'avvio della procedura di fallimento dell'IdP. I sistemi di eID non sono pignorabili e non rientrano nella massa fallimentare.

[2] L'IdP notifica al Servizio di riconoscimento la prevista cessazione dell'attività indicando il modo di procedere previsto per quanto riguarda le eID rilasciate.

[3] I sistemi di eID di un IdP che cessa la sua attività o nei cui confronti è stata avviata una procedura di fallimento possono essere ceduti a un altro IdP riconosciuto. Il ricavato della cessione rientra in un'eventuale massa fallimentare.

**Art. 12** Misure di vigilanza e revoca del riconoscimento

[1] Il Servizio di riconoscimento adotta le misure necessarie se constata che un IdP non rispetta le prescrizioni, segnatamente se non adempie più i presupposti per il riconoscimento.

[2] Se sussiste la speranza di sanare il vizio, il Servizio di riconoscimento stabilisce a tal fine un termine adeguato.

[3] Il Servizio di riconoscimento può revocare il riconoscimento dell'IdP che:

a. viola le disposizioni della presente legge;

b. non adempie più i presupposti per il riconoscimento secondo l'articolo 4 capoverso 1;

c. non soddisfa i requisiti posti dal Servizio di riconoscimento; o

d. impiega, in veste di responsabili dei sistemi di eID, persone oggetto di una condanna passata in giudicato per reati connessi alla criminalità su Internet.

**Art. 13** Sistema di eID sussidiario della Confederazione

[1] Se nessun IdP è riconosciuto per il rilascio di eID di livello di sicurezza significativo o elevato, il Consiglio federale può designare un'unità amministrativa che gestisca un sistema di eID e rilasci eID al fine di soddisfare le esigenze delle autorità.

[2] Può inoltre prevedere che tale sistema possa essere istituito e gestito in collaborazione con privati.

## Sezione 3: Titolari di un'eID

### Art. 14 Obblighi

[1] Un'eID è personale e non può essere messa a disposizione di terzi.

[2] Il titolare di un'eID deve adottare le misure necessarie e ragionevolmente esigibili nelle circostanze date, affinché l'eID non possa essere usata in modo abusivo.

[3] Il Consiglio federale stabilisce gli obblighi di diligenza da rispettare in relazione all'eID.

## Sezione 4: Gestori di servizi che utilizzano eID

### Art. 15 Accordo con un IdP

Chi intende gestire un servizio che utilizza un'eID deve stipulare un accordo con un IdP. Tale accordo disciplina in particolare:

a. i livelli di sicurezza applicati;

b. i processi tecnici e organizzativi da rispettare.

### Art. 16 Autorità in veste di gestori di servizi che utilizzano eID

L'autorità che, in esecuzione del diritto federale, prevede di effettuare un'identificazione elettronica deve accettare tutte le eID ai sensi della presente legge che adempiono il livello di sicurezza richiesto.

## Sezione 5: Fornitori di servizi identitari (IdP)

### Art. 17 Obblighi

[1] L'IdP ha i seguenti obblighi:

a. provvede al corretto funzionamento e alla gestione sicura del sistema di eID;

b. attribuisce i dati d'identificazione personale all'eID e l'eID alla persona fisica;

c. allestisce il sistema di eID in modo da poter sempre verificare in modo affidabile e gratuitamente, mediante una procedura usuale, la validità di tutte le eID che rilascia;

d. rispetta i requisiti di sicurezza secondo l'articolo 4 capoverso 1 lettera e;

e. aggiorna periodicamente i dati d'identificazione personale presso il Servizio delle identità;

f. chiede al titolare dell'eID il consenso esplicito per la prima trasmissione di dati d'identificazione personale a gestori di servizi che utilizzano l'eID;

g. cancella i dati sull'utilizzo di un'eID dopo sei mesi.

[2] Istituisce un servizio clienti che consente di ricevere e trattare le notifiche di problemi o perdite di un'eID. Notifica al Servizio delle identità errori nei dati d'identificazione personale.

[3] Se vi è il pericolo che un terzo possa avere accesso a un'eID o se sono notificati la perdita o il sospetto di uso abusivo di un'eID, l'IdP è tenuto a bloccare immediatamente l'eID.

[4] Deve accertare che la persona che ha richiesto il blocco dell'eID vi sia autorizzata. Informa immediatamente il titolare dell'eID sul blocco.

**Art. 18** Interoperabilità

[1] Gli IdP riconoscono vicendevolmente i loro sistemi di eID e ne garantiscono l'interoperabilità.

[2] Il Consiglio federale stabilisce gli standard tecnici e definisce le interfacce.

## Sezione 6: Servizio svizzero delle identità elettroniche

**Art. 19** Organizzazione

Il Servizio svizzero delle identità elettroniche (Servizio delle identità) è aggregato al DFGP.

**Art. 20** Compiti e obblighi

[1] Il Servizio delle identità attribuisce i dati d'identificazione personale di cui all'articolo 7 capoversi 1 e 2 ai corrispondenti numeri di registrazione eID e li trasmette agli IdP.

[2] Gestisce un sistema d'informazione per la trasmissione dei dati d'identificazione personale agli IdP. Questo sistema d'informazione ha accesso ai registri di persone seguenti:

a. il sistema d'informazione sui documenti d'identità (ISA);

b. il sistema d'informazione centrale sulla migrazione (SIMIC);

c. il registro informatizzato dello stato civile (Infostar); e

d. il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI).

[3] Il sistema d'informazione è concepito in modo da poter confrontare i propri dati con quelli dei registri di persone di cui al capoverso 2.

[4] Il Servizio delle identità garantisce che l'IdP possa sempre verificare la validità del numero di registrazione eID in modo affidabile e gratuitamente mediante una procedura usuale.

[5] Il Consiglio federale definisce gli standard applicabili e i protocolli tecnici per la trasmissione e disciplina il modo di procedere per il caso in cui differenti registri di persone forniscano dati contradditori.

## Sezione 7: Servizio di riconoscimento per i fornitori di servizi identitari

### Art. 21 Competenza

[1] Il Servizio di riconoscimento per i fornitori di servizi identitari (Servizio di riconoscimento) è aggregato al DFF.

[2] È competente per il riconoscimento degli IdP e dei loro sistemi di eID e per la relativa vigilanza.

### Art. 22 Elenco degli IdP riconosciuti

Il Servizio di riconoscimento pubblica l'elenco degli IdP riconosciuti e dei loro sistemi di eID.

## Sezione 8: Emolumenti

### Art. 23

[1] Il Servizio delle identità e il Servizio di riconoscimento riscuotono degli emolumenti dagli IdP per decisioni e prestazioni di servizi.

[2] Il Consiglio federale disciplina gli emolumenti nel quadro dell'articolo 46*a* della legge del 21 marzo 1997[7] sull'organizzazione del Governo e dell'Amministrazione. Al fine di stabilire gli emolumenti per la trasmissione di dati d'identificazione personale può in particolare considerare se si tratta di una prima trasmissione o dell'aggiornamento di dati d'identificazione personale e se l'IdP rilascia gratuitamente l'eID al titolare.

[7] RS **172.010**

## Sezione 9: Responsabilità

### Art. 24

1 Le responsabilità del titolare, del gestore di servizi che utilizzano eID e dell'IdP sono rette dal Codice delle obbligazioni[8].

2 Le responsabilità del Servizio delle identità e del Servizio di riconoscimento sono rette dalla legge del 14 marzo 1958[9] sulla responsabilità.

## Sezione 10: Disposizioni finali

### Art. 25 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato.

### Art. 26 Referendum ed entrata in vigore

[1] La presente legge sottostà a referendum facoltativo.

[2] Il Consiglio federale ne determina l'entrata in vigore.

8 RS **220**
9 RS **170.32**

*Allegato*

## Modifica di altri atti normativi

Gli atti normativi qui appresso sono modificati come segue:

## 1. Legge del 22 giugno 2001[10] sui documenti d'identità

*Art. 1 cpv. 3 secondo periodo*

**3** … I titolari possono anche essere cittadini stranieri.

*Art. 11 cpv. 1 lett. k e cpv. 3*

1 L'Ufficio federale di polizia gestisce un sistema d'informazione. Tale sistema contiene i dati personali che figurano nel documento d'identità e quelli che vi sono registrati, nonché i dati seguenti:

k. il numero d'assicurato conformemente alla legge su l'assicurazione per la vecchiaia e per i superstiti.

3 Il trattamento dei dati serve per rilasciare e aggiornare i mezzi d'identificazione elettronica conformemente alla legge del ….[11] sull'eID.

*Art. 12 cpv. 2 lett. g e h*

2 Per adempiere i compiti spettanti loro per legge, le autorità o i servizi seguenti possono, mediante procedura di richiamo, consultare i dati del sistema d'informazione:

g. la Direzione consolare del Dipartimento federale degli affari esteri;

h. il Servizio svizzero delle identità elettroniche (Servizio delle identità) di cui all'articolo 19 della legge sull'eID[12].

*Art. 14* Divieto di gestire banche dati parallele

È vietata la gestione di banche dati parallele, tranne per la conservazione limitata nel tempo da parte dell'autorità di rilascio dei moduli della domanda e dei dati trasmessi al Servizio delle identità.

10 RS **143.1**
11 RS …., FF ….
12 RS …., FF ….

## 2. Codice civile[13]

*Art. 43a cpv. 4 n. 5*

4 Hanno accesso mediante procedura di richiamo ai dati necessari alla verifica dell'identità di una persona:

5. il Servizio svizzero delle identità elettroniche di cui all'articolo 19 della legge del ….[14] sull'eID.

## 3. Legge federale del 20 dicembre 1946[15] su l'assicurazione per la vecchiaia e per i superstiti (LAVS)

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

1 Purché nessun interesse privato preponderante vi si opponga, gli organi incaricati di applicare la presente legge o di controllarne o sorvegliarne l'esecuzione possono comunicare i dati, in deroga all'articolo 33 LPGA[16]:

b^quater^ al Servizio svizzero delle identità elettroniche di cui all'articolo 19 della legge del ...[17] sull'eID;

## 4. Legge del 18 marzo 2016[18] sulla firma elettronica (FiEle)

*Art. 9 cpv. 1bis*

1bis Se l'identità è provata mediante un'eID ai sensi della legge del ….[19] sull'eID, i richiedenti non devono presentarsi personalmente.

13 RS **210**
14 RS …., FF…
15 RS **831.10**
16 RS 830.1
17 RS …., FF…
18 RS **943.03**
19 RS …., FF…

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.

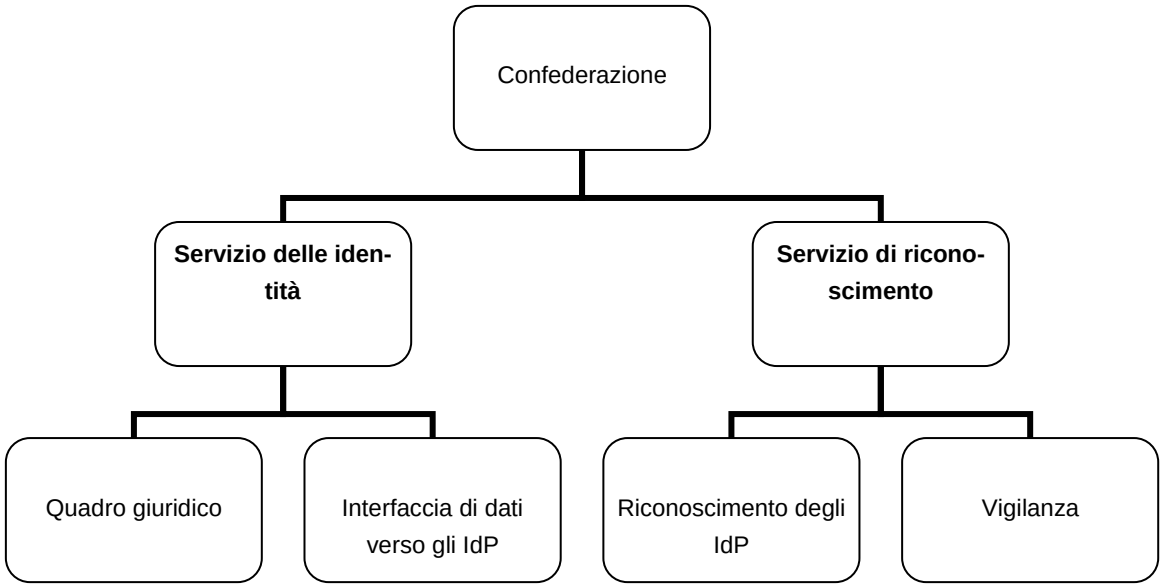
### 1.2.6 Contributo dello Stato ai sistemi di eID

**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).

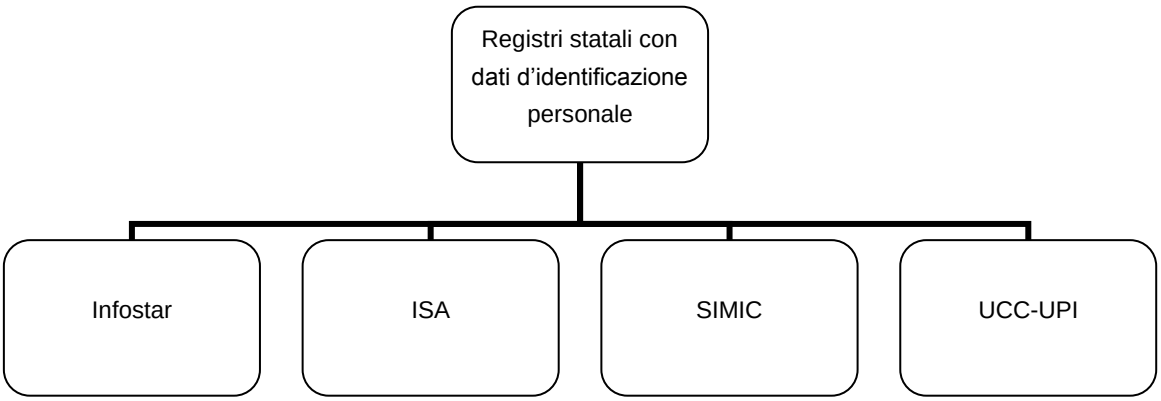



**Registro con dati d'identificazione personale**

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 attributi 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 16-25$^{bis}$ 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. 143$^{bis}$ 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. 144$^{bis}$, 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 1$^{bis}$**
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<br><br>GU L 257 del 28.8.2014, pag. 73, rettificato in GU L 272 del 7.10.2016, pag. 96<br><br>http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:02014R0910-20140917&from=DE |
| 5<br><br>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<br><br>GU L 53 del 25.2.2015, pag. 14<br><br>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<br><br>GU L 235 del 9.9.2015, pag. 26<br><br>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<br><br>GU L 235 del 9.9.2015, pag. 37<br><br>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<br><br>GU L 289 del 5.11.2015, pag. 18<br><br>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<br><br>GU L 109 del 26.4.2016, pag. 40<br><br>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<br><br>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<br><br>GU L 235 del 9.9.2015, pag. 7<br><br>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<br><br>GU L 128 del 23.5.2015, pag. 13<br><br>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<br><br>GU L 348 del 20.12.2013, pag. 129, modificato dall'ordinanza (UE) 2015/1017, GU L 169 del 1.7.2015, pag. 16<br><br>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<br><br>https://www.nist.gov/itl/nstic |
| 21 | Requisiti NIST di sicurezza | Cybersecurity Framework<br><br>https://www.nist.gov/cyberframework |

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
**Ufficio federale di polizia fedpol**
Settore Sviluppo documenti d'identità

# Mezzi d'identificazione elettronica riconosciuti a livello statale (eID)

# Piano 2016

Versione del 02.02.2017

Un'eID serve a provare la propria identità nel mondo digitale.

## Panoramica

Con la diffusione di Internet e la grande disponibilità di dispositivi mobili altamente performanti, è sempre più semplice trasferire i processi operativi nel mondo digitale. Secondo i dati dell'Ufficio federale di statistica [1], nel 2015 in media l'88% della popolazione ha usato Internet: il 56% per acquisti online, il 49% per operazioni di eBanking, il 48% per servizi legati ai viaggi, il 48% per compilare moduli delle autorità online e il 35% per attività politiche. Ha usato Internet per i contatti con le autorità il 79% del totale degli utenti della rete. Le spese in eCommerce delle famiglie sono salite nell'arco di un decennio a oltre sette miliardi di franchi nel 2014.

La certezza del diritto e la sicurezza sono premesse essenziali per lo svolgimento delle operazioni. Questo 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. Ad integrazione di tutto questo, ora dovrà essere possibile provare l'identità di una persona fisica anche in un ambiente elettronico. A tale scopo, il Consiglio federale ha incaricato il DFGP di elaborare un piano per i mezzi d'identificazione elettronica (eID) riconosciuti a livello statale. Le eID riconosciute a livello statale consentiranno a chi ne è in possesso di registrarsi in modo sicuro ai servizi online e successivamente di fare il log-in sempre in sicurezza. I gestori dell'identità digitale possono offrire ulteriori servizi fiduciari, come la firma elettronica, ma essi non rientrano nell'eID.

Il piano per l'eID, ora disponibile, si basa sui lavori svolti da fedpol negli anni 2013-2015, nel cui ambito sono stati consultati anche importanti stakeholder del mercato. Esso tiene inoltre conto delle conoscenze relative a soluzioni precedenti per sistemi di eID, delle direttive [2][3] relative alla compatibilità UE[1] e degli sviluppi internazionali relativi a soluzioni pratiche valide per sistemi di eID [4][5][6][7][8]. Per quanto possibile, si è tenuto anche conto dei requisiti nel campo della cartella informatizzata del paziente (LCIP) [9] e della firma elettronica (FiEle) [10].

Il piano prevede che la Confederazione non rilasci una propria eID ma possa riconoscere e controllare, a tre livelli di sicurezza, a livello statale, sistemi di eID idonei presenti sul mercato. A tal fine la Confederazione istituisce ex novo un Servizio di riconoscimento per i gestori dell'identità elettronica *(SRGI)*. La Confederazione funge inoltre da garante dell'identità dei titolari di un'eID, trasmettendo per via elettronica i dati di identificazione personali (cognome, nome/nomi, data di nascita, foto ecc.) agli emettitori di eID riconosciuti a livello statale. Sarà responsabile di questo secondo compito presso la Confederazione il nuovo Servizio svizzero per l'identità elettronica *(SIE)*.

Al fine di garantire la certezza del diritto nel campo dell'eID, la Confederazione vara una *Legge federale sulle unità d'identificazione elettronica riconosciute a livello statale (legge sull'eID*)*,* con le necessarie disposizioni d'esecuzione, che conterranno le direttive tecniche ed organizzative concrete per i sistemi di eID riconosciuti a livello statale, al fine di creare quella solida base di fiducia di cui si ha bisogno. Andrà, tra le altre cose, garantita l'interoperabilità tra i diversi gestori di sistemi di eID. Il presente piano è servito come base, a livello di contenuti, per l'elaborazione della legge sull'eID.

[1] Esse consentono il riconoscimento reciproco dei sistemi di eID. Per la cosiddetta notifica c'è comunque bisogno della sottoscrizione di un accordo bilaterale con l'UE.

Indice

## Indice delle figure



## Indice delle tabelle

## Indice dei termini

A livello nazionale ed internazionale si sono affermati nel campo dell'eID diversi termini, per i quali rimandiamo all'indice seguente e al glossario nell'allegato.

| Piano eID | Legge sull'eID | eIDAS | English |
|---|---|---|---|
| Servizio di riconoscimento per gestori dell'identità elettronica (SRGI) | Servizio di riconoscimento per i gestori dell'identità elettronica (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 di identificazione riconosciuti dallo Stato (eID) | Unità d'identificazione 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 | Gestore dell'identità elettronica (Identity Provider, IdP) riconosciuto a livello statale | Rilasciante | Identity Provider (IdP), Credential Service Provider (CSP) |
| 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 per l'identità elettronica (Servizio per l'identità) | Fonte affidabile | Steering Group and Attribute Authority, Root Attribute Authority |
| Parti facenti affidamento sulla certificazione (pfac) | Gestore di servizi facenti affidamento sulla certificazione | Parte facente affidamento sulla certificazione | Relying Party (RP) |
| Servizio che fa affidamento sulla certificazione | Servizio facente affidamento sulla certificazione | - | Relying Service |
| Livello di garanzia | Livello di sicurezza | Livello di garanzia | Level of Assurance / Assurance Level |

# 1 Introduzione

## 1.1 Struttura e contenuti

Questo documento illustra le riflessioni di fondo che hanno portato al piano sull'eID e al relativo disegno di legge, concernente i mezzi d'identificazione elettronica riconosciuti a livello statale. Si presentano le funzioni dei partecipanti all'ambiente eID, i procedimenti per l'acquisizione e l'utilizzo di eID riconosciute a livello statale, le riflessioni concernenti la sicurezza e il ruolo dello Stato e le conseguenze di natura finanziaria. In un capitolo a parte si presentano l'organizzazione, la funzionalità e i costi del nuovo **Servizio svizzero per l'identità elettronica (SIE)** e del nuovo **Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)** presso la Confederazione. Il primo funge da servizio elettronico per la trasmissione ai gestori dell'identità elettronica di ulteriori attributi identitari amministrati a livello statale, mentre il secondo interviene principalmente come organo di controllo. In allegato vengono infine introdotti i contesti e i termini della gestione dell'identità digitale, che sono alla base del presente piano.

## 1.2 Mezzi d'identificazione elettronica

### 1.2.1 Di cosa si tratta?

Per svolgere online i processi operativi, i partner (di seguito denominati **parti facenti affidamento sulla certificazione (pfac**) devono avere fiducia nell'identità dichiarata e nell'autenticazione online della controparte, sia a livello nazionale che internazionale. Se nel mondo fisico i documenti pubblici, come il passaporto o la carta d'identità, sono i mezzi con i quali si prova in modo affidabile la propria identità, nel mondo digitale sono i **mezzi d'identificazione elettronica (eID)**. Un'eID consente alle parti facenti affidamento sulla certificazione di identificare ed autenticare i soggetti prima dell'erogazione di un servizio fiduciario. Le eID affidabili sono quindi elementi necessari ai fini dell'implementazione di processi operativi elettronici.

L'eID viene rilasciata da un **gestore dell'identità elettronica (Identity Provider, IdP)** statale o privato, che attribuisce l'eID ad una persona identificata in modo affidabile (di seguito denominato **titolare**) attraverso un processo di registrazione. Un'eID contiene un **identificatore**[2] digitale univoco ed una funzione che collega in modo sicuro l'eID ad una persona e che viene chiamato **autenticatore**[3]. Con un'eID, un titolare può trasmettere ad una parte facente affidamento sulla certificazione, ad es. un portale Internet di uno shop di eCommerce, **attributi identitari** come il nome, l'età, la nazionalità ecc. (**identificazione**) e provare di essere la persona a cui appartengono gli attributi identitari indicati (**autenticazione**). Tale persona sarà poi nota alla parte facente affidamento sulla certificazione attraverso l'identificatore digitale univoco dell'eID o tramite uno pseudonimo ad essa attribuito[4].

---

[2] L'identificatore è un codice digitale legato all'eID in modo sicuro; esso rappresenta il titolare di un'eID in un'identificazione online.

[3] L'autenticatore verifica, quando viene utilizzata l'eID, la presenza fisica del titolare, controllando ad esempio che sia stato inserito il codice PIN corretto o la caratteristica biometrica appartenente al titolare. Svolge la funzione di autenticatore anche il supporto fisico di un'eID (smartcard, smartphone ecc.), che un titolare detiene stabilmente.

[4] L'identificatore dell'eID può essere anche utilizzato con la protezione della crittografia ed essere definito a livello settoriale per ciascuna parte facente affidamento sulla certificazione o persino in via transitoria, per un contatto di breve durata.

Al momento dell'utilizzo, l'eID identifica il titolare tramite l'identificatore digitale e fornisce una prova digitale[5] della presenza del soggetto. L'eID consente così alle parti facenti affidamento sulla certificazione di identificare ed autenticare il titolare ad un determinato **livello di garanzia**. Ciò dipende da quanto sicuro è il processo di registrazione[6], da quanto sicuro è il funzionamento dell'eID sul campo, dalla sicurezza con la quale si verifica la presenza del titolare quando viene utilizzata l'eID e dalla sicurezza della comunicazione del risultato di un'identificazione o autenticazione alla parte facente affidamento sulla certificazione[7]. Anche gli attributi identitari trasmessi sono definiti ad un determinato livello di sicurezza, potendo presumere che gli attributi identitari definiti a livello statale, i cosiddetti **dati di identificazione personale (DIP)** siano molto sicuri. Lo Stato è dunque predestinato a mettere tali dati a disposizione degli IdP riconosciuti a livello statale, i quali possono a loro volta trasmetterli alle parti facenti affidamento sulla certificazione su incarico del titolare.

Un'eID, con i relativi dati di identificazione personale, diventa l'elemento di collegamento digitale tra la persona fisica e la sua identità definita a livello statale (di seguito denominata **identità civile**[8]**)**, utilizzata da parti facenti affidamento sulla certificazione per organizzare i processi operativi. Ai fini della semplificazione di tali operazioni, in Svizzera viene introdotto nel contesto dell'eID anche un **identificatore personale univoco (IPU**) come ulteriore attributo dell'identità civile.

In allegato si fornisce un'introduzione dettagliata ai contesti e ai concetti relativi alla gestione dell'identità digitale. Qui si presentano solamente i concetti più importanti e il loro significato.

Nell'insieme, si definiscono **ambiente eID** tutte le persone fisiche e giuridiche, le parti facenti affidamento sulla certificazione, i gestori dell'identità elettronica e le istanze pubbliche che utilizzano o contribuiscono a far funzionare i mezzi d'identificazione elettronica e i servizi fiduciari su di essi basati, come la firma elettronica, le protezioni delle transazioni ecc. Rientrano nell'ambiente eID anche i servizi statali svizzeri e quelli dell'UE che attuano le disposizioni di legge e quelli che erogano eventualmente altri servizi a sostegno del mercato digitale, come ad esempio un **servizio attributi** o i servizi proxy paneuropei pianificati per l'utilizzo internazionale delle eID. La **gestione dell'identità elettronica (eIDM)** e i corrispondenti **sistemi di eID**, gestiti dagli IdP, costituiscono la spina dorsale dell'ambiente eID.

Le istanze e le relazioni più importanti di un ambiente eID per i sistemi di eID svizzeri riconosciuti a livello statale sono riportati nella Figura 1[9].

---

5 In casi normali, l'eID è utilizzabile solo se la persona autorizzata attiva l'eID con un'azione appropriata e quindi prova in modo implicito anche la propria presenza fisica.

6 Nel processo di registrazione, al momento del rilascio dell'eID, da un lato si collega la persona all'eID (ad es. definendo un codice PIN che la persona deve poi sempre inserire al momento dell'utilizzo dell'eID) e dall'altro si verifica l'identità della persona (ad es. attraverso l'esibizione di un documento statale).

7 I livelli di garanzia sono definiti da standard e regole comuni („Trust Framework" [28] [8]) che tutte le parti dell'ambiente eID devono rispettare. La fiducia complessiva nella sicurezza è composta da tre elementi: robustezza della registrazione e dell'identificazione iniziale, robustezza dell'autenticazione al momento dell'utilizzo dell'eID e robustezza della trasmissione dei risultati di una verifica alle parti facenti affidamento sulla certificazione [6].

8 L'identità civile è l'insieme dei dati di identificazione personale rilevati per una persona nei registri dello stato civile. Alcuni di questi attributi o il nuovo identificatore personale univoco sono già sufficienti per determinare un'identità civile in modo univoco.

9 Si trova un modello di riferimento completo per un ambiente eID, ad esempio in [29]. Tuttavia, il modello che riporta solo le istanze più rilevanti è più utile ai fini del posizionamento e di una rappresentazione semplice da comprendere delle interazioni di fondo di un'eID statale.

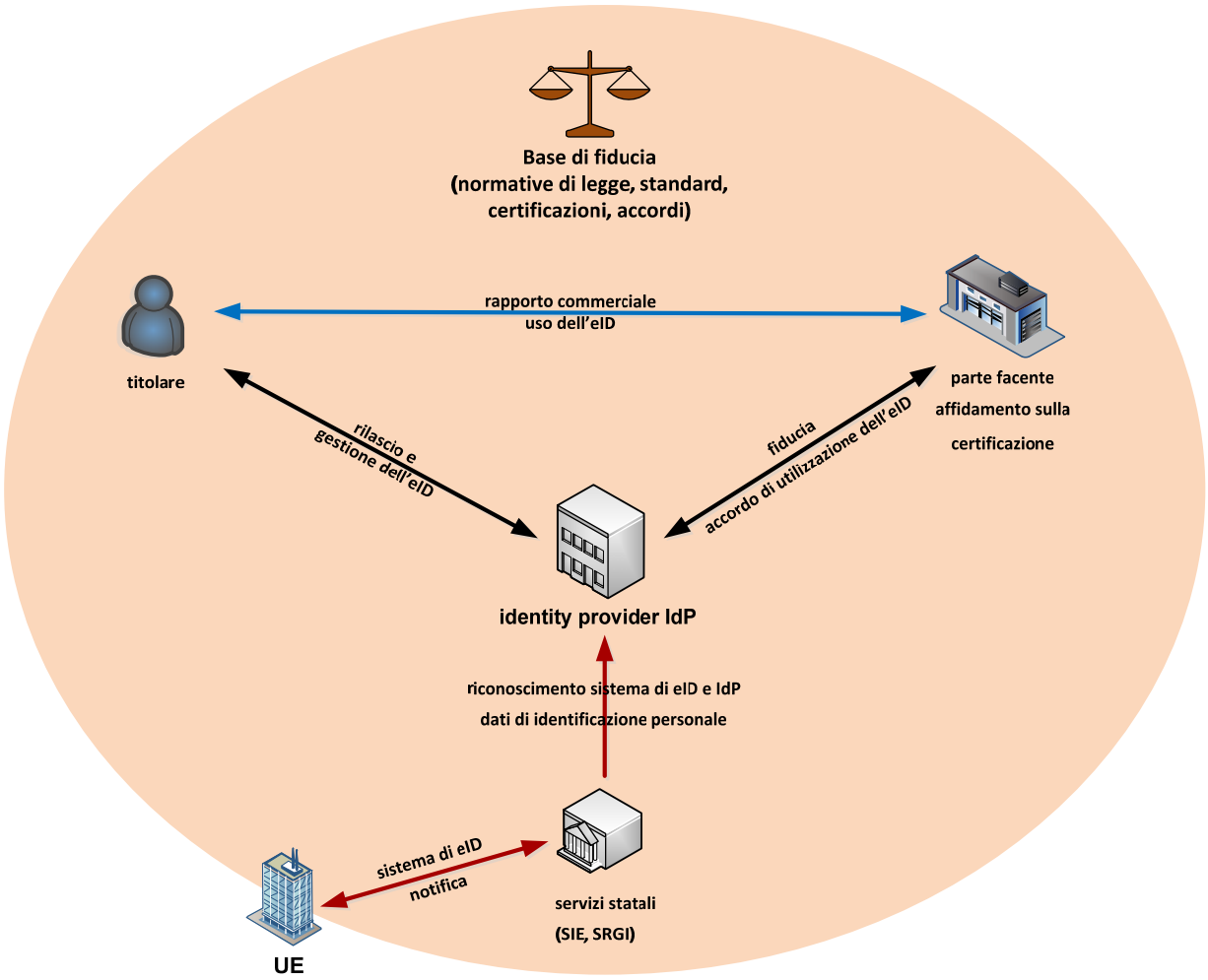



Figura 1: Le istanze e le relazioni più importanti dell'ambiente eID

### 1.2.2 Affidabilità

Si può ritenere un'eID affidabile se i processi e i procedimenti di rilascio ed utilizzo dell'eID nonché la trasmissione dei risultati delle verifiche da parte degli IdP a parti facenti affidamento sulla certificazione sono sicuri e se si verifica periodicamente che l'intero sistema di eID soddisfi i criteri di sicurezza, standardizzati ed aggiornati.

Sono a tal fine particolarmente importanti la registrazione, la tecnologia usata nel sistema di eID e l'organizzazione dell'IdP, la correttezza degli attributi rilevati, la sicurezza dell'eID sul campo e i protocolli per l'utilizzazione interoperabile dell'eiD:

- Al momento della **registrazione** di una persona nel sistema di eID, l'IdP da un lato rileva gli attributi dell'identità civile, che identificano il titolare all'interno della **popolazione**, e dall'altro gli **attributi personali** come **fattori di autenticazione** per la successiva autenticazione del titolare con l'eID. I fattori di autenticazione vengono perlopiù rilevati non a livello centrale ma solo nel dispositivo di supporto dell'eID. Nel corso del **processo di collegamento**, essi sono connessi in modo definitivo all'autenticatore dell'eID[10]. Entrambi

[10] Al momento della registrazione, l'autenticatore dell'eID rileva i fattori di autenticazione come dati di riferimento. In occasione di una successiva autenticazione, al momento dell'utilizzo, l'eID rileva automaticamente ex novo i fattori di autenticazione, li confronta con i dati di riferimento ed accetta o rifiuta la persona rilevata come autenticata o meno.

i processi parziali vanno gestiti nel quadro di un protocollo sicuro dal punto di vista tecnico ed organizzativo, definito in base ai requisiti corrispondenti al livello di garanzia dell'eID. Dopo la registrazione, nell'IdP l'identificatore univoco dell'eID è attribuito ai dati identitari del titolare rilevati.

- La **tecnologia** utilizzata e l'**organizzazione** dell'IdP devono soddisfare i requisiti per il livello di garanzia definito del sistema di eID[11]. L'IdP è responsabile della corretta registrazione, del corretto funzionamento dell'eID sul campo e della corretta trasmissione dei dati identitari e dei risultati dell'autenticazione alle parti facenti affidamento sulla certificazione in tutto l'ambiente di eID. L'IdP deve implementare a tal fine sistemi e processi sicuri, standardizzati, trasparenti e certificati[12]. Ciò viene garantito nel quadro del processo di riconoscimento del sistema di eID e dell'IdP rilasciante e viene periodicamente controllato mediante audit. Gli IdP riconosciuti a livello statale devono avere una sede legale in Svizzera e garantire di essere in grado di far fronte ad eventuali responsabilità derivanti dalle disposizioni di legge. Devono inoltre provare di conservare esclusivamente in Svizzera tutti i dati di identificazione personale.
- L'IdP è responsabile della **corretta assegnazione degli attributi identitari all'eID**. Utilizza fonti di attributi sicure e affidabili[13], garantite sempre laddove possibile dallo Stato. Col consenso del titolare, riceve i dati di identificazione personale garantiti a livello statale dal SIE. Può trasmettere tali dati a parti facenti affidamento sulla certificazione solo con il permesso esplicito del titolare.
- Il ***Servizio svizzero per l'identità elettronica (SIE)*** è responsabile della corretta attribuzione dei dati di identificazione personale all'**identificatore personale univoco (IPU)** al momento della trasmissione all'IdP riconosciuto[14]. Anche tali dati possono essere trasmessi dal SIE all'IdP solo con l'autorizzazione esplicita del titolare. I dati di identificazione personale vengono rilevati dal SIE direttamente dai registri presso la Confederazione (Infostar, ISA, SIMIC, UCC-UPI). Il livello di garanzia dell'eID definisce quali dati di identificazione personale statali vengano trasmessi all'IdP (vedi 2.6.3)[15].
- La **sicurezza dell'eID** sul campo viene determinata essenzialmente dal numero ovvero dalla qualità dei fattori di autenticazione indipendenti, verificati dall'autenticatore al momento dell'utilizzo dell'eID. Tali fattori sono: il ‚possesso di un oggetto personalizzato', la 'conoscenza di un segreto' o una ‚caratteristica intrinseca della persona', che può essere misurata a livello biometrico. L'eID deve essere resa sicura a livello tecnico in modo tale da poter essere identificata dal sistema di eID in modo univoco attraverso il suo identificatore, che l'autenticazione della persona avvenga nel rispetto dei requisiti del livello di garanzia dell'eID e che eventuali segnalazioni al display del dispositivo di supporto dell'eID e riscontri del titolare siano autentici.

---

[11] I sistemi svizzeri di eID possono essere riconosciuti a tre livelli di garanzia. I tre livelli di garanzia corrispondono a quelli definiti nel regolamento eIDAS dell'UE e anche nelle direttive per l'autenticazione digitale degli USA.

[12] Per i sistemi di eID vengono definiti profili di protezione idonei per ciascun livello di sicurezza ai sensi di ISO/IEC 15408. Ai fini del riconoscimento, vanno realizzate certificazioni nel rispetto di questi profili di protezione.

[13] Non tutti gli Stati stranieri i cui cittadini vivono in Svizzera come stranieri aventi diritto all'eID, tengono registri delle persone del livello qualitativo che è usuale per i registri svizzeri. Ma non appena i dati sono inseriti in SIMIC, questi dati, per definizione, sono considerati fonti valide per gli attributi dell'identità civile.

[14] Al momento della registrazione, l'IdP rileva il numero di un documento statale o l'identificatore personale univoco della persona e chiede con quest'informazione la trasmissione dei dati di identificazione personale relativi all'eID presso il SIE.

[15] Gli attributi che neanche nella normale vita commerciale vengono comunicati liberamente, sono riservati per livelli di garanzia dell'eID superiori; ad esempio, l'immagine della firma viene fornita solo al massimo livello di garanzia.

- Deve essere possibile utilizzare tutte le eID, indipendentemente da chi le ha emesse, presso tutte le parti facenti affidamento sulla certificazione che accettano un'identificazione o un'autenticazione al livello di garanzia dell'eID. L'**interoperabilità** è un presupposto importante affinché un'eID sia accettata nelle operazioni digitali. Ciò è possibile definendo protocolli, formati di messaggistica e obblighi di collaborazione tra gli IdP. L'impiego e l'uso di un'eID riconosciuta devono essere ovunque uniformi e trasparenti, sia per le parti facenti affidamento sulla certificazione che per i titolari dell'eID.

Una parte facente affidamento sulla certificazione porrà sempre l'utilizzo di un'eID in relazione alle sue esigenze operative tenendo conto di questi aspetti di sicurezza. Infatti, nella pratica, il livello di garanzia necessario per uno specifico processo operativo viene definito dalla parte facente affidamento sulla certificazione. Essa accetta solo i sistemi di eID che soddisfano i suoi requisiti in materia di identificazione ed autenticazione delle controparti. Acquisisce i servizi identitari desiderati dall'IdP o dagli IdP, che hanno stabilito sul mercato sistemi di eID idonei riconosciuti a livello statale. Grazie al requisito che prevede che i sistemi di eID riconosciuti a livello statale siano interoperabili e standardizzati, la parte facente affidamento sulla certificazione non è pressoché ostacolata nella propria scelta da elementi tecnici e il mercato può svilupparsi liberamente. Sono possibili diversi modelli operativi tra le parti facenti affidamento sulla certificazione, i titolari e gli IdP. È il mercato a deciderne il successo.

I titolari e le parti facenti affidamento sulla certificazione devono poter fare affidamento sul fatto che i sistemi di eID riconosciuti a livello statale rispettino i livelli di garanzia dichiarati. Tuttavia rispondono degli aspetti di sicurezza di cui sono responsabili:

- il titolare risponde dell'uso corretto dell'eID e non può, in particolare, cederla a terzi;
- la parte facente affidamento sulla certificazione deve garantire, rispettando i processi tecnici ed organizzativi stabiliti dall'IdP, la corretta identificazione ed autenticazione da parte del sistema di eID degli IdP quando viene utilizzata l'eID.

La figura sottostante illustra le competenze e la suddivisione della responsabilità tra Stato ed IdP. Le norme fondamentali sono definite dalla legge; i dettagli sono definiti nell'ordinanza.

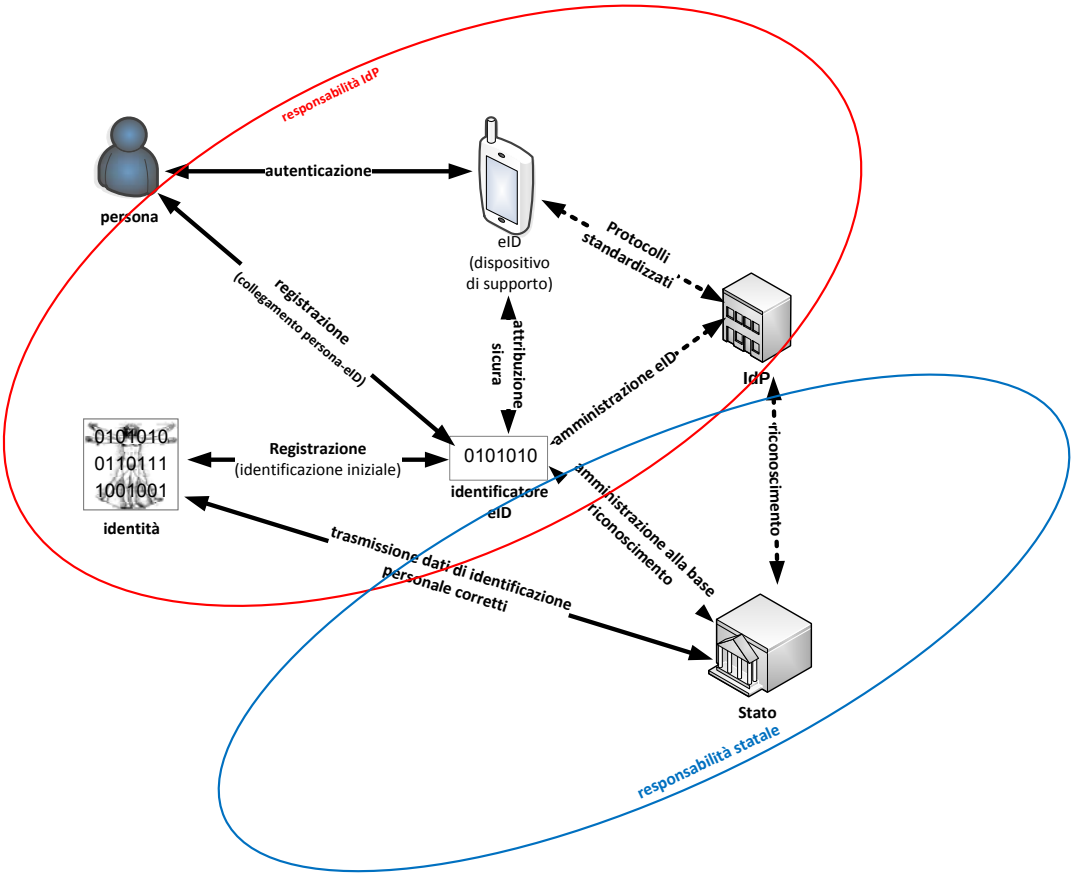



Figura 2: Suddivisione della responsabilità tra Stato ed IdP.

### 1.2.3 Facilità d'uso

Il comportamento degli utenti sui mercati digitali è strettamente legato alle innovazioni e agli sviluppi tecnologici internazionali sul mercato globale delle tecnologie dell'informazione. Il mercato è soggetto a rapidi cambiamenti e non è pressoché influenzabile da normative rigide o da imposizioni statali. Semplicemente, un sistema è facile da usare se è accettato dal mercato e viceversa. Spesso i requisiti più alti in termini di sicurezza e di protezione della sfera privata sono posti proprio nell'ambito dei sistemi rilevanti sotto il profilo della sicurezza, tra i quali rientra anche un sistema di eID. C'è però una fondamentale discrepanza tra i requisiti ideali e il comportamento concreto degli utenti all'atto pratico. Molto spesso, misure di sicurezza che sono ottimali a livello teorico, ma frequentemente anche piuttosto laboriose, causano comportamenti elusivi da parte degli utenti e quindi a falle sostanziali nella sicurezza, che potrebbero essere evitate con misure di sicurezza più semplici e più a misura d'utente.

Sono caratteristiche importanti di fini di una elevata facilità d'uso di sistemi di eID:

- Numerose **offerte online trasparenti** di organizzazioni note ed affidabili, con una forte

presenza sul mercato, presso le quali si può utilizzare l'eID. Un'eID deve poter essere utilizzata presso tutte le parti facenti affidamento sulla certificazione, indipendentemente da quale sia l'IdP che ha rilasciato l'eID. L'unica condizione è che l'eID soddisfi il livello di garanzia richiesto per l'offerta.

- **Rilascio semplice e semplice messa in funzione**, con la possibilità, nei limiti del fattibile, di effettuare online, nell'ambito di un processo senza soluzione di continuità, tutti i passaggi; i colloqui personali eventualmente richiesti devono comunque essere flessibili e in zona o, ancora meglio, devono essere sostituiti da alternative sicure come ad esempio le videoconferenze.
- **Stesso procedimento ovunque** quando si usa un'eID ad un determinato livello di garanzia. È molto importante che i titolari conoscano la propria eID e la usino volentieri e il più frequentemente possibile. Affinché ciò avvenga, l'esperienza dell'utente deve essere semplice, uniforme e comprensibile in tutti gli ambiti di utilizzo. La standardizzazione di sistemi di eID riconosciuti comprenderà quindi anche dei requisiti per l'interfaccia utente e il protocollo applicativo.
- **Utilizzo universale dell'eID**, se possibile in qualsiasi momento dal proprio dispositivo personale (PC, smartphone). Ma, al contempo, ampia autonomia dalle tecnologie e dai dispositivi del momento che hanno vita breve, in modo che l'eID possa essere trasferita senza problemi da un dispositivo di supporto al successivo.
- **Misure di sicurezza comprensibili** in modo che i titolari capiscano il senso di un passaggio del protocollo di sicurezza e non siano tentati di eluderlo.
- **Costi accettabili e periodo di validità lungo**. Un'eID deve essere valida ed utilizzabile per parecchi anni. Qualora sia prevista una partecipazione ai costi da parte del titolare per l'utilizzo dell'eID, essa dovrebbe seguire un modello pay per use, con un prezzo per tutto il servizio online. I costi totali legati ad un'eID dovrebbero essere calcolati in modo che il possesso di un'eID riconosciuta a livello statale sia percepito come vantaggioso e conveniente. Il rilascio iniziale di un'eID dovrebbe essere laddove possibile gratuito.

Il sistema di eID deve essere semplice da utilizzare non solo per i titolari ma anche, in particolare, per le parti facenti affidamento sulla certificazione che accettano un'eID e creano quindi molteplici possibilità di impiego dell'eID stessa. Sono criteri importanti nell'implementazione di un sistema di eID in un processo di accesso ad un servizio **facente affidamento sulla certificazione**:

- L'**integrazione dei protocolli del sistema di eID**, se possibile, in tutti i processi operativi di una pfac che richiedono un'identificazione ed un'autenticazione, deve essere semplice. La parte facente affidamento sulla certificazione installa sul proprio portale (definito **servizio facente affidamento sulla certificazione**) un'interfaccia integrabile in modo standard per l'utilizzo dei servizi identitari del sistema di eID (denominata **interfaccia eID)**. Questa interfaccia eID viene definita dall'IdP col quale collabora la parte facente affidamento sulla certificazione e contiene, in particolare, anche l'interfaccia utente standardizzata per l'uso online dell'eID. Lo svolgimento dell'identificazione e dell'autenticazione è poi delegato dal servizio facente affidamento sulla certificazione al sistema di eID attraverso l'interfaccia eID. Il risultato del servizio identitario viene da esso rimandato sotto forma di ticket sicuro al servizio facente affidamento sulla certificazione attraverso l'interfaccia eID. La maggior parte dei sistemi di eID oggi sul mercato funzionano secondo questo schema e consentono l'integrazione minimamente invasiva di un sistema di eID in un'applicazione di eCommerce già esistente. Attraverso la standardizzazione, ad esempio l'autenticazione nel rispetto delle specifiche FIDO [4] e la gestione degli attributi in base ai relativi standard eCH [11], sarà semplice realizzare l'integrazione ma anche il passaggio da un sistema di eID ad un altro.

- Grazie all'**interoperabilità** richiesta tra i sistemi di eID riconosciuti a livello statale, è possibile impiegare ogni eID indipendentemente dall'IdP che l'ha rilasciata, presso ogni parte facente affidamento sulla certificazione, se l'eID rispetta il livello di garanzia richiesto. A tal fine, l'IdP, presso cui la parte facente affidamento sulla certificazione acquisisce il servizio identitario, inoltra l'ordine di identificazione o autenticazione della pfac all'IdP che ha emesso l'eID specifica. Ciò è sempre possibile perché gli IdP devono predisporre interfacce interoperabili. L'IdP competente esegue l'ordine e rimanda il ticket di risposta alla parte facente affidamento sulla certificazione attraverso lo stesso canale. In questo modo non vi sono limiti a livello di accettazione o impiego di un'eID né per le parti facenti affidamento sulla certificazione né per i titolari.
- L'utilizzo di un'eID implica solo **un piccolo adeguamento dei procedimenti operativi,** in modo da non pregiudicare l'attività online. Grazie alla standardizzazione richiesta, le parti facenti affidamento sulla certificazione potranno usare i sistemi di eID senza dover adeguare in modo significativo la propria infrastruttura di TI o il proprio modello operativo. L'identificazione e l'autenticazione mediante eID deve comportare solamente semplici aggiunte al protocollo per i processi operativi già in essere. Agli IdP verrà richiesto di allineare le proprie offerte in modo da soddisfare tale esigenza del mercato. Lo Stato aiuta gli IdP a far fronte a tale richiesta con direttive per la standardizzazione e un modello tariffario semplice per la trasmissione dei dati di identificazione personale.
- Deve essere garantita la **protezione dei dati operativi**. Attraverso l'integrazione di un'eID universalmente utilizzabile non possono essere rivelati dati operativi sensibili e riservati delle parti facenti affidamento sulla certificazione, ma neppure quelli dell'IdP o del titolare. Lo Stato, ponendo idonee condizioni in materia di protezione dei dati e di vigilanza, provvede affinché i sistemi di eID riconosciuti a livello statale e gli IdP che li gestiscono soddisfino tale requisito.
- L'utilizzo di un un'eID riconosciuta a livello statale deve offrire un **vantaggio economico** ed essere in definitiva più economica della realizzazione e della gestione di una propria soluzione di autenticazione (sistema ad architettura centralizzata) o addirittura della rinuncia ad un'identificazione online sicura. I modelli operativi degli IdP, che offrono sistemi di eID riconosciuti a livello statale, devono tenere conto di questa condizione economica vincolante. D'altra parte lo Stato, attraverso un'idonea regolamentazione della responsabilità, dovrà incoraggiare le parti facenti affidamento sulla certificazione ad utilizzare sistemi di eID affidabili per i propri servizi online.

Secondo il regolamento eIDAS (art. 7) si possono solamente notificare sistemi di eID utilizzati anche da servizi pubblici per l'identificazione online. Per tale ragione, la legge sull'eID obbliga i portali online della Confederazione ad utilizzare sistemi di eID che raggiungano il livello di garanzia necessario per il servizio. Per contro, l'utilizzo di un'eID da parte di servizi pubblici andrà offerto dagli IdP ad una tariffa uniforme secondo un modello pay per use.

## 1.3 Contesto

### 1.3.1 Sviluppo socioeconomico

Con la diffusione di Internet e la grande disponibilità di dispositivi mobili altamente performanti, è sempre più semplice trasferire i processi operativi nel mondo digitale. Le giovani generazioni, che sono adeguatamente formate, hanno familiarità con le tecnologie, sono molto ben connesse e sono sempre online, favoriscono questo cambiamento di natura socioeconomica.

Secondo i dati dell'Ufficio federale di statistica [1], nel 2015 l'88% della popolazione di età

superiore ai 14 anni aveva usato almeno una volta Internet nei sei mesi precedenti, con un 99% dei soggetti di età compresa tra 14 e 19 anni e ben il 43% degli ultrasettantenni che usavano Internet almeno una volta la settimana o ogni giorno. Rispetto al resto d'Europa, la Svizzera si colloca al di sopra della media, che è pari al 76%, ma è comunque indietro rispetto a Paesi come l'Islanda (97%) e la Danimarca (93%). Il 42% degli utenti di Internet, lo usa quotidianamente da 1 a 5 ore e il 15% è già online per oltre 15 ore.

L'uso mobile di Internet è aumentato significativamente negli ultimi anni e nel 2015 interessava il 42% della popolazione totale. Si sono utilizzati allo scopo nel 95% dei casi il telefono cellulare e nel 23% dei casi il tablet. Per contro, l'uso del laptop si è quasi dimezzato dal 2010, arrivando al 42%.

Il 56% della popolazione usava nel 2015 Internet per fare acquisti online, il 49% per l'eBanking, il 48% per servizi legati ai viaggi, il 48% per compilare moduli online delle autorità e il 35% per attività politiche. Ha usato Internet per i contatti con le autorità il 79% del totale degli utenti. Le spese in eCommerce delle famiglie sono salite nell'arco di un decennio a oltre sette miliardi di franchi nel 2014.

### 1.3.2 Contesto internazionale

La Svizzera non è la sola ad introdurre un mezzo d'identificazione elettronica riconosciuto a livello statale. Questo tema è all'ordine del giorno degli Stati più sviluppati da ormai 15 anni.

Ci sono varie ragioni per studiare la situazione in altri Paesi e a livello internazionale e tenerne conto nel proprio sistema. La problematica concernente l'eID in Paesi simili alla Svizzera è generalmente la stessa; per questo si può beneficiare delle esperienze fatte altrove. Considerando la natura globale dei servizi online in Internet, è importante che un mezzo d'identificazione elettronica riconosciuto a livello statale sia realizzato a livello concettuale, tecnico e giuridico in modo da poter essere utilizzato in ambito internazionale e in particolare in Europa. Infine, in aree fortemente soggette all'influenza tecnologica, è importante fare riferimento alle tendenze prevalenti. Un singolo Paese, e a maggior ragione la Svizzera, è troppo piccolo per riuscire ad influenzare le tendenze nel campo della tecnica in misura determinante.

In vari Paesi europei e in un numero considerevole di Paesi emergenti sono già state introdotte eID statali, perlopiù integrate in smartcard contact. L'accettazione tra la popolazione e in ambito economico è ancora modesta; in particolare, nei Paesi europei che non hanno introdotto vincoli di utilizzo di un'eID, i sistemi avviati, in parte con grande dispendio, non si sono ancora affermati. Va citato come esempio la nuova carta d'identità tedesca (neuer deutscher Personalausweis - nPA), introdotta già qualche anno fa e che contiene un'eID concepita in modo da garantire un'elevata sicurezza. Si è visto però che l'eID nella nPA è poco accettata perché, benché la sicurezza sia eccellente, è complicata da utilizzare nella vita di tutti i giorni ed è molto costosa per lo Stato che la gestisce [12]. In Germania si cerca ora di rendere disponibile l'eID anche su dispositivi mobili come gli smartphone. Anche altre soluzioni di sistemi di eID, che richiedono componenti infrastrutturali aggiuntive presso gli utenti finali, faticano ad essere accettate; l'eID belga [13], ad esempio, viene perlopiù usata solo per compilare la dichiarazione dei redditi, perché i cittadini sono obbligati in tal senso, e l'eID della carta austriaca (österreichische Bürgerkarte) viene usata solo da una piccola minoranza di persone [14] (al contrario della soluzione offerta su smartphone).

Quando gli Stati hanno cominciato ad occuparsi del tema dell'eID, si è trattato innanzitutto di definire da quando, con quale tecnologia e con quali funzioni lo Stato avrebbe aggiunto l'eID alla propria carta d'identità. Le questioni sostanziali erano quale tecnologia di microchip e quale sistema di gestione del microchip usare e se il microchip dovesse comunicare con l'ambiente attraverso un sistema contact o radio (NFC). Dal punto di vista giuridico e politico, un tema

importante era quello dell'eventuale riferimento dell'eID ad un identificatore personale già in essere e di quale tipo. A livello funzionale, bisognava decidere se il microchip contenesse contemporaneamente una chiave per la firma elettronica e, successivamente, se vi fosse la funzione nel frattempo standardizzata da ICAO del passaporto (funzione passaporto elettronico) [15] con tecnologia radio.

Sulla scorta di tali riflessioni, negli ultimi 15 anni, sempre più Stati europei hanno introdotto un'eID legata alla carta d'identità come elemento centrale di un sistema nazionale di eID. La Finlandia è stata la prima ad adottare, nel 1999, una carta d'identità con l'eID, seguita dall'Estonia, dal Belgio, dalla Spagna e dal Portogallo. La Germania ha introdotto nel 2010 la propria carta d'identità elettronica (ePA / nPA) [16]. Negli ultimi anni sono stati soprattutto Paesi del Medio Oriente e dell'Asia ad adottare nuove carte d'identità statali con la funzione di eID, forse, non di rado, anche perché non si voleva restare indietro, considerati i lunghi cicli di prodotto delle carte d'identità rispetto al rapido sviluppo tecnologico (mainstream). Per contro, né gli USA né il Regno Unito hanno adottato un'eID statale, in linea con il generale scetticismo nei confronti delle carte d'identità che esiste in tali Paesi. Perlomeno negli USA, però, si usa spesso il permesso di condurre come „documento d'identità". Alcuni Stati degli USA hanno iniziato ad introdurre o a pensare di introdurre un permesso di condurre elettronico [17] [18].

Una prima situazione tipica erano le smartcard con certificati X.509 con chip contact, basate essenzialmente sulla tecnologia delle carte di firma. Ne erano un esempio la carta eID finlandese, estone e belga nonché in sostanza anche la SuisseID. Queste carte sono già state sostituite nel frattempo da una seconda generazione.

Un'ulteriore diffusa situazione è emersa dagli sforzi compiuti dall'industria europea dei microchip per definire una serie di standard con opzioni per una European Citizen Card (ECC). Queste carte contengono la funzione di passaporto elettronico secondo ICAO, nonché una funzione basata sulla funzione di passaporto elettronico per l'identificazione elettronica online. La Svezia, il Principato di Monaco, la Lettonia, la Finlandia (seconda edizione) e i Paesi Bassi hanno questo tipo di carte di identità. Nel frattempo lo standard ECC non è mai riuscito ad affermarsi completamente. Una sua espressione si è però consolidata, in particolare nell'UE, tra i documenti per gli stranieri (permessi di soggiorno per i cittadini di Paesi terzi). La ragione risiede nel fatto che l'UE può legiferare in questo ambito, a differenza di quanto vale per le carte d'identità. Anche la carta di soggiorno svizzera per i cittadini di Stati terzi segue questo standard.

Questa fase nello sviluppo dell'eID ha raggiunto una sorta di culmine con il documento personale elettronico (elektronischer Personalausweis ePA) introdotto dalla Germania nel 2010. Esso contiene essenzialmente le componenti sopra menzionate ma è stato migliorato in alcuni punti, in particolare aggiungendo vari procedimenti complessi a livello tecnico per rafforzare la protezione della personalità. I prestatori di servizi (service provider) devono così farsi registrare per acquisire determinati attributi dallo Stato e anche autenticarsi rispetto all'eID al momento dell'utilizzo. Una funzione di pseudonimizzazione ('restricted identity') assicura che il documento di legittimazione si presenti ad ogni prestatore di servizi con un identificatore diverso in modo che sia più complicato creare dei profili utente. Con una strategia trasversale, la Germania ha fatto in modo che i titoli di soggiorno per gli stranieri fossero dotati di funzioni online di documentazione dell'identità (Online-Ausweisfunktionen) compatibili. Negli ultimi anni, l'ePA tedesca è davvero diventata il riferimento a livello mondiale per la nuova eID statale. Nel frattempo in Germania la metà della popolazione si è provvista dell'ePA e non è ancora chiaro se l'eID sulla nPA verrà prima o poi ampiamente utilizzata.

Un fattore essenziale nel determinare se un'eID venga usata dal titolare o meno è la disponibilità di un'offerta ampia di servizi per i quali l'eID possa essere utilizzata. Si è visto che nei grandi agglomerati urbani tedeschi, attivi nel rendere disponibili offerte online, il tasso di attivazione dell'eID dell'ePA è notevolmente maggiore. Viceversa, nelle zone in cui l'offerta online

scarseggia, prevale lo scetticismo nei confronti dell'eID del documento di legittimazione tedesco.

Il sistema di eID più sviluppato è quello estone, in uso da oltre dieci anni e che oggi include la maggior parte dei servizi, dall'e-banking al vote électronique per tutta la popolazione online. Ha avuto molto successo anche il modello svedese con il BankID, che si fonda sulla collaborazione tra le banche e lo Stato e che è molto simile come concetto al modello qui proposto per la Svizzera. I criteri che sono risultati decisivi per il successo dell'eID in questi Paesi sono [19]

- l'accettazione generale dell'eID presso tutti i servizi pubblici online,
- la collaborazione tra il settore pubblico e quello privato,
- un modello operativo funzionante per tutti i soggetti coinvolti,
- un'esperienza di utilizzo uniforme in tutte le applicazioni di utilizzo dell'eID,
- un identificatore personale univoco disponibile in linea generale e
- regole vincolanti alla base della fiducia e standard unitari per l'infrastruttura.

### 1.3.3 Sviluppi attuali

L'ottimizzazione sporadica della sicurezza di singole componenti nello svolgimento di processi operativi elettronici non è in grado di aumentare la sicurezza complessiva; questo vale anche per l'eID [20]. Anche SuisseID dimostra come la sicurezza da sola non sia efficace come criterio determinante di progettazione. Malgrado vi fossero grandi aspettative, finora si è infatti affermata in Svizzera solo come prodotto di nicchia. Tra i punti deboli ovvero le ragioni della limitata diffusione di SuisseID si citano in particolare l'installazione poco agevole, il periodo di validità dei certificati limitato a tre anni, la mancanza di applicazioni e interoperabilità internazionale nonché il dispendio e il costo elevato che procurarsela comporta [21] [22]. Per contro, nel caso ad esempio della più recente Mobile ID, non vi sono costi diretti per l'utente (essi vengono addebitati alle parti facenti affidamento sulla certificazione con un contratto di utilizzazione) e il rilascio e l'uso sono più semplici per l'utente. Anche al di fuori della Svizzera quasi tutti i sistemi di eID che, indipendentemente dai casi operativi concreti, danno la priorità solo alla sicurezza in modo unilaterale e trascurano la semplicità di utilizzo, hanno problemi ad essere accettati [23] [24] [25].

La soluzione nell'ambito dell'eID pianificata per la Svizzera deve invece soddisfare nel modo migliore e più equilibrato possibile i principali criteri per l'accettazione da parte del mercato. A tale scopo, si sono già chiariti molti aspetti a vari livelli nel quadro dei preparativi al presente piano di eID. Si sono consultati enti pubblici e privati che rilasciano eID, potenziali parti facenti affidamento sulla certificazione e trend setter per i futuri sviluppi tecnologici nel campo della gestione elettronica dell'identità. Nell'attuale piano di eID si sono apportate ulteriori semplificazioni e miglioramenti per i sistemi di eID riconosciuti, tutti intesi ad aumentare ulteriormente l'accettazione da parte del mercato. I criteri determinanti per un'eID accettata e utilizzabile sono la fiducia di fondo nella sicurezza giuridica, tecnica ed organizzativa, la facilità d'uso, l'economicità, l'applicazione standardizzata e i molteplici possibili impieghi [19] [26]. Le funzioni maggiormente utilizzate dell'eID sono la registrazione presso una parte facente affidamento sulla certificazione e successivamente la registrazione presso il servizio facente affidamento sulla certificazione, una volta che si è già registrati come utenti. Tali procedimenti devono essere quindi particolarmente semplici da applicare ed aggiornati dal punto di vista tecnologico [27].

Per questo negli ultimi anni le riflessioni sulla promozione a livello statale dell'eID non si sono più chieste quale eID integrare nella carta d'identità ma hanno preso una nuova direzione. Le ragioni principali potrebbero essere che il ciclo del prodotto di una carta d'identità statale è troppo lungo rispetto alla rapidità dello sviluppo del mondo elettronico e che le eID sulle carte necessitano sempre anche di un'infrastruttura costosa e affidabile in termini di apparecchi di lettura, la cui acquisizione iniziale non è molto dispendiosa ma il cui utilizzo e la cui manutenzione sono perlopiù complicati e costosi. Inoltre, non su tutte le attuali piattaforme, e in particolare sui dispositivi mobili che oggi predominano, sono disponibili i relativi apparecchi di lettura o collegamenti.

Parallelamente al progetto statunitense dello sviluppo congiunto di un Identity Ecosystem [28] in molti Paesi si è iniziato a considerare più approfonditamente come dovesse configurarsi una buona architettura per l'intero ecosistema nazionale ed internazionale dell'eID, che coinvolgesse tutti gli attori e anche quale contributo a tale ambiente eID potesse dare lo Stato. I singoli Paesi sono arrivati a conclusioni diverse.

Negli USA, il ruolo dello Stato è limitato a quello di organizzatore e promotore dell'ambiente eID: esso non mette direttamente a disposizione servizi ma influenza fortemente il mercato come acquirente di eID per i propri collaboratori e come gestore di servizi che fanno affidamento sulla certificazione nel quadro di offerte di eGovernment. In Svezia, in Norvegia e in Danimarca le banche sono state tra i principali offerenti di eID per tutti i settori e da parecchio tempo offrono tali prodotti per i propri servizi. I requisiti minimi statali garantiscono una specifica qualità e l'interoperabilità.

Il già citato regolamento eIDAS dell'UE ha dovuto accogliere alla fine tale sviluppo ed accettare come equivalenti per il reciproco riconoscimento, oltre alle eID emesse dallo Stato, anche i sistemi di eID riconosciuti a livello statale. Questa concezione trova espressione nell'articolo 7 in questi termini:

**Ammissibilità alla notifica dei regimi di identificazione elettronica**
Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:

a) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica sono rilasciati:
- i) dallo Stato membro notificante;
- ii) su incarico dello Stato membro notificante; o
- iii) a titolo indipendente dallo Stato membro notificante e sono riconosciuti da tale Stato membro.

Nello stesso articolo si sanciscono poi la responsabilità di chi ha rilasciato un'eID e i doveri ai quali lo Stato non può mai sottrarsi, neppure nella situazione delineata all'articolo 7 lettera a) iii).

### 1.3.4 Conseguenze per la Svizzera

Già oggi operano nell'ambiente svizzero dell'eID numerosi gestori dell'identità elettronica che offrono un'eID, come ad esempio SuisseID, Mobile ID, Google ID, AppleID, Open ID ecc. Esistono anche soluzioni interne all'amministrazione, con una smartcard personale, come nel caso dell'autenticazione presso il portale SSO del DFGP. Nel quadro del progetto IAM della Confederazione andrà addirittura realizzata una soluzione unitaria per l'intera amministrazione confederale. Inoltre, le aziende, come ad esempio le banche o le assicurazioni, emettono per i propri clienti mezzi di identificazione che vengono utilizzati esclusivamente per le loro attività. Tali mezzi di identificazione, limitati ad un'applicazione, vengono definiti „soluzioni ad

architettura centralizzata“, al contrario delle soluzioni sopra citate, che possono essere usate in contatti multipli („soluzioni federalizzate e/o interoperabili“). Tutti questi sistemi hanno una diversa diffusione, facilità d’uso, funzionalità e sicurezza e nella maggior parte dei casi non sono tra loro compatibili. A livello internazionale, la tendenza va invece chiaramente nella direzione di un’autenticazione ed identificazione incentrate sul cliente, sicure ed interoperabili, come base per tutti i servizi fiduciari su di esse basati.

Se si confronta il piano che qui viene presentato e che trova attuazione nel disegno di legge per il riconoscimento a livello statale dei mezzi d’identificazione elettronica con gli sviluppi, le esperienze e le attuali riflessioni in ambito nazionale ed internazionale, la situazione è la seguente:

- Col suo piano per un’eID riconosciuta a livello statale, la Svizzera è in linea con le tendenze e ha chiaramente tratto insegnamenti dalle esperienze degli altri Paesi negli ultimi 15 anni.
- Il piano svizzero è conforme in linea di massima all’UE ovvero a eIDAS.
- Il piano svizzero è molto flessibile e dovrebbe sostenere anche significativi sviluppi tecnici ed economici.

Il piano presentato è anche compatibile col modello di riferimento sviluppato in Svizzera per un ambiente eID [29].

### 1.3.5 Compatibilità UE

Se l’utilizzabilità a livello internazionale è importante anche per il documento tradizionale con dati visibili, a maggior ragione ciò vale per l’eID che, in qualità di documento online, viene usata in Internet, per sua natura privo di confini. Per l’UE, che si è impegnata a realizzare un mercato unico europeo senza barriere, si tratta di un’aspirazione particolarmente importante.

Il 23 luglio 2014, l’UE ha quindi emanato il regolamento (UE) n. 910/2014 [2] 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 (regolamento eIDAS). Oltre alla regolamentazione e alla certificazione dei prestatori della firma elettronica e di altri servizi fiduciari, il regolamento contiene il tema nuovo della notifica e del relativo riconoscimento reciproco di sistemi nazionali per l’identificazione elettronica. Tutti gli Stati membri sono sempre tenuti, quando richiedono un’eID per l’accesso ai servizi del settore pubblico, anche ad ammettere ogni eID estera proveniente dal sistema notificato (articolo 6). Tale obbligo vale persino per uno Stato membro che non abbia un proprio sistema notificato di eID.

La programmata legge sull’eID e i sistemi di eID riconosciuti a livello statale della Svizzera devono essere compatibili con i sistemi di eID dell’UE (cfr. anche la Panoramica).

## 1.4 Strategie e mandato

### 1.4.1 Strategia del Consiglio federale per una Svizzera digitale

La strategia „Svizzera digitale“ del Consiglio federale dell’aprile 2016 [30] include l’obiettivo: „Un sistema sicuro e semplice per la gestione dell’identità è disponibile in tutta la Svizzera“. Si tratta di approntare, sulla base di standard internazionali, una soluzione digitale sicura, senza barriere

e semplice per attestare le identità applicabile in tutta la Svizzera.

### 1.4.2 Strategia di eGovernment Svizzera

La „**Strategia di eGovernment Svizzera**“ [31] [32] si prefigge di far sì che sia l'economia che la popolazione possano svolgere per via elettronica importanti operazioni con le autorità pubbliche. Il progetto prioritario „B2.15 Identità elettronica riconosciuta a livello nazionale e nell'area europea“ [33] è uno dei pilastri nell'attuazione della strategia del Consiglio federale, che con questo piano per l'eID si è chiamati a predisporre.

### 1.4.3 Mandato della Confederazione per mezzi di identificazione riconosciuti a livello statale

Sulla base di un documento interlocutorio del DFGP del 23 dicembre 2015, il 13 gennaio 2016 il Consiglio federale, tra le altre cose, ha fissato i seguenti aspetti essenziali per l'ulteriore sviluppo di un'eID riconosciuta a livello statale e ha incaricato il DFGP di sottoporgli entro la fine del 2016 un avamprogetto da porre in consultazione:

- La Confederazione creerà un quadro giuridico e di standardizzazione nonché la struttura organizzativa per il riconoscimento a livello statale dei sistemi di eID e dei gestori dell'identità elettronica che rilasciano le eID. Ciò andrà configurato in modo che sia successivamente possibile il riconoscimento reciproco tra la Svizzera e l'UE dei sistemi di eID riconosciuti a livello statale.
- I sistemi di eID riconoscibili a livello statale devono essere predisposti da gestori privati e pubblici dell'identità elettronica (IdP). La Confederazione rinuncia a rilasciare una propria eID statale.
- I sistemi di eID idonei devono poter essere riconosciuti a livello statale ad uno di tre livelli di sicurezza.
- I sistemi di eID riconosciuti a livello statale devono essere accessibili in linea di principio a tutti i cittadini svizzeri nonché agli stranieri in Svizzera.
- I dati di identificazione personale tenuti nei registri presso la Confederazione vanno trasmessi agli IdP attraverso un'interfaccia elettronica per i sistemi di eID riconosciuti a livello statale.
- Per l'identificazione di una persona va creato un identificatore personale univoco (IPU).
- Il NAVS13 sarà utilizzato come attributo d'identità, impedendo tecnicamente la trasmissione a terzi non autorizzati ad un uso sistematico.
- Un'ulteriore semplificazione dei procedimenti in relazione alla trasmissione di dati di identificazione personale andrà verificata nel quadro di ulteriori lavori inerenti il piano.
- Come misura di protezione dell'investimento, tutti gli uffici federali dovranno essere sostanzialmente tenuti ad utilizzare i sistemi di eID riconosciuti a livello statale nelle loro applicazioni di eGovernment che richiedono un'autenticazione dell'utente, al giusto livello di garanzia.

## 1.5 Limiti

Questo piano non si occupa di altri servizi fiduciari come l'amministrazione di ruoli e diritti in

ambito digitale, la firma digitale o il sigillo elettronico o prove di funzionamento per le transazioni online da effettuare. I sistemi di eID sono esclusivamente strumentali alla gestione dell'identità elettronica (eIDM) e costituiscono quindi solo una componente fondamentale di sistemi completi di gestione dell'identità e dell'accesso. A differenza delle gestioni dell'accesso, che devono essere concepite individualmente da tutte le parti facenti affidamento sulla certificazione in linea con i servizi che offrono, l'eIDM può essere realizzata in modo trasversale alle diverse istituzioni e quindi in modo molto efficiente.

# 2 Piano dell'eID riconosciuta a livello statale

## 2.1 Introduzione

I diretti beneficiari di sistemi di eID riconosciuti a livello statale che siano di semplice utilizzo ed utilizzabili in una varietà di situazioni, sono le parti facenti affidamento sulla certificazione dell'economia privata e delle autorità pubbliche[34]. Anche i titolari però beneficiano di un'offerta online ampia grazie all'eID.

L'approccio adottato in questo piano, finalizzato all'utilizzo dell'ambiente eID con una soluzione idonea per l'eID, si distingue dai sistemi già realizzati a livello statale in altri Paesi europei (cfr. 1.3.2). Visto che sinora i sistemi di eID hanno avuto, salvo poche eccezioni, problemi di accettazione, un nuovo approccio attuativo non solo appare opportuno ma anche dovuto. La capacità innovatrice del mercato nel campo dei servizi elettronici in generale e dei mezzi d'identificazione elettronica in special modo, non deve essere limitata da soluzioni statali rigide. In particolare, la messa a disposizione di sistemi di eID riconosciuti a livello statale non deve avvenire sotto forma di monopolio dello Stato. I modelli operativi devono essere sviluppati e validati sul mercato, in modo da ottenerne l'accettazione. Chi rilascia e gestisce sistemi di eID presta servizi fiduciari, necessari ad un mercato elettronico funzionante.

I sistemi di eID di successo [35] …

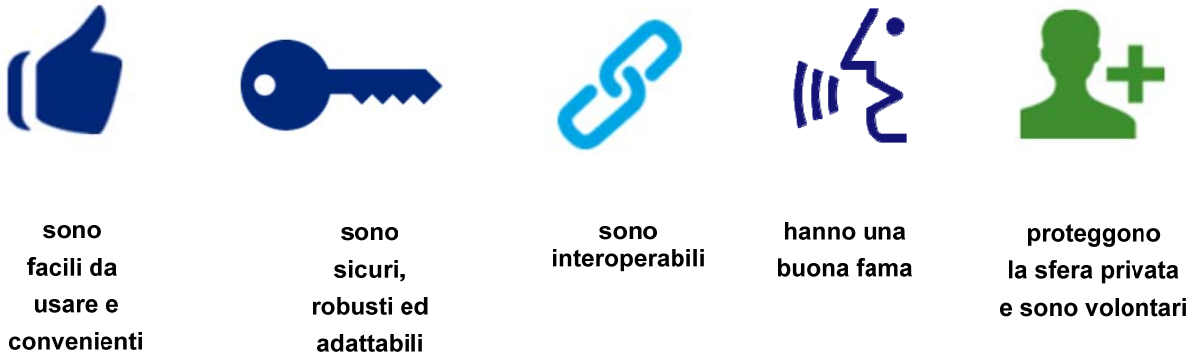



Figura 3: Principi guida dei sistemi di eID di successo

In questo piano gli IdP si assoggettano volontariamente con i propri sistemi di eID alle direttive ai fini del riconoscimento a livello statale e ricevono per questo il sigillo di qualità statale che attesta il riconoscimento e l'affidabilità nonché, direttamente dallo Stato, i dati di identificazione personale dei titolari delle loro eID riconosciute a livello statale.

## 2.2 Finalità

Il contributo principale dello Stato all'ambiente eID svizzero è la messa a disposizione di un quadro giuridico e di standardizzazione („Trust Framework") per i sistemi di eID riconosciuti a livello statale. Tale quadro fornisce la base necessaria per una crescente fiducia nei servizi online e regolamenta il mercato in modo da promuovere l'interoperabilità, il riconoscimento internazionale, la facilità d'uso, l'ampia applicabilità, la sicurezza e la protezione della sfera privata.

Un'eID riconosciuta a livello statale può essere rilasciata

- a tutti gli svizzeri in possesso di un documento svizzero valido in base alla legge svizzera sui documenti d'identità (LDI) al momento del rilascio e
- agli stranieri in possesso di una carta di soggiorno valida in base alla legge federale sugli stranieri (LStr) al momento del rilascio.

Le diverse esigenze in materia di sicurezza dell'identificazione e dell'autenticazione dei titolari da parte della pfac sono soddisfatte attraverso i diversi livelli di garanzia dei sistemi di eID riconosciuti a livello statale. I livelli di garanzia sono definiti a tre livelli, corrispondenti alla classificazione dell'eID europea e anche americana.

Le eID riconosciute a livello statale, indipendentemente dall'IdP che le ha rilasciate, devono poter essere utilizzate nel modo più versatile possibile presso le parti facenti affidamento sulla certificazione. Il protocollo di utilizzo sarà quindi integrabile ovunque in modo uniforme e semplice nei processi operativi della pfac. Basterà che la parte facente affidamento sulla certificazione stipuli un accordo di utilizzazione con un IdP per un sistema di eID. L'interoperabilità per le eID estranee al sistema, utilizzate da una parte facente affidamento sulla certificazione, viene realizzata dagli IdP riconosciuti, che collegano reciprocamente i propri sistemi in modo interoperabile. Le eID riconosciute a livello statale ad un sufficiente livello di garanzia dovranno poter essere usate senza ulteriori limitazioni, in particolare da parte delle autorità, per la registrazione o l'accesso ad un servizio facente affidamento sulla certificazione.

Inoltre, lo Stato gestisce un servizio attributi per la trasmissione di dati di identificazione personale registrati a livello statale agli IdP, che gestiscono i sistemi di eID riconosciuti a livello statale. I titolari depositano i propri dati statali di identificazione personale presso l'IdP, che rilascia loro un'eID. Dopo la registrazione, possono incaricare l'IdP, presso il quale sono depositati i loro dati di identificazione personale, di fornire gli attributi della loro identità civile anche a parti facenti affidamento sulla certificazione di loro scelta.

## 2.3 Principi

I principi fondamentali della soluzione proposta sono sintetizzati nei punti seguenti:

- Molti servizi fiduciari fanno parte della vita economica e sono principalmente erogati da attori del mercato privati e di diritto pubblico e non da parte dello Stato. Ciò vale di conseguenza anche per la predisposizione di sistemi di eID.
- Lo Stato funge però da regolatore affinché il mercato sia affidabile, riconoscendo a livello statale i sistemi di eID idonei e gli IdP erogatori. Gli IdP sono vincolati a corrispondenti standard e disposizioni in materia di sicurezza, di protezione dei dati e di interoperabilità. Lo Stato rinuncia esplicitamente a rilasciare una propria eID statale (sulla CID), che farebbe concorrenza alle soluzioni innovative proposte dal mercato.
- Un'eID, almeno nella visione di oggi, non è un passaporto e la si procura quindi solo se l'eID viene usata per attività online di carattere economico, sociale o amministrativo. I sistemi di eID devono quindi affermarsi sui mercati digitali nel quadro dell'interazione tra domanda e offerta. Ciò significa che i modelli operativi degli IdP vanno sviluppati e validati nella realtà dei mercati elettronici, in modo da essere accettati.
- Il mercato dei gestori dell'identità elettronica rende disponibili eID di qualità diversa in relazione alla sicurezza e alla semplicità d'utilizzo (soglia d'ingresso bassa, uso semplice, ampia applicabilità). Lo Stato riconosce i sistemi di eID a tre livelli di garanzia (basso o „argento", significativo, corrispondente a „oro", elevato, ovvero „platino"), che sono definiti equivalenti ai livelli di garanzia dei sistemi di eID dell'UE[2].

- In linea di principio, tutti gli aventi diritto in Svizzera possono acquisire gratuitamente un'eID riconosciuta a livello statale da un IdP riconosciuto a livello statale di propria scelta. Scelgono l'eID secondo le proprie esigenze in relazione al livello di garanzia e alla semplicità d'uso. A tal fine devono completare il processo di registrazione previsto e far trasmettere per il riconoscimento statale, in particolare, i propri dati di identificazione personale dal Servizio svizzero per l'identità elettronica (SIE) all'IdP.
- L'IdP che effettua il rilascio è l'interlocutore diretto per tutte le questioni concernenti l'eID, sia nei confronti dei titolari che delle parti facenti affidamento sulla certificazione, con le quali ha un accordo di utilizzazione. L'IdP rende disponibili idonei servizi di Support ed Exception Handling. Risponde di malfunzionamenti secondo gli obblighi di legge che valgono per il livello di garanzia del suo sistema di eID. L'IdP è anche responsabile del fatto che gli attributi identitari siano assegnati in modo aggiornato e corretto e che siano forniti a parti facenti affidamento sulla certificazione che ne hanno diritto solo col consenso del titolare.
- L'integrità dei dati di identificazione personale utilizzati con un'eID riconosciuta a livello statale è importante. La Confederazione, col Sistema d'informazione per documenti d'identità (ISA), col Sistema d'informazione centrale sulla migrazione (SIMIC) e il registro dello stato civile (Infostar), dispone già di registri gestiti dallo Stato di dati di identificazione personale, che si basano su un'identificazione sovrana delle persone. Lo Stato fornisce agli IdP, per i sistemi di eID riconosciuti, i dati di identificazione personale iscritti in tali registri in occasione dell'ultima identificazione statale ufficiale, in forma crittografata e sicura. La quantità degli attributi trasmessi è definita in modo diverso per i tre livelli di garanzia (vedi 2.6.3). Con ogni trasmissione viene fornita anche la data dell'identificazione di base. Lo Stato risponde degli errori in tali dati.
- Lo Stato definisce, come parte dell'identità civile che amministra, un identificatore personale univoco (IPU), che viene fornito per ogni livello di garanzia dell'eID con i dati di identificazione personale trasmessi all'IdP.
- I gestori di sistemi di eID sono liberi di decidere se vogliono ottenere un riconoscimento statale dei propri sistemi di eID e trarne quindi un vantaggio commerciale. Non è obbligatorio far riconoscere a livello statale un sistema di eID. Lo Stato definisce le normative in modo che i sistemi di eID riconosciuti possano essere riconosciuti a livello europeo, possano cioè essere notificati in conformità con il livello di garanzia raggiunto.
- I sistemi di eID riconosciuti a livello statale devono essere interoperabili. L'interoperabilità viene realizzata da un lato attraverso semplici interfacce elettroniche standardizzate (interfaccia eID) presso i servizi che fanno affidamento sulla certificazione della pfac e dall'altro con l'interoperabilità dei sistemi di eID tra loro. Gli IdP di sistemi di eID riconosciuti devono inoltre mettere a disposizione di tutti gli altri IdP con sistemi di eID riconosciuti delle interfacce standardizzate per l'utilizzo interoperabile delle loro eID. Le eID interoperabili, che possono essere usate presso tutte le parti facenti affidamento sulla certificazione in conformità con il livello di garanzia richiesto, promuovono la rapida diffusione di sistemi di eID riconosciuti nell'ambiente eID.
- Le parti facenti affidamento sulla certificazione, che utilizzano sistemi di eID riconosciuti a livello statale presenti sul mercato per l'identificazione e l'autenticazione dei loro clienti in linea con i requisiti (affidabilità, sicurezza, regolamentazioni, caso operativo, responsabilità), possono fare affidamento sul rispetto di standard interoperabili da parte di tutti i gestori di sistemi di eID. Rispondono però dell'utilizzo conforme dell'eID da parte del loro servizio facente affidamento sulla certificazione nell'identificazione o nell'autenticazione dei titolari.

- Gli aventi diritto decidono liberamente se vogliono acquisire un'eID riconosciuta a livello statale. Per il riconoscimento statale della propria eID devono però dare all'IdP che la rilascia il permesso esplicito di acquisire i dati di identificazione personale corrispondenti al livello di garanzia presso il servizio attributi statale. In qualità di titolari possono decidere di volta in volta se e quali attributi dell'identità civile debbano essere trasmessi dall'IdP alla pfac.
- I titolari sono tenuti ad utilizzare la propria eID con cura e in modo sicuro nell'ambito della propria sfera d'azione. Rispondono dei danni derivanti da un suo uso improprio. Anche le parti facenti affidamento sulla certificazione rispondono dei danni che derivano dall'utilizzo erroneo della eID all'identificazione o autenticazione dei loro clienti.

La Confederazione rende disponibile l'infrastruttura necessaria ai fini dell'attuazione delle disposizioni di legge e del servizio di trasmissione di dati di identificazione personale (vedi il cap. 3). Gestisce allo scopo un'unità amministrativa, denominata **Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)**, che svolge il processo di riconoscimento per gli IdP e i sistemi di eID riconosciuti a livello statale e che vigila sugli IdP riconosciuti. Gestisce inoltre un'unità amministrativa denominata **Servizio svizzero per l'identità elettronica (SIE)** che opera un sistema d'informazione che può richiedere dati di identificazione personale presso i relativi registri statali della Confederazione e che li trasmette agli IdP riconosciuti a livello statale, che gestiscono sistemi di eID, col consenso dei titolari.

## 2.4 Architettura e processi

Tutto comincia con l'avvio di un rapporto operativo tra un titolare e una parte facente affidamento sulla certificazione. Nella gestione dell'identità elettronica (eIDM) vi sono altri due ruoli, oltre a quello del titolare e a quello della parte facente affidamento sulla certificazione, che intende identificare ed autenticare il titolare: quello del gestore dell'identità elettronica (IdP), che gestisce il sistema di eID, e quello dello Stato regolatore. Quest'ultimo definisce le regole della cooperazione tra i soggetti coinvolti e i requisiti dei sistemi di eID riconosciuti a livello statale, in modo che si crei una base di fiducia certa, ed è anche l'amministratore dell'identità civile di tutte le persone nell'ambiente eID. Nell'ambiente eID le parti facenti affidamento sulla certificazione (pfac) delegano i processi dell'identificazione e dell'autenticazione elettronica dei titolari di un'eID all'IdP. Ogni pfac gestisce allo scopo un'applicazione informatica come servizio che fa affidamento sulla certificazione, collegato attraverso un'interfaccia eID ad un sistema di eID di un IdP. Dopo l'esecuzione dell'ordine per un servizio identitario, il sistema di eID restituisce al servizio facente affidamento sulla certificazione, che ha conferito l'ordine, il risultato dell'identificazione o dell'autenticazione.

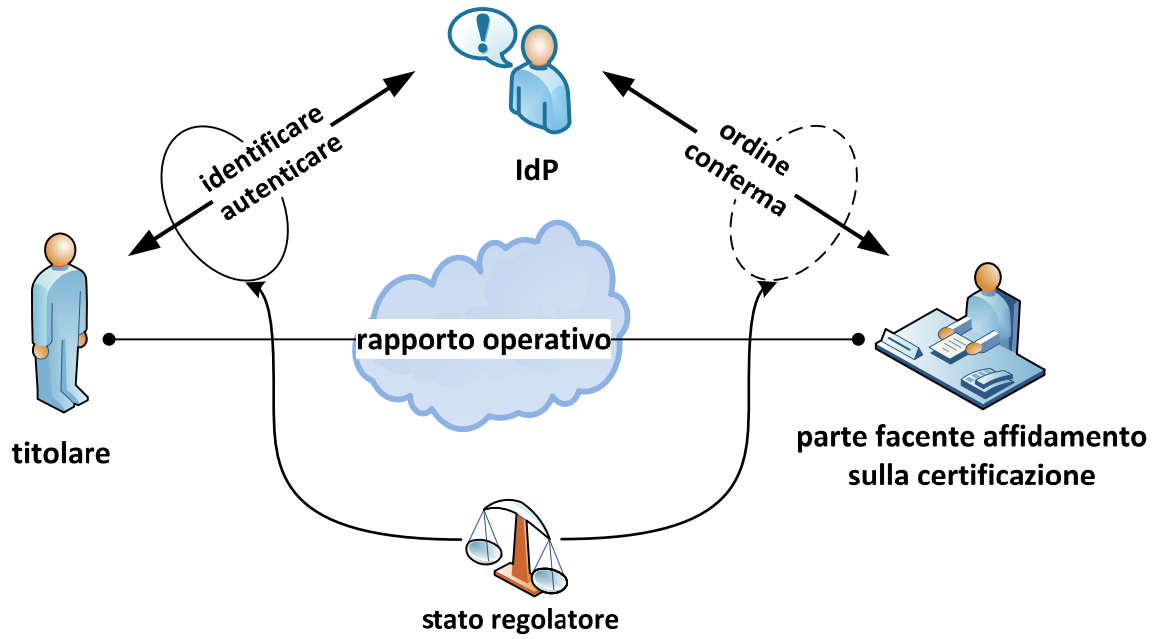



Figura 4: I ruoli nella gestione dell'identità elettronica

### 2.4.1 Sistemi di eIDM

I sistemi digitali dell'eIDM dei diversi ruoli sono:

- L'autenticatore perlopiù sotto forma di dispositivo personale[16] del titolare con l'applicazione eID integrata in modo sicuro ed affidabile. Questa applicazione ha un identificatore, una funzione di autenticazione con i dati di riferimento per il riconoscimento del titolare, un segreto collegato in modo stabile con l'identificatore ed un'interfaccia di comunicazione sicura con il sistema centrale dell'IdP. Si può anche optare nell'utilizzare l'eID per la visualizzazione del dispositivo di supporto in sicurezza, sotto il controllo dell'applicazione eID installata.
- Il sistema di amministrazione e servizi delle parti facenti affidamento sulla certificazione per le operazioni online come servizio facente affidamento sulla certificazione, con un'interfaccia integrata e standardizzata col sistema di eID. Questa interfaccia eID è costituita da processi e protocolli standardizzati, che trovano applicazione al momento della registrazione o dell'accesso di un titolare presso il servizio facente affidamento sulla certificazione e che generano l'ordine per il servizio identitario. Riceve dal titolare e dal servizio facente affidamento sulla certificazione i dati necessari per l'ordine e li inoltra al sistema di eID dell'IdP. Riceve a sua volta il ticket di risposta col risultato dell'ordine eseguito ed inoltra il risultato al servizio facente affidamento sulla certificazione.
- Le componenti del sistema di eID dell'IdP amministrano tutti gli attributi identitari[17] dei titolari rilevati, ricevono gli ordini dei servizi facenti affidamento sulla certificazione attraverso le interfacce eID, eseguono tramite le eID sul campo le identificazioni ed

[16] L'autenticatore è un termine dal significato ampio (in inglese authenticator o, in passato, token), che non si riferisce solo ai dispositivi elettronici come supporto. La cosa importante è che, sotto il controllo personale del titolare, possa provarne l'identità.

[17] L'insieme degli attributi identitari di un titolare che l'IdP può ricevere da fonti diverse, viene definito identità parziale (vedi in merito i chiarimenti nell'allegato).

autenticazioni sicure dei titolari ed emettono i ticket di risposta per i servizi facenti affidamento sulla certificazione. Ogni IdP ha un'interfaccia sicura con il servizio attributi statale ed un service per la realizzazione dell'interoperabilità con altri IdP riconosciuti. Gestisce inoltre un elenco consultabile online delle eID bloccate provvisoriamente o disattivate in via permanente.

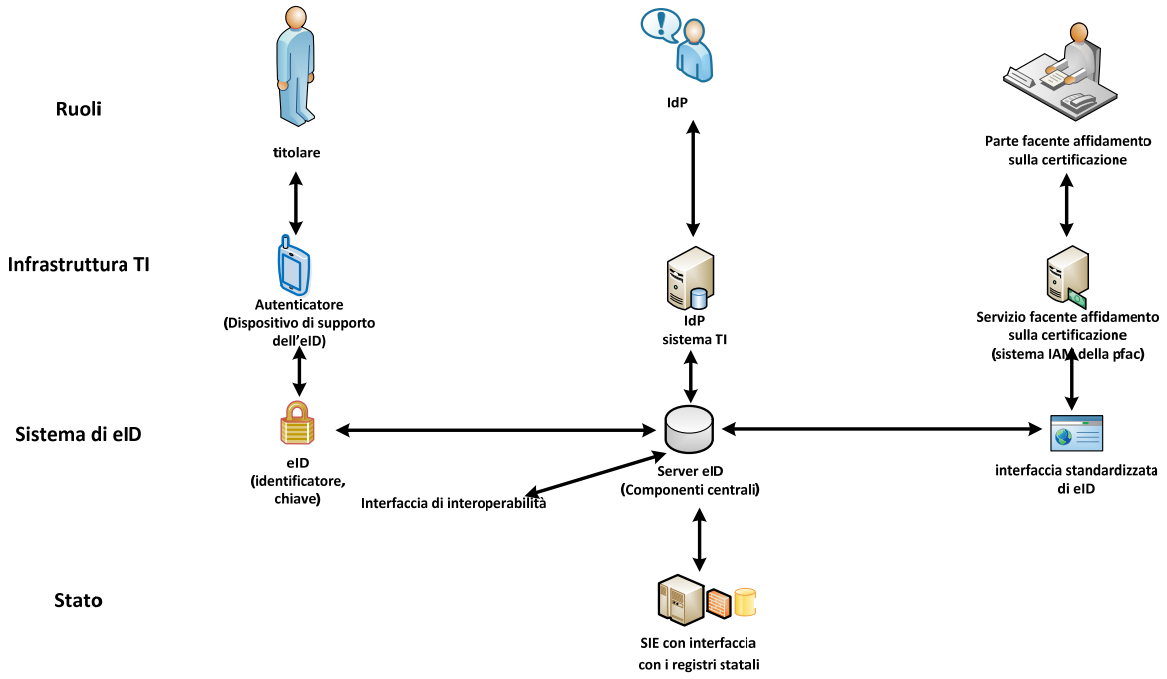



Figura 5: Livelli di sistema e componenti eIDM ad essi assegnate

### 2.4.2 Autenticatore ed eID

L'autenticatore, che garantisce il collegamento tra la persona fisica e la sua identità registrata nel sistema di eID, rappresenta un elemento centrale di un sistema di eID. L'autenticatore può assumere diverse forme. Può essere, ad esempio, una componente di sicurezza (chip) inserita in una carta di plastica, un'applicazione di una carta SIM, una chiave USB oppure un dispositivo speciale ma anche varianti di software come certificati collegati ad un meccanismo di attivazione o altro ancora. In linea di principio anche la combinazione di UserID e password può essere considerata una forma astratta di autenticatore. La cosa importante è che l'autenticatore sia collegato in modo univoco ad una persona nel quadro di un processo di registrazione, che sia rappresentato da un identificatore integrato e che possa connettersi in modo sicuro con il server delle eID. L'identificatore può essere definito in modo diverso in relazione al settore, alla pfac o al lasso di tempo ma deve sempre essere attribuibile in modo univoco ad un autenticatore nel contesto del sistema di eID.

Al momento della registrazione, l'autenticatore viene collegato da un lato ad una persona e dall'altro (dal server) ai suoi dati identitari e quindi diventa un'eID. Solo con questa eID, così predisposta, la persona registrata può autenticarsi ed identificarsi a livello digitale.

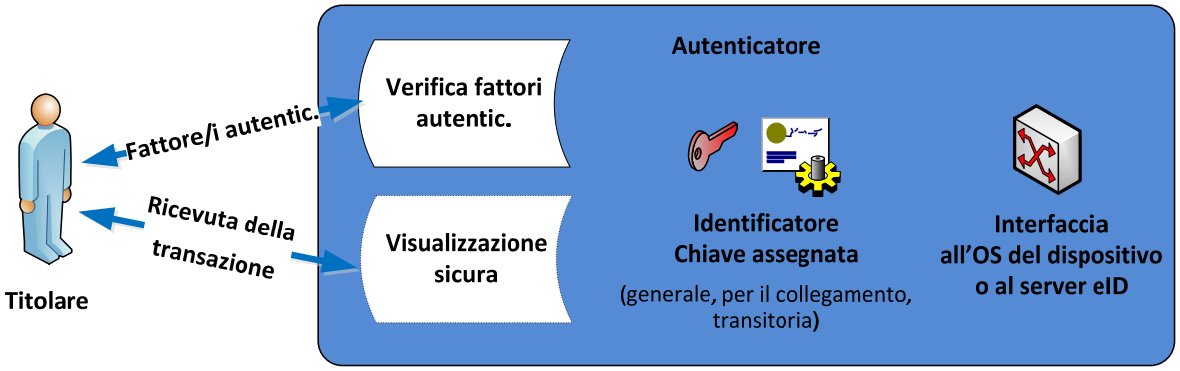



Figura 6: Un'eID è un autenticatore registrato per una persona, con i dati identitari assegnati a tale persona.

## 2.5 Cicli di vita nel sistema di eID

Ogni sistema di eID da un lato compirà come sistema un ciclo di vita e dall'altro amministrerà il ciclo di vita delle singole eID e quello dell'interfaccia eID presso le parti facenti affidamento sulla certificazione. A tale scopo devono essere implementati per ciascuno dei tre cicli di vita dei procedimenti organizzativi e dei processi TI. A titolo illustrativo sono descritti i cicli e i processi di un sistema preso come modello. Nella pratica vi sarà sicuramente una grande varietà di cicli di vita e processi, limitata solo da requisiti normativi cogenti.

La descrizione del sistema modello presuppone che l'eID sia un'applicazione per smartphone (autenticatore) che può essere installata in un'area sicura dello smartphone (TEE o app SIM).

### 2.5.1 Struttura e funzionamento di un sistema di eID

Un IdP, che vuole gestire un sistema di eID riconosciuto a livello statale, deve soddisfare le condizioni per il riconoscimento statale. Deve quindi

- avere o aprire una sede aziendale in Svizzera ed impiegare per la regione del sistema di eID soggetti qualificati che siano incensurati;
- dimostrare la disponibilità di mezzi finanziari sufficienti per far fronte ad eventuali danni che potrebbero derivare da una sua inadempienza rispetto alle proprie responsabilità;
- realizzare un'infrastruttura TI certificata in relazione ai relativi profili di protezione per il sistema di eID, con salvataggio dei dati esclusivamente in Svizzera. Ciò comprende, in particolare
  - processi organizzativi e tecnici certificati sicuri per la registrazione di futuri titolari dell'eID e per l'esecuzione degli ordini di autenticazione ed identificazione.
  - L'applicazione eID certificata sicura come autenticatore per il riconoscimento del titolare. A seconda del livello di garanzia del sistema di eID desiderato, la funzione di autenticazione integrata deve essere in grado di riconoscere una persona con due fattori di autenticazione indipendenti (livello: oro) o con due fattori di cui uno biometrico (livello: platino). L'applicazione viene realizzata per le aree sicure[18] dei diversi sistemi operativi degli smartphone sui quali è possibile installare l'eID;
  - Un sistema sicuro di distribuzione per le applicazioni eID con la definizione di

[18] Le aree sicure degli smartphone moderni sono realizzate ad esempio attraverso i cosiddetti Trusted Execution Environment (TEE) o Secure Elements (SE) [58] [47]

identificatori dell'eID in un formato standardizzato che sono collegati in modo stabile con lo smartphone come supporto dopo l'installazione. Gli identificatori dell'eID devono avere una componente identificativa in modo da poter essere attribuiti da tutti i sistemi di eID all'IdP autore del rilascio[19];

- L'applicazione standardizzata interfaccia eID come interfaccia con i servizi che fanno affidamento sulla certificazione nei sistemi IAM delle parti facenti affidamento sulla certificazione, in modo che presso tutte le parti facenti affidamento sulla certificazione si eseguano sempre gli stessi protocolli di utilizzo quando viene usata un'eID;
- L'interfaccia di interoperabilità standardizzata con tutti i sistemi di eID riconosciuti a livello statale in essere, riconosciuti allo stesso livello di garanzia o ad un livello superiore;
- L'interfaccia standardizzata sicura con il canale di comunicazione protetto con il SIE per la trasmissione e l'aggiornamento periodico dei dati di identificazione personale;
- Il Web service per la predisposizione di liste consultabili di blocco e di revoca dell'eID sul campo;

- Un'offerta online di assistenza e aiuto che dia chiarimenti specifici e aiuto per ciascuna operazione che si può svolgere con l'eID.
- Un servizio clienti come entità a cui rivolgersi in caso di guasti, abusi o perdita di un'eID.

In presenza di tali condizioni, l'IdP richiede il riconoscimento statale presso il SRGI e fornisce le prove del soddisfacimento delle condizioni necessarie per il riconoscimento, principalmente sotto forma di certificazioni relative ai profili di protezione e rapporti di audit. Dopo aver verificato tali prove, il SRGI riconosce l'IdP e il sistema o i sistemi di eID per il livello di garanzia conseguito. Il SRGI pubblica gli IdP e i sistemi di eID riconosciuti nonché gli identificatori assegnati per le componenti da identificare degli identificatori dell'eID.

L'IdP riconosciuto a livello statale deve far sottoporre ad audit i propri sistemi di eID almeno ogni tre anni per dimostrare il costante rispetto delle condizioni di riconoscimento e deve consegnare i rapporti degli audit al SRGI. Il SRGI proroga il riconoscimento se il rapporto dell'audit conferma il soddisfacimento delle condizioni e se l'IdP ha pagato quanto dovuto per la trasmissione dei dati di identificazione personale.

Il riconoscimento statale può essere revocato se l'IdP viola le disposizioni di legge, se non soddisfa più le condizioni per il riconoscimento o se interrompe la propria attività o deve interromperla causa fallimento. In tale caso, il sistema di eID può essere assunto da un altro IdP riconosciuto a livello statale.

Un IdP può offrire i propri sistemi di eID riconosciuti a livello statale alle parti facenti affidamento sulla certificazione e a soggetti autorizzati ad acquisire un'eID. Il rilascio di un'eID dovrebbe essere gratuito per la persona. L'IdP può però utilizzare il modello operativo che preferisce per l'esecuzione di identificazioni ed autenticazioni. La Confederazione definirà però dei limiti per le quote aggiuntive che possono essere addebitate per l'utilizzo dei servizi di interoperabilità. Tutti i servizi federali che richiedono un'identificazione o un'autenticazione per i loro servizi online, devono accettare come mezzo d'identificazione l'eID di un sistema di eID riconosciuto di un livello di garanzia sufficiente. Ogni servizio federale interessato deve stipulare un accordo con

[19] Così come chi emette carte di credito viene identificato attraverso una parte del numero della carta di credito, l'identificatore dell'eID dovrà includere una parte di identificazione che individua l'IdP rilasciante e il sistema di eID. Questo identificatore contribuisce alla realizzazione dell'interoperabilità tra i sistemi di eID.

almeno un IdP[20], in modo che si possano utilizzare tutte le eID riconosciute a livello statale idonee in base al livello di sicurezza.

Non appena la Svizzera stipulerà con l'UE il relativo trattato internazionale, un IdP potrà far notificare dalla Confederazione presso l'UE un sistema di eID riconosciuto a livello statale e da lui gestito, che sia sufficientemente affermato sul mercato sulla base della quota di mercato che detiene. Le condizioni precise potranno essere definite solo nel momento in cui verrà stipulato il trattato.

### 2.5.2 Ciclo di vita di utilizzo di un sistema di eID

Qualora una parte facente affidamento sulla certificazione desideri utilizzare per il proprio sistema IAM eID riconosciute a livello statale per l'identificazione e l'autenticazione dei propri associati nella propria base di persone, deve concludere un accordo di utilizzazione per un sistema di eID al livello di garanzia richiesto con almeno un IdP. Può scegliere liberamente tra gli IdP offerenti e decide in base a considerazioni commerciali. Le interfacce tecniche ed organizzative sono invece ampiamente standardizzate per tutti i sistemi di eID offerti. Per poter usare l'eID, deve integrare un'interfaccia eID nel proprio servizio facente affidamento sulla certificazione, che offra le seguenti funzioni:

- Portale standardizzato di registrazione ed accesso per i titolari di eID per il rilevamento dell'identificatore dell'eID o di uno pseudonimo assegnato dall'IdP all'identificatore. In occasione dell'inserimento di un nuovo titolare nella base di persone della pfac (registrazione), il portale mostra al titolare anche quali attributi identitari siano richiesti presso l'IdP per la trasmissione.
- Interfaccia standardizzata al servizio facente affidamento sulla certificazione, attraverso la quale vengono ricevuti gli ordini di registrazione o accesso del servizio facente affidamento sulla certificazione e sono forniti i ticket di risposta emessi dalle componenti del sistema centrale di eID. Ogni ordine ed ogni risposta sono definiti in un formato standardizzato e ricevono sempre il relativo identificatore dell'eID ovvero l'identificatore derivato relativo all'ordine. Tipicamente, l'interfaccia eID è un Web service con i necessari elementi di sicurezza per la trasmissione dell'ordine e la ricezione delle risposte.
- Ricezione di dati di identificazione personale che vengono forniti dal sistema di eID su richiesta del servizio facente affidamento sulla certificazione e con l'autorizzazione del titolare in forma standardizzata e sicura. Il titolare conferisce l'autorizzazione con un on time code, che riceve dall'IdP e che rispedisce all'IdP attraverso il portale di registrazione del servizio facente affidamento sulla certificazione attraverso l'interfaccia eID.

[20] Ci sarà per questo un bando pubblico, al quale potranno partecipare tutti gli IdP con un sistema di eID all'idoneo livello di garanzia.

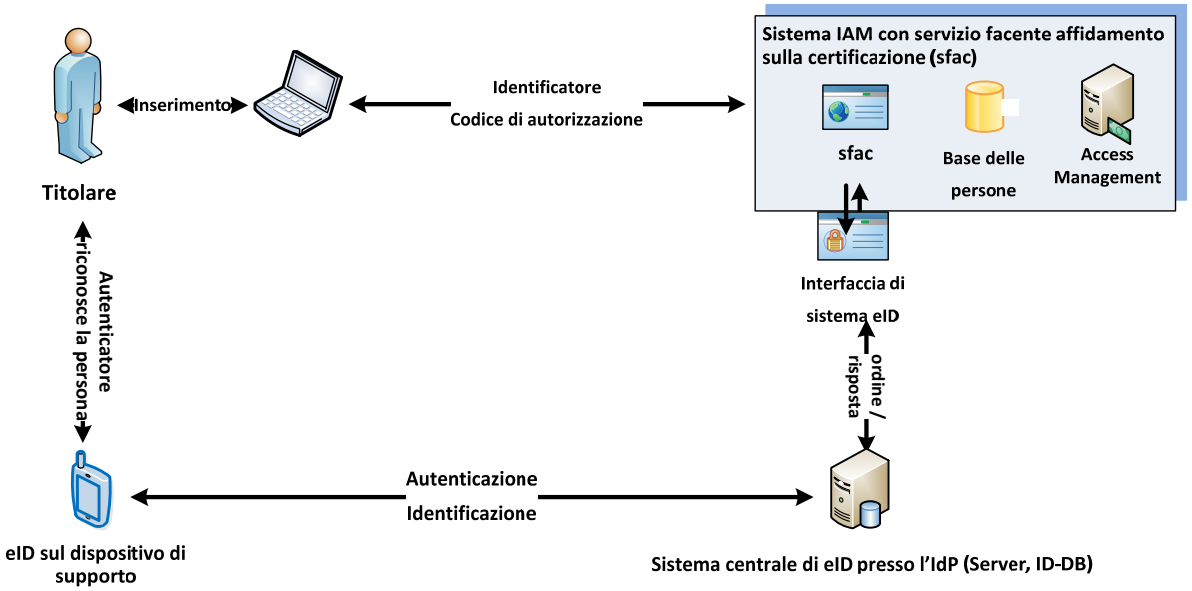



Figura 7: Interfacce del sistema di eID

Il servizio facente affidamento sulla certificazione, laddove necessario, viene adeguato dalla pfac allo sviluppo del proprio sistema IAM ma anche per l'accettazione di generazioni più recenti di eID. Il servizio facente affidamento sulla certificazione è tenuto ad accettare tutte le eID che rispettano il livello di garanzia richiesto, indipendentemente dall'IdP rilasciante. L'interfaccia eID è standardizzata in modo tale da potere elaborare tutte le forme di identificatori dell'eID, i ticket e i codici di risposta.

Una pfac può addebitare al titolare i costi diretti dell'utilizzo dell'eID presso il proprio servizio facente affidamento sulla certificazione.

### 2.5.3 Ciclo di vita dell'eID

Per l'attivazione e l'utilizzo di un'eID, concepita, a seconda del sistema di eID, per uno dei tre livelli di garanzia, si realizzano i seguenti passaggi:

- **Rilascio di un autenticatore dell'eID.** Il rilascio dell'autenticatore avviene in modo integrato in un dispositivo di supporto ovvero come applicazione per un dispositivo finale idoneo del futuro titolare e persino semplicemente sotto forma di istruzione di processo, che il titolare deve conoscere se sa usare come autenticatore un'infrastruttura comunemente disponibile. L'autenticatore dell'eID ha interfacce sicure per l'inserimento dei fattori di autenticazione, per la comunicazione con le componenti centrali del sistema di eID (server eID) presso l'IdP e per la visualizzazione di codici one time. Se possibile, l'autenticatore può anche regolare in modo sicuro una funzione comoda di visualizzazione ed inserimento e consentire quindi determinate protezioni delle transazioni. L'autenticatore dell'eID genera, dopo l'installazione sicura sul dispositivo, un identificatore univoco ed elementi di sicurezza per la comunicazione con il server eID dell'IdP. In alternativa, l'autenticatore dell'eID può essere fornito su un dispositivo di supporto sicuro dedicato con elementi di sicurezza e l'identificatore preinstallato. L'autenticatore dell'eID è pronto per la registrazione del titolare, se la comunicazione sicura con il server eID è stabilita e se l'identificatore è registrato nel server eID centrale.

- **Registrazione del titolare presso l'IdP.** La registrazione del titolare implica la generazione di un collegamento fisso della persona all'autenticatore dell'eID mediante la funzione di autenticazione e l'identificazione iniziale della persona, che ha creato un collegamento all'eID, rilevando i suoi dati di identificazione personale.
  - Il collegamento avviene attraverso il rilevamento degli attributi personali come dati di riferimento per i fattori di autenticazione:
    - definizione di un segreto ad esempio attraverso il rilevamento da parte del titolare di un codice PIN,
    - rilevamento di caratteristiche biometriche del titolare nell'autenticatore dell'eID sul dispositivo di supporto; si considerano come caratteristiche biometriche anche la misurazione permanente di vari comportamenti tipici da parte dei sensori del dispositivo di supporto, come ad esempio la misurazione della dinamica di movimento per inserimenti su touch screen,
    - presa di possesso dell'autenticatore dell'eID come dispositivo di supporto personale. Ad esempio una smart card personalizzata ma anche uno smartphone personale con carta SIM registrata rappresentano un dispositivo di supporto personale, sempre in possesso del titolare.
  - L'identificazione iniziale avviene rilevando i dati di identificazione personale, assegnati con un grado di sicurezza ben definito alla persona che ha creato un collegamento con l'autenticatore dell'eID. Ciò può avvenire in occasione di un colloquio personale presso un ufficio dell'IdP autorizzato ad effettuare l'identificazione oppure nel quadro di una identificazione video. È obbligatorio che la persona dimostri che l'autenticatore dell'eID la riconosce con i fattori di autenticazione stabiliti e che dimostri contestualmente la propria identità civile con un documento statale. In questa fase viene verificata la corretta attribuzione dei fattori di autenticazione personale, incapsulati nell'autenticatore dell'eID, agli attributi dell'identità civile. Il server eID centrale registra i dati di identificazione personale assieme all'identificatore dell'eID, che corrisponde agli attributi personali verificati tramite l'autenticatore. Normalmente nel server eID centrale non vengono rilevati altri attributi personali[21].
- **Richiamo di dati statali di identificazione personale**. Nel caso di un'eID riconosciuta a livello statale, l'attribuzione dell'identità civile all'eID, che in linea di principio deve essere fatta anche per le eID non riconosciute a livello statale, è ulteriormente rafforzata. Nell'ambito dell'identificazione iniziale della persona, l'IdP rileva il numero del documento di legittimazione presentato e i dati per l'apertura di un collegamento col titolare tramite un canale di comunicazione indipendente. Si tratta preferibilmente di un numero telefonico ma può anche trattarsi di un indirizzo e-mail o persino di un indirizzo postale. L'IdP trasmette entrambe le informazioni al SIE e richiede l'attribuzione dei dati di identificazione personale statali, che appartengono al numero di documento e che corrispondono al livello di garanzia dell'eID. Il SIE chiede poi al titolare, tramite il canale di comunicazione indipendente, il permesso di trasmettere i dati richiesti all'IdP. Gli invia a tale scopo un codice one time per la conferma dell'autorizzazione, che il titolare può comunicare all'IdP. L'IdP inoltra la conferma di autorizzazione al SIE e da esso riceve i dati statali di identificazione personale del titolare incluso l'identificatore personale univoco (IPU) attribuito a livello statale. L'IdP attiva quindi l'eID. Se il titolare nega l'autorizzazione, si può comunque attivare l'eID, a seconda della politica operativa dell'IdP. Non si tratterà però allora di un'eID riconosciuta a livello statale e questo andrà

[21] Diversamente dai dati di identificazione personale, gli attributi personali sono attributi della persona che non sono pubblicamente noti, come ad esempio i dati biometrici (vedi in merito i chiarimenti nell'allegato).

comunicato in occasione di ogni successiva identificazione o autenticazione al servizio facente affidamento sulla certificazione incaricante. Se, nel quadro dell'introduzione delle eID riconosciute a livello statale, si riconosce come nuovo un sistema di eID già esistente, le eID del sistema già attivate possono essere gestite come eID riconosciute a livello statale a condizione che per il riconoscimento statale manchi solo il richiamo dei dati di identificazione personale. Il processo di richiamo dovrà poi avvenire entro un determinato termine.

- **Registrazione del titolare presso una parte facente affidamento sulla certificazione.** Con un'eID riconosciuta a livello statale attivata, il titolare può registrarsi online presso tutti i servizi della pfac che fanno affidamento sulla certificazione che accettano eID riconosciute a livello statale, premesso che il livello di garanzia dell'eID sia sufficiente per il servizio facente affidamento sulla certificazione. Richiede sul portale del servizio facente affidamento sulla certificazione della pfac una nuova registrazione per la base di persone della pfac. Il servizio facente affidamento sulla certificazione della pfac visualizza la pagina di registrazione con i dati relativi alle informazioni di accesso richieste. Il titolare inserisce in tale modulo di iscrizione[22] l'identificatore dell'eID[23] e richiede una registrazione. Se non è già attivo in via permanente, avvia al più tardi in questo momento l'autenticatore dell'eID. Eventualmente può poi essere già fornita una prova dell'autenticazione congiuntamente all'identificatore, a seconda dell'eID. Il servizio facente affidamento sulla certificazione conferisce un **ordine di registrazione** per l'eID definita dall'identificatore e la invia tramite l'interfaccia eID al proprio IdP. Quest'ultimo verifica se gestisce lui tale eID o se deve inoltrare l'ordine ad un altro IdP, a cui ciò compete, attraverso l'interfaccia di interoperabilità. L'IdP competente autentica il titolare con l'eID. Se il titolare dell'eID si è autenticato, al titolare viene consegnato un messaggio con la richiesta di autorizzazione per la trasmissione dei dati richiesti dal servizio facente affidamento sulla certificazione[24]. Il messaggio contiene ad esempio un codice one time come conferma di autorizzazione. A seconda della situazione della comunicazione, il titolare conferisce l'autorizzazione direttamente attraverso la propria eID o inserendo il codice one time nel modulo di accesso del servizio facente affidamento sulla certificazione, che lo inoltra all'IdP come integrazione dell'ordine di registrazione. Qualora il permesso venga conferito, l'IdP trasmette un ticket di risposta all'interfaccia eID presso il servizio facente affidamento sulla certificazione con la conferma di identificazione e i dati autorizzati per la pfac. Qualora non vi sia tale autorizzazione, l'IdP invia dopo un time-out solo un ticket di risposta con la conferma di autenticazione. La pfac deve quindi decidere se desidera o meno registrare nella propria base di persone il nuovo associato solo con l'identificatore inserito[25]. In tal caso, in occasione di un successivo accesso potrebbe determinare di volta in volta solo se si tratti dello stesso titolare ma non avrebbe i dati dell'identità civile della persona.
- **Nuovo accesso presso una pfac (login).** Il titolare si iscrive presso il servizio facente affidamento sulla certificazione sul portale d'accesso con l'identificatore dell'eID o il relativo pseudonimo e inserisce, se richiesto, ulteriori dati di identificazione. Avvia a tal fine l'autenticatore dell'eID se l'eID non è attiva in via permanente. Il servizio facente affidamento sulla certificazione emette per il proprio IdP un **ordine di accesso**. Esso

[22] I moduli di accesso della pfac dovranno soddisfare determinati requisiti di standardizzazione in modo che lo schema di base sia identico su tutti i portali.

[23] A seconda del portale del servizio facente affidamento sulla certificazione, l'inserimento avviene tramite tastiera o in via elettronica, se l'eID e il dispositivo del portale, ad esempio, hanno un'interfaccia NFC.

[24] La pfac può richiedere, per la gestione della propria base di persone, attributi dei dati statali di identificazione ma anche altri attributi gestiti dall'IdP.

[25] L'identificatore può essere rivelato in forma derivata per settori o anche in via transitoria. In tal caso sarebbe identificativo solo per la pfac ed eventualmente solo per un determinato periodo.

verifica se gestisce lui tale eID o se deve inoltrare l'ordine all'IdP competente tramite l'interfaccia di interoperabilità. L'IdP competente autentica il titolare con l'eID. Ad autenticazione avvenuta, l'IdP invia un ticket di risposta all'interfaccia eID presso il servizio facente affidamento sulla certificazione con la conferma di autenticazione.

- **Interoperabilità dell'eID.** L'assegnazione interoperabile degli ordini da parte della pfac all'IdP e dei ticket di risposta dell'IdP alla pfac nell'ambiente eID avviene in un formato fisso e in modo protetto attraverso Web services sicuri. I messaggi contengono l'identificatore univoco dell'IdP competente. Se un IdP riceve tale messaggio, verifica se sia il destinatario corretto e invia eventualmente il messaggio all'IdP ricevente giusto ai fini della sua elaborazione. È quindi sufficiente che l'infrastruttura di interoperabilità colleghi tutti gli IdP riconosciuti. In presenza di una sufficiente standardizzazione, non servono ulteriori servizi di interfaccia. Se non vengono introdotti determinati standard, l'interoperabilità potrebbe essere anche realizzata con uno hub centralizzato ma questo genererebbe dei costi aggiuntivi e in linea di principio evitabili, di cui dovrebbero farsi carico gli IdP, perlomeno in via transitoria.
- **Cancellazione di un'eID da parte del titolare.** Il titolare può richiedere all'IdP la cancellazione della propria eID. Ciò avviene contattando il servizio clienti online dell'IdP e richiedendo la cancellazione dell'eID. L'IdP richiede un'autenticazione con la eID ed invia ad autenticazione avvenuta un codice one time sul display dell'eID. Con tale codice il titolare può confermare la cancellazione. L'IdP rende poi inattiva l'eID e cancella i dati del titolare inseriti nella propria base di persone. Si può richiedere la cancellazione dell'eID anche in caso di abusi o smarrimento. In tal caso il titolare deve autenticarsi come soggetto avente diritto in un altro modo.
- **Blocco.** L'eID può essere bloccata in via transitoria o permanente dall'autenticatore o dall'IdP al verificarsi di tre situazioni:
  - Il titolare cerca più volte, invano, di autenticarsi rispetto alla funzione di autenticazione dell'eID. Se si supera il numero massimo di tentativi consentiti, l'eID si blocca a livello locale sul dispositivo di supporto. A seconda del tipo di eID e della politica di sicurezza del'IdP, tale blocco può essere rimosso o può essere permanente.
  - Se all'IdP viene comunicato in modo attendibile attraverso un canale qualsiasi che una certa eID è corrotta o nelle mani sbagliate, la bloccherà ed inserirà l'identificatore dell'eID in una lista di blocco. Informa del blocco il titolare.
  - L'IdP stabilisce attraverso la verifica periodica della validità dell'IPU che un determinato IPU è stato contrassegnato come non valido dal SIE in modo temporaneo o permanente. Se ha rilasciato un'eID ad una persona con tale IPU, dovrà bloccarla o revocarla e inserire il relativo identificatore dell'eID nella lista di blocco.
- **Riattivazione.** L'IdP può rimuovere un blocco e riattivare l'eID se il titolare è in grado di dimostrare che l'eID funziona normalmente e di esserne in possesso. Per lo sblocco locale deve essere stata avviata l'eID.

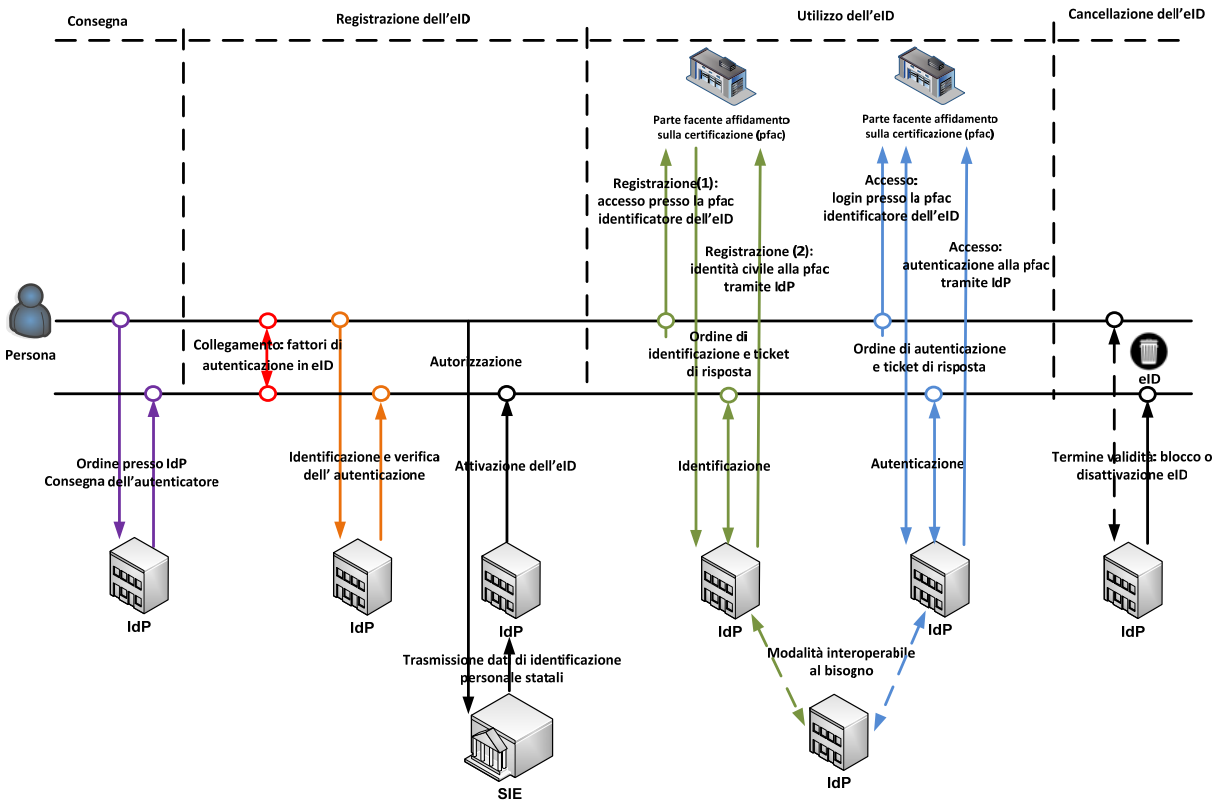



Figura 8: Processi dei cicli di vita dell'eID con rilascio (consegna, registrazione), utilizzo e cancellazione

Tabella 1: Rilascio di un'eID presso l'IdP

| **Livello di garanzia dell'eID** | **Argento** | **Oro** | **Platino** |
|---|---|---|---|
| Fase 1<br>Richiedere, ricevere ed installare l'autenticatore dell'eID | Assegnazione dell'autenticatore dell'eID per posta come token oppure online come applicazione<br>Installazione automatica sul dispositivo di supporto<br>Test di funzionamento con l'identificatore dell'eID all'IdP | | |
| Fase 2: registrazione presso l'IdP (1)<br>Collegamento della persona all'eID | Rilevamento di un fattore di autenticazione (event. solo possesso) | Rilevamento di 2 fattori di autenticazione | Rilevamento di 2 fattori di autenticazione con biometria |
| Fase 3: registrazione presso l'IdP (2)<br>Verifica dell'identità della persona con validazione della validità del documento, identità personale e collegamento della persona all'eID | Numero carta d'identità | Colloquio personale o identificazione video sulla base del documento d'identità | |
| | - | | Verifica immagine del volto |
| Fase 4: registrazione presso l'IdP (3)<br>Trasmissione dati di identificazione personale dal SIE all'IdP | Richiesta di autorizzazione tramite canale indipendente<br>Codice di autorizzazione dal titolare all'IdP<br>Consegna dei dati di identificazione personale all'IdP | | |
| Fase 5<br>Attivazione dell'eID | L'IdP attiva l'eID per l'utilizzo<br>Comunicazione al titolare | | |

Tabella 2: Processo operativo del primo accesso presso la pfac

| **Livello di garanzia dell'eID** | **Argento** | **Oro** | **Platino** |
|---|---|---|---|
| **Primo accesso presso la pfac con registrazione** | | | |
| Fase 1<br>Registrazione presso la pfac | Accesso con identificatore dell'eID o lo pseudonimo presso il servizio facente affidamento sulla certificazione della pfac (interfaccia eID)<br>Avvio dell'aautenticatore dell'eID | | |
| Ordine di identificazione pfac all'IdP | Identificatore dell'eID, livello di garanzia e richiesta attributi attraverso l'interfaccia eID | | |
| Fase 2<br>Autenticazione da parte dell'IdP in base al livello di garanzia | Rilevamento di un fattore di autenticazione | Rilevamento di 2 fattori di autenticazione | Rilevamento di 2 fattori di autenticazione con biometria |

| | |
|---|---|
| Fase 3 Trasmissione attributi dell'identità civile dall'IdP alla pfac | Visualizzazione elenco attributi e codice one time per l'autorizzazione sul display del dispositivo di supporto dell'eID<br>Re-invio codici dal titolare all'IdP |
| Ticket di risposta dall'IdP alla pfac | Identificatore dell'eID e attributi dell'identità civile |
| Fase 4: Completamento registrazione presso la pfac | Il titolare ottiene l'accesso al servizio pfac |

Tabella 3: Processo operativo di log-in presso la pfac

| **Livello di garanzia dell'eID** | **Argento** | **Oro** | **Platino** |
|---|---|---|---|
| **Log-in** | | | |
| Fase 1 Accesso presso la pfac | Accesso con identificatore dell'eID o pseudonimo presso il servizio facente affidamento sulla certificazione della pfac (interfaccia eID)<br>Avvio dell'autenticatore dell'eID | | |
| Ordine di autenticazione dalla pfac all'IdP | Identificatore dell'eID e livello di garanzia | | |
| Fase 2 Autenticazione da parte dell'IdP secondo il livello di garanzia | Rilevamento di un fattore di autenticazione | Rilevamento di 2 fattori di autenticazione | Rilevamento di 2 fattori di autenticazione con biometria |
| Ticket di risposta dall'IdP alla pfac | Identificatore dell'eID e conferma autenticazione | | |
| Fase 4: Completamento accesso presso la pfac | Il titolare può accedere al servizio pfac | | |

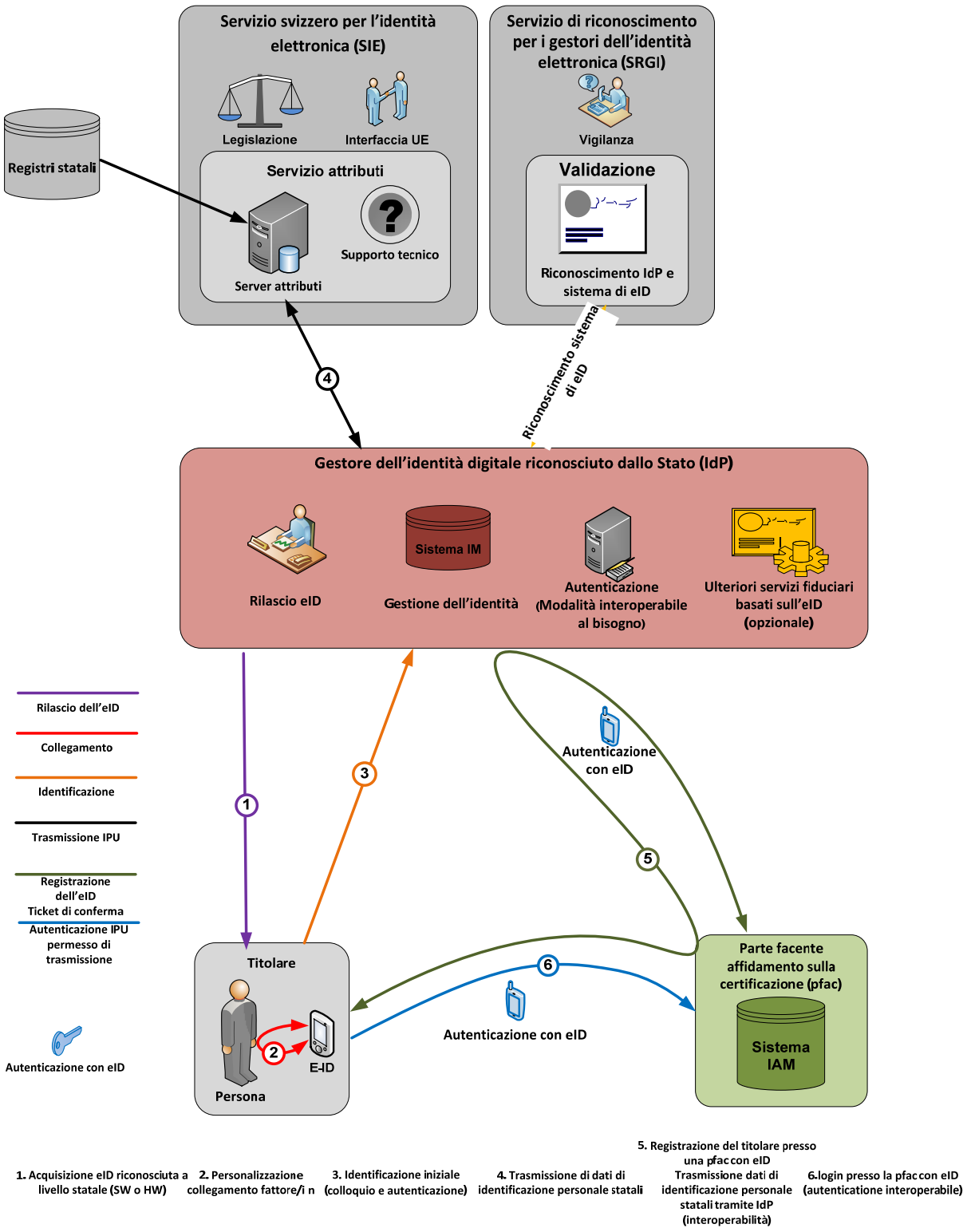



Figura 9: Rilascio ed impiego dell'eID

## 2.6 Elementi attuativi chiave

Si descrivono ora con un grado maggiore di dettaglio alcuni elementi importanti per la soluzione svizzera, come il concetto dei livelli di garanzia, il nuovo identificatore personale univoco e i dati statali di identificazione personale disponibili per ciascun livello di garanzia, il processo di trasmissione dei dati statali di identificazione personale all'IdP e l'interoperabilità all'interno della

rete dei sistemi di eID riconosciuti a livello statale.

### 2.6.1 I tre livelli di garanzia dell'eID

Non serve per ogni caso operativo un'eID del massimo livello di garanzia. Un livello di garanzia elevato è spesso legato ad una minore facilità d'uso, in particolare per la registrazione iniziale, e a costi più elevati. Spesso, per i casi operativi più semplici, basta un livello di garanzia relativamente basso, ottenibile con una semplice registrazione con identificazione iniziale online (come nel caso di Apple ID o Google ID) e il rilevamento di un fattore per l'autenticazione. Solo per i processi operativi più critici l'eID deve garantire un livello di garanzia più elevato che comporterà al momento della registrazione un colloquio personale per l'identificazione iniziale (come ad es. per SuisseID o Mobile ID) e un'autenticazione attraverso almeno due fattori in fase di utilizzo. La riduzione ad un solo livello di garanzia ostacolerebbe quindi la diffusione di un'eID riconosciuta a livello statale. Per questo si riconoscono a livello statale i sistemi di eID idonei ad uno di tre livelli di garanzia. I tre livelli di garanzia dei sistemi di eID riconosciuti a livello statale in Svizzera sono definiti in modo tale da soddisfare gli stessi requisiti in materia di sicurezza che sono richiesti per i tre livelli di garanzia dell'eID definiti nel regolamento eIDAS dell'UE (art 8 del regolamento eIDAS [2] e relativi atti di esecuzione[3]). Anche i requisiti di autenticazione del NIST prevedono gli stessi tre livelli di garanzia [6]. Ogni livello di garanzia offre un grado diverso di fiducia nell'identità e nell'autenticità del titolare dell'eID. Quale livello di garanzia venga preso in considerazione per quale tipo di applicazione viene stabilito nei rispettivi atti normativi specifici per le applicazioni di eGovernment, ovvero viene definito dai privati facenti affidamento sulla certificazione. Per l'eEducation viene così scelto un livello di garanzia diverso rispetto a quanto prescritto per vote électronique o per applicazioni di eHealth.

Oltre all'affidabilità dell'IdP e alle fonti degli attributi che gli IdP utilizzano per creare l'identità civile per il titolare, la registrazione (identificazione iniziale della persona e collegamento dell'eID alla persona), l'autenticazione sul campo mediante l'eID (1 fattore, 2 fattori, biometria) e la trasmissione ed elaborazione degli ordini e delle risposte nella rete interoperabile dei sistemi di eID riconosciuti influiscono in misura significativa sul livello di garanzia di un'eID. I tre livelli vengono chiamati Argento, Oro e Platino per motivi di comunicazione. Le principali caratteristiche dei tre livelli sono illustrate nei punti seguenti e nella tabella 3 (in parentesi le denominazioni UE per il corrispondente livello di garanzia):

- ARGENTO (basso): l'eID, nel quadro di un sistema di eID, ha lo scopo di ridurre il rischio di uso abusivo o alterazione dell'identità. La registrazione può avvenire online sulla base di un documento statale. Il SIE trasmette all'IdP solo pochi dati di identificazione personale (cognome, nome(i), data di nascita e IPU). L'uso dell'eID richiede almeno un'autenticazione tramite un fattore. Il trattamento di un'eID di questo tipo è quindi paragonabile ad un badge di accesso, ad una soluzione di pagamento contactless per importi non elevati o ad un login tramite identificatore e password sicura o PIN. Il livello di garanzia „ARGENTO" si riferisce ad un mezzo di identificazione elettronica che fornisce un grado di sicurezza relativamente basso ma pur sempre più alto di una semplice autodichiarazione con un'user id di propria scelta ed una password a piacere riguardo all'identità pretesa o dichiarata di una persona.
- ORO (significativo): l'eID, nel quadro di un sistema di eID, ha lo scopo di ridurre in misura significativa il rischio di uso abusivo o alterazione dell'identità. La registrazione avviene con un colloquio personale presso l'IdP o mediante videoidentificazione sulla base di un documento statale. Oltre ai dati di identificazione personale del livello inferiore, il SIE trasmette ulteriori attributi (ad es. sesso, stato civile, immagine del volto ecc.). L'utilizzo dell'eID richiede almeno un'autenticazione con 2 fattori. Il trattamento di un'eID di questo tipo è quindi paragonabile, alle usuali soluzioni in ambito bancario (carte conto, carte di

credito, soluzioni di eBanking). Il livello di garanzia „ORO“ si riferisce ad un mezzo di identificazione elettronica che offre un significativo livello di sicurezza riguardo all'identità pretesa o dichiarata di una persona.

- PLATINO (elevato): l'eID, nel quadro di un sistema di eID, ha lo scopo di ridurre il rischio di uso abusivo o alterazione dell'identità. La registrazione avviene con un colloquio personale presso l'IdP o mediante videoidentificazione, sulla base di un documento statale. Inoltre, si verifica l'autenticità del documento e almeno una caratteristica biometrica sulla base di una fonte che è un'autorità indipendente (validità del documento e immagine del volto o altra caratteristica biometrica di riconoscimento). Il SIE trasmette tutti i dati disponibili di identificazione personale (ad es. anche l'immagine della firma). L'utilizzo dell'eID richiede almeno un'autenticazione con 2 fattori, di cui uno necessariamente biometrico («fattore inerente» secondo gli atti esecutivi eIDAS [3]).). Il trattamento di un'eID di questo tipo è paragonabile ad uno smartphone con riconoscimento attraverso l'impronta digitale, il volto o la voce. L'autenticazione biometrica crea un collegamento ancora più stretto tra l'eID e il titolare. Il livello di garanzia „PLATINO“ si riferisce ad un mezzo di identificazione elettronica che offre IL MASSIMO livello di sicurezza riguardo all'identità pretesa o dichiarata di una persona.

Tabella 4: Livelli di garanzia dell'eID

| Livello | Argento (basso) | Oro (significativo) | Platino (elevato) |
|---|---|---|---|
| **Autenticazione** | Almeno 1 fattore | 2 fattori | 2 o 3 fattori con biometria |
| **Registrazione: collegamento persona all'eID** | La persona esegue il collegamento all'eID non sorvegliata | La persona esegue il collegamento all'eID con verifica da parte dell'IdP | La persona esegue il collegamento all'eID con verifica del fattore biometrico da parte dell'IdP |
| **Registrazione: identificazione iniziale** | Online con numero del documento e data di scadenza | Mediante colloquio o videoconferenza con documento; test autenticazione eID | Mediante colloquio o videoconferenza con documento; test autenticazione eID |
| **Dati di identificazione personale** | Set minimo e IPU; incrocio annuale dei dati con il SIE | Tutti a parte determinati dati biometrici; incrocio trimestrale dei dati con il SIE | Tutti i dati di identificazione personale; incrocio settimanale dei dati con il SIE |
| **Requisito per IdP e sistema di eID secondo le definizioni eIDAS [3], art. 2.4** | Riconoscimento del sistema di eID con audit di sicurezza per livello di garanzia ‚basso', significativo' o ‚elevato' in base all'art. 2.4.7 in[3] | | |

Con tale modello è possibile innanzitutto registrare un'eID idonea con un'autenticazione mediante 2 fattori (attualmente, di fatto, lo standard dell'industria) al livello Argento e portarla successivamente, al bisogno, ad un livello di garanzia più alto mediante un colloquio personale. Col livello di garanzia Argento si mantiene semplice l'accesso ad un'eID riconosciuta a livello statale e questo può rappresentare un fattore di successo essenziale per chi offre sul mercato sistemi di eID riconosciuti a livello statale. Inoltre, una persona può possedere più eID di vari IdP o a livelli di garanzia diversi.

### 2.6.2 Identificatore personale univoco (IPU)

Il concetto presuppone il persistere dell'attuale pratica di utilizzo del NAVS13 ed introduce perciò un ulteriore e nuovo identificatore personale univoco (IPU), disponibile per l'eID ma anche per altre applicazioni. Qualora si dovesse invece allentare la rigida pratica di applicazione del NAVS13, il NAVS13 potrebbe essere utilizzato direttamente come IPU anche per l'eID. Attualmente si sta appurando se ciò sia possibile.

Lo Stato definisce un nuovo identificatore personale univoco (IPU), indipendente da altri dati di identificazione personale come il nome o il NAVS13, per tutte le persone rilevate nei pertinenti registri della Confederazione con un documento emesso dallo Stato e aventi diritto di soggiorno. L'IPU funge da ancora per tutti i dati di identificazione personale appartenenti ad una persona, che il SIE trasmette all'IdP, e per tutti gli altri attributi che un IdP o una pfac attribuisce ad una persona. I dati statali di identificazione personale, che il SIE trasmette all'IdP, sono abbinati all'IPU in modo crittografato in modo che l'IdP possa verificare in qualsiasi momento l'integrità e l'autenticità di un attributo trasmesso. L'IdP è tenuto ad aggiornare periodicamente i dati di identificazione personale relativi ad un'eID emessa attraverso un corrispondente rilevamento presso il SIE e la frequenza dei rilevamenti dipende dal livello di garanzia. L'IdP associa in particolare nel proprio eIDM anche l'identificatore dell'eID all'IPU del titolare. Ciò vale anche per eventuali identificatori derivati o per gli identificatori di una seconda eID, in modo che una parte facente affidamento sulla certificazione possa sempre attribuire ad una persona in modo univoco eventuali accessi multipli con diverse eID, con l'aiuto dell'IdP. Grazie all'IPU, le parti facenti affidamento sulla certificazione possono semplificare i propri processi amministrativi, renderli più affidabili e quindi ridurre i costi. Al posto dell'IPU, se così viene stabilito dall'IdP, può essere usata per ogni parte facente affidamento sulla certificazione un'identificazione personale derivata, in modo tale da escludere una profilazione trasversale a diverse istanze o settori.

### 2.6.3 Dati di identificazione personale (DIP)

Il SIE acquisisce per ogni persona avente diritto i dati di identificazione personale (DIP) dai relativi registri della Confederazione (vedi cap. 4). I DIP sono amministrati dallo Stato e gli attributi registrati coincidono con i valori rilevati in occasione della più recente identificazione della persona da parte dello Stato, per l'emissione di un documento di legittimazione o di un altro atto statale, che ha condotto ad un'iscrizione nei registri della Confederazione (ISA, SIMIC, Infostar, UCC-UPI)[26].

Ulteriori attributi identitari statali possono essere assunti successivamente, qualora nell'ambiente eID ve ne fosse l'esigenza e a fronte di un fondamento giuridico. È importante capire che né un IdP né una parte facente affidamento sulla certificazione hanno accesso a tali attributi senza il consenso esplicito della persona in questione. È sempre la persona che fa trasmettere i DIP di un livello di garanzia esplicitamente, consapevolmente ed esclusivamente agli IdP riconosciuti, da cui acquisisce un'eID riconosciuta a livello statale. Anche la successiva trasmissione di singoli attributi dei DIP statali da parte dell'IdP ad una parte facente affidamento sulla certificazione può avvenire solo con l'autorizzazione esplicita del titolare.

Tabella 5: Dati di identificazione personale disponibili

[26] Per motivi di coerenza, anche per l'eID vengono sempre trasmessi gli stessi attributi così come inseriti nel più recente documento pubblico emesso o in Infostar. I casi speciali, come quello del ritiro del documento, di un decesso o dei cambi di identità nei programmi di protezione dei testimoni sono regolamentati nel piano dettagliato.

| Attributo | Argento | Oro | Platino |
|---|---|---|---|
| **IPU** | X | X | X |
| **Cognome ufficiale** | X | X | X |
| **Nome(i)** | X | X | X |
| **Data di nascita** | X | X | X |
| **NAVS13 (solo per aventi diritto)** | | X | X |
| **Sesso** | | X | X |
| **Luogo di nascita** | | X | X |
| **Stato civile** | | X | X |
| **Nazionalità** | | X | X |
| **Status di soggiorno** | | X | X |
| **Immagine del volto** | | X | X |
| **Tipo e numero del documento** | | X | X |
| **Immagine della firma** | | | X |
| **Data del più recente accertamento degli attributi per tutti gli attributi** | X | X | X |

### 2.6.4 Trasmissione dei dati di identificazione personale

La trasmissione di dati di identificazione personale ad un IdP fa seguito ad una richiesta dell'IdP. Nella richiesta, l'IdP comunica al SIE, indicando il numero di un documento pubblico valido rilasciato dalla Svizzera, per quale persona sia richiesta la trasmissione dei DIP. La comunicazione dell'IdP al SIE contiene anche la data di rilascio del documento, con il quale la persona si è identificata in occasione dell'identificazione iniziale, il livello di garanzia del sistema di eID, per il quale vengono richiesti i DIP, e i dati relativi alla modalità con cui contattare il titolare attraverso un canale indipendente.

Il SIE comunica al titolare attraverso il canale indicato (ad es. numero di cellulare, indirizzo e-mail o indirizzo postale) che l'IdP richiedente, per il riconoscimento statale dell'eID rilasciata, desidera ricevere i DIP corrispondenti al relativo livello di garanzia. Il SIE comunica alla persona un codice di autorizzazione che essa dovrà fornire all'IdP qualora acconsenta alla trasmissione.

L'IdP rimanda questo codice di autorizzazione al SIE entro un lasso di tempo ben definito. I tempi dipendono dal canale di comunicazione utilizzato dal SIE con la persona. Non appena il SIE riceve il codice di autorizzazione, trasmette i DIP del corrispondente livello di garanzia all'IdP. La data, che viene sempre trasmessa, dell'ultima identificazione non deve essere necessariamente identica alla data del documento, trasmessa dall'IdP. Una persona può avere più documenti validi e i DIP corrispondono sempre ai valori che sono stati accertati in occasione dell'ultima identificazione statale.

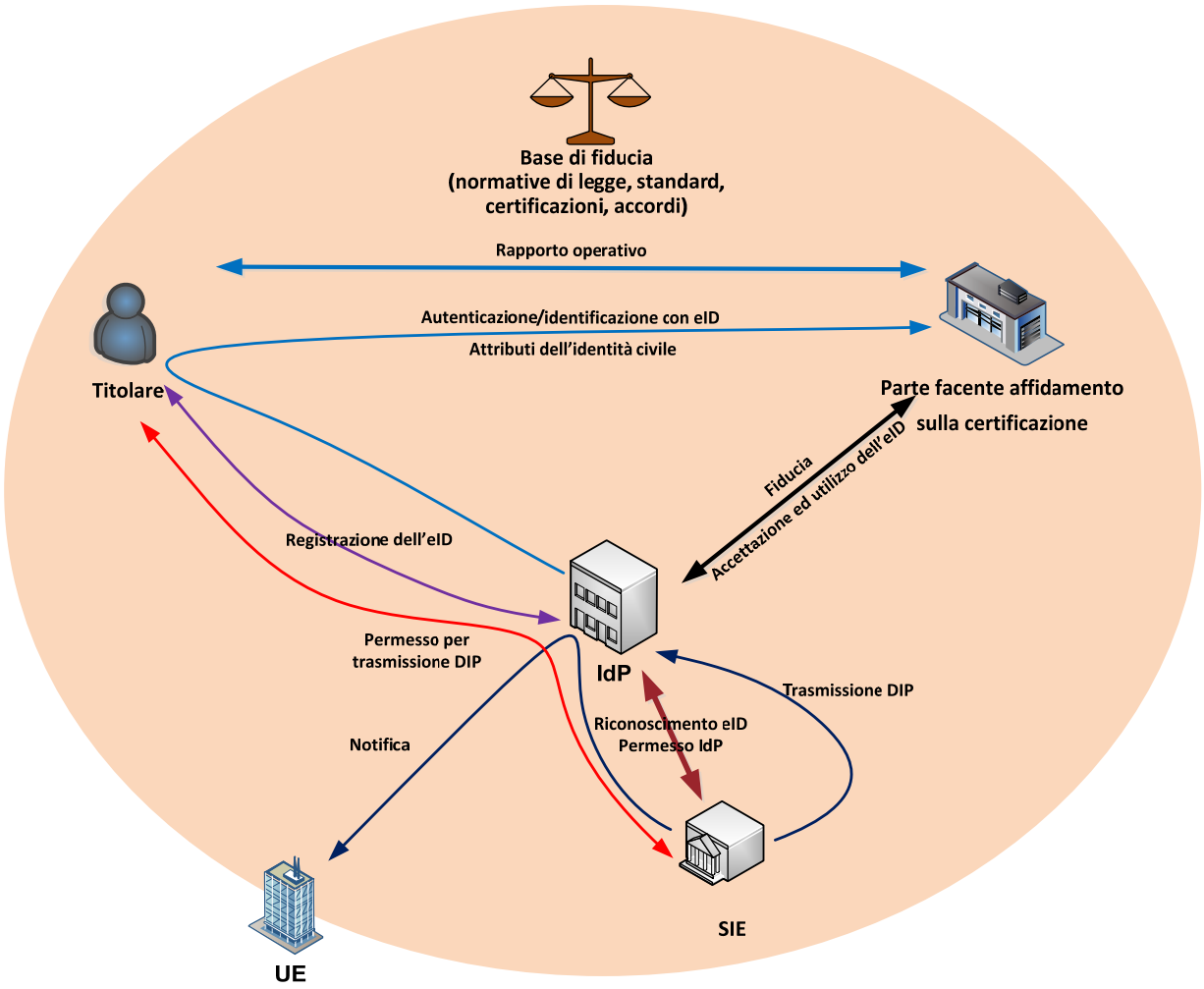



Figura 10: Rapporti e processi nel quadro del rilascio e dell'utilizzo di un'eID

L'IdP deve aggiornare periodicamente i dati trasmessi con i dati aggiornati del SIE. La periodicità dipende dal livello di garanzia della relativa eID. L'IdP deve anche richiedere quotidianamente la lista pubblicata dal SIE con le modifiche dei DIP, rilevate per determinati IPU[27]. L'aggiornamento non necessita di una nuova autorizzazione del titolare.

### 2.6.5 Interoperabilità dei sistemi di eID

L'interoperabilità tra i sistemi di eID dello stesso livello di garanzia è un fattore importante per una rapida diffusione e per l'accettazione di sistemi di eID riconosciuti a livello statale nell'ambiente eID. Non ha però molto senso che ogni parte facente affidamento sulla certificazione debba stipulare con ciascun IdP riconosciuto a livello statale degli accordi di utilizzazione per i sistemi di eID utilizzabili. Per questo il piano stabilisce che ogni eID che raggiunge il necessario livello di garanzia o lo supera, possa essere utilizzata presso tutti i servizi che fanno affidamento sulla certificazione da parte della pfac, indipendentemente dall'IdP che ha effettuato il rilascio.

Il protocollo per l'utilizzo di un'eID in sede di registrazione o di accesso ad un servizio facente

[27] Le modifiche degli attributi possono verificarsi, per esempio, in seguito ad un matrimonio, se nel frattempo si sono rilasciati una nuova CID o un nuovo passaporto. Anche il decesso di una persona deve comportare naturalmente una revoca dell'eID.

affidamento sulla certificazione è sempre lo stesso, nel procedimento e nella struttura, per ogni mezzo (dispositivi mobili, PC, chiosco Internet ecc.) e offre al titolare un'esperienza di utilizzo sicura. I servizi facenti affidamento sulla certificazione integrano nei propri portali le pagine di registrazione ed accesso corrispondenti sotto forma di un'interfaccia eID ampiamente standardizzata. La comunicazione in sede di utilizzo col titolare dell'eID deve essere sempre simile, indipendentemente dal sistema di eID e dalla pfac.

Anche per i servizi facenti affidamento sulla certificazione non risultano oneri aggiuntivi per via del requisito dell'interoperabilità. Creano gli stessi ordini di identificazione ed autenticazione per tutte le eID e li inviano all'IdP al cui sistema di eID sono collegati. Ricevono i ticket di risposta sempre tramite quell'IdP, in un formato standard.

L'interoperabilità viene realizzata esclusivamente attraverso i sistemi di eID dell'IdP. Ogni ordine contiene l'identificatore dell'eID. Parte dell'identificatore identifica il sistema di eID e l'IdP che ha effettuato il rilascio (ciò corrisponde agli identificatori dei sistemi di eID riconosciuti a livello statale pubblicati nell'elenco del SRGI). L'IdP inoltra un ordine di identificazione o di autenticazione all'IdP competete e riceve da lui il ticket di risposta dopo l'esecuzione, che restituisce al servizio facente affidamento sulla certificazione.

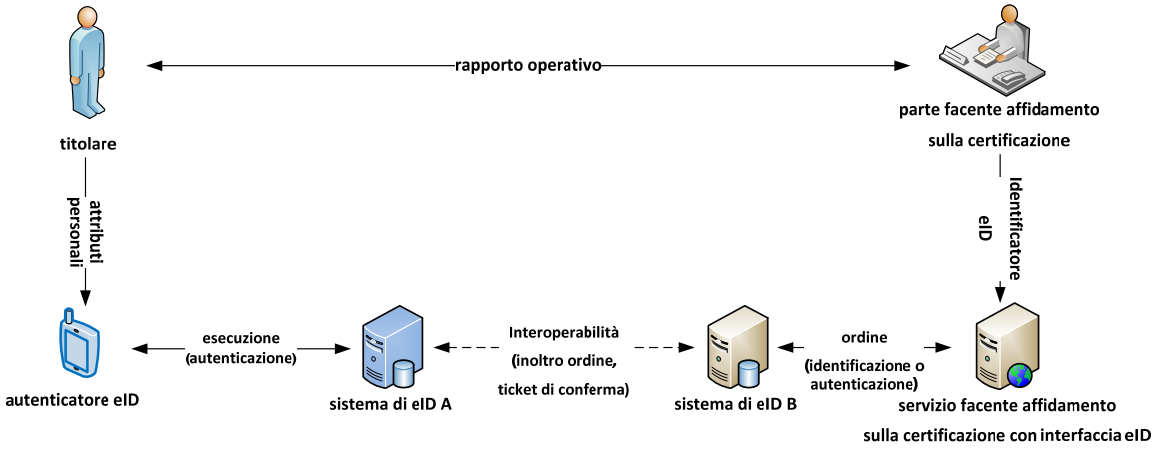



Figura 11: Realizzazione dell'interoperabilità attraverso la federalizzazione

## 2.7 Notificabilità

Il 23 luglio 2014 l'UE ha emanato il regolamento (UE) n. 910/2014 [2] 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. I relativi atti di esecuzione sono stati varati a partire dal settembre del 2015 [36] [37] [38] [39].

Di seguito si affrontano in sintesi i requisiti di un sistema di eID svizzero che sia conforme al regolamento in materia di eID, affinché possa eventualmente essere successivamente notificato. Ovviamente la Svizzera non è soggetta ad alcun obbligo giuridico di recepire il regolamento UE. Tuttavia, in considerazione dei fitti rapporti commerciali e sociali con la maggioranza dei Paesi membri dell'UE, si ritiene che la Svizzera abbia interesse ad essere, prima o poi, inserita nel sistema europeo per l'interoperabilità delle identità elettroniche. Anche se al momento non si sa se, quando e come la Svizzera entrerà in tale sistema con un trattato internazionale, il sistema svizzero di eID va concepito fin da subito in modo che possa essere, in linea di principio, notificato.

Per poter essere notificato, un sistema nazionale deve soddisfare le condizioni sancite all'articolo 7 del Regolamento eIDAS. La lettera a) numero iii) prevede anche sistemi di eID come quello ivi regolamentato, in cui lo Stato riconosce sistemi offerti da privati. Gli altri requisiti sono espressi alle lettere da c) a f) e sono:

c) Sia il sistema di eID che le eID soddisfano i requisiti di almeno uno dei livelli di garanzia di cui all'articolo 8 paragrafo 3.

d) Lo Stato notificante garantisce che, al momento del rilascio, siano attribuiti all'eID i dati di identificazione personale corretti e ne è obbligatoriamente responsabile anche ai sensi dell'articolo 11 numero (1).

e) L'IdP che rilascia l'eID assicura anche che l'eID sia attribuita solo alla persona corretta conformemente alle specifiche relative al livello di garanzia.

f) Lo Stato notificante stesso garantisce la disponibilità dell'autenticazione online per ogni servizio facente affidamento sulla certificazione in qualsiasi momento, in tutta l'UE e ne è responsabile in caso di danni sempre ai sensi dell'articolo 11 numero (1).

Questi requisiti influenzano la regolamentazione svizzera. Con la pianificata legge in materia di eID si istituisce, tra l'altro, un quadro giuridico e di standardizzazione per il riconoscimento a livello statale di sistemi di eID e il riconoscimento dell'IdP. Ciò è configurato in modo da consentire successivamente il reciproco riconoscimento dei sistemi di eID riconosciuti a livello statale tra la Svizzera e l'UE o singoli Stati membri. La compatibilità di questo piano con gli atti di esecuzione del regolamento eIDAS è stata per quanto possibile verificata e ritenuta presente.

# 3 Contributo dello Stato all'eID

## 3.1 Panoramica

Le autorità svizzere tengono già oggi vari registri contenenti dati di identificazione personale, ci cui si possono citare, a titolo rappresentativo, il registro informatizzato dello stato civile (Infostar), il registro degli abitanti e il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC). Nel campo dei documenti, i dati di identificazione personale per gli svizzeri sono tenuti nel Sistema d'informazione per documenti d'identità (ISA) e per gli stranieri nel Sistema d'informazione centrale sulla migrazione (SIMIC). Anche il registro UPI dell'Ufficio centrale di compensazione serve per l'identificazione ufficiale delle persone fisiche e per l'attribuzione di un numero univoco AVS (UPI è l'acronimo di „Unique Person Identification").

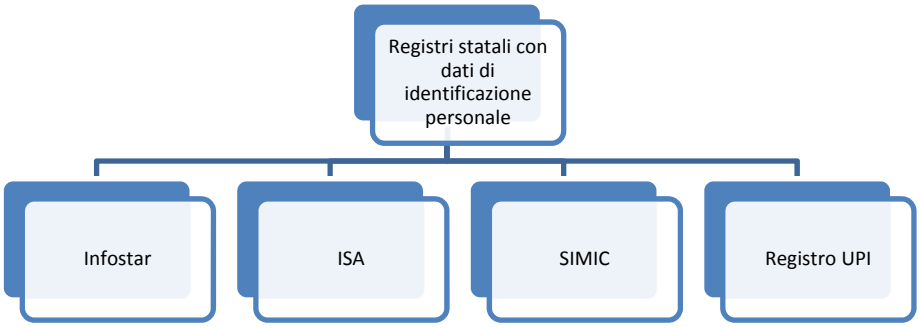



Figura 12: Registri confederali delle persone

Nell'ambito della legge sull'armonizzazione dei registri (LArRA) il nuovo numero AVS (NAVS13) è stato designato come identificatore personale unico ed univoco nei registri interessati dal censimento della popolazione, vale a dire i registri federali di persone ed i registri cantonali e comunali degli abitanti. Anche la tessera d'assicurato rilasciata dagli assicuratori-malattie ai sensi dell'ordinanza sull'assicurazione malattie del 27 giugno 1995 (OAMal) contiene il numero AVS quale identificatore personale univoco. Il NAVS13 non consente di risalire alla data di nascita e all'identità della persona ed è una serie di 13 cifre (3 cifre del codice del Paese secondo ISO 3166, 9 cifre casuali, 1 cifra di controllo).

Sulla base dei dati di identificazione personale in ISA o SIMIC, la Confederazione rilascia attualmente mezzi di identificazione tradizionali: il passaporto svizzero, la carta d'identità e la carta di soggiorno. La Confederazione funge in tal modo da garante dell'identità statale di una persona. Con l'introduzione di un'eID riconosciuta a livello statale, potranno essere rilasciati, sulla base dei dati di identificazione personale presenti presso la Confederazione, mezzi d'identificazione elettronica basati sui dati di identificazione personale trasmessi a livello statale.

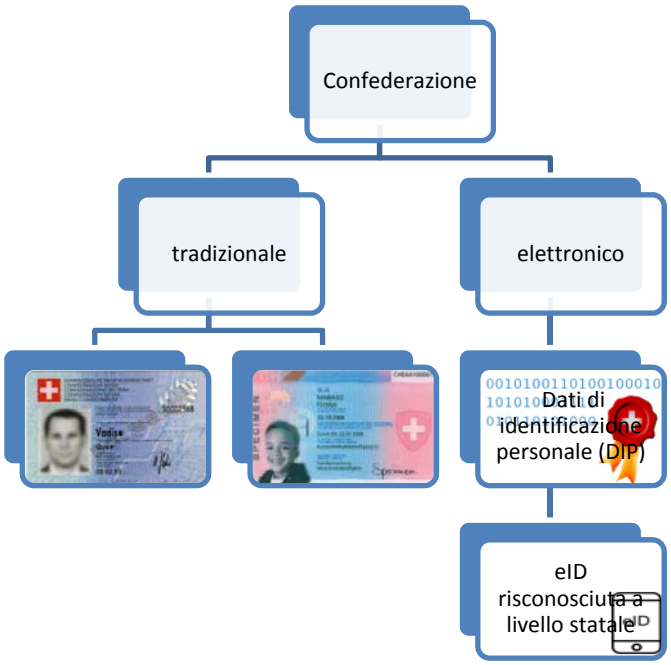



Figura 13: Mezzi statali di identificazione

La Confederazione svolge quattro compiti: innanzitutto crea e cura un quadro giuridico e di fiducia trasparente, in secondo luogo gestisce un'interfaccia elettronica attraverso la quale gli IdP riconosciuti a livello statale possono acquisire dati di identificazione personale gestiti a livello statale, in terzo luogo può riconoscere a livello statale gli IdP e i loro sistemi di eID e in quarto luogo vigila sugli IdP riconosciuti a livello statale e sui sistemi di eID. Questi due compiti saranno svolti presso la Confederazione da due unità amministrative: il „Servizio svizzero per l'identità elettronica (SIE)" e il „Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)".

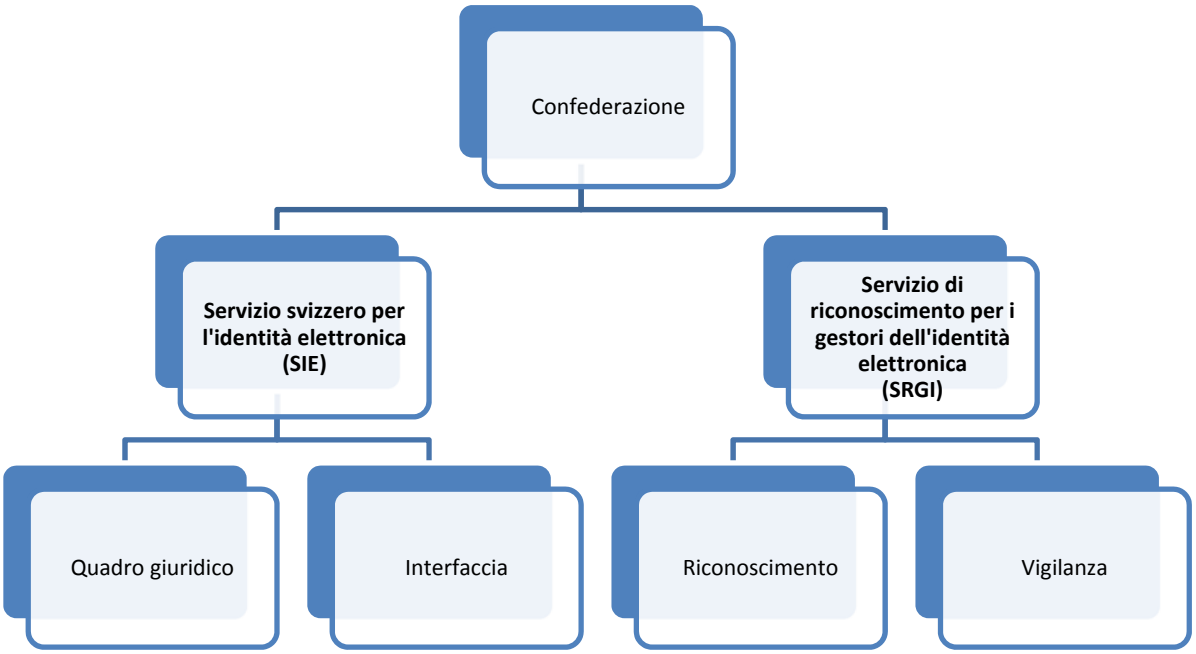



Figura 14: Compiti del SIE e del SRGI

## 3.2 Servizio svizzero per l'identità elettronica (SIE)

### 3.2.1 Quadro giuridico

Il SIE (chiamato anche Servizio per l'identità) cura a livello operativo, in collaborazione con il SRGI, i requisiti giuridici, organizzativi e tecnici. In particolare, definisce gli standard delle interfacce per l'interoperabilità dei sistemi di eID e adegua agli sviluppi tecnici e socioeconomici i requisiti tecnici ed organizzativi nell'ambito del riconoscimento degli IdP e dei sistemi di eID.

Per poter essere notificato successivamente all'UE, un sistema di eID deve rispettare i requisiti del regolamento eIDAS dell'UE. Per questo bisognerà prestare attenzione che i requisiti per i sistemi di eID riconosciuti a livello statale della Svizzera rispettino il regolamento eIDAS, come stipulato dal Consiglio federale nel suo mandato.

### 3.2.2 Interfaccia

Il SIE rende disponibili agli IdP riconosciuti i dati di identificazione personale gestiti presso la Confederazione, attraverso un'interfaccia elettronica. Definendo e trasmettendo un identificatore personale univoco, è possibile assicurare l'integrità dell'attribuzione dei dati di identificazione personale alla persona corretta. In quanto interfaccia B2B, è accessibile esclusivamente agli IdP riconosciuti.

Nel quadro del rilascio di un'eID riconosciuta a livello statale, la persona si identifica con un documento tradizionale presso l'IdP, che trasmette al SIE il numero del documento. Il SIE rileva, consultando ISA o SIMIC, l'IPU corrispondente e lo trasmette all'IdP, assieme ai dati di identificazione personale corrispondenti al livello di garanzia dell'eID.

Per quanto riguarda la migrazione di dati esistenti, si potranno utilizzare i sistemi identificativi già esistenti (come ad esempio NAVS13) per l'assicurazione della qualità.

Ogni trasmissione viene protocollata dal SIE e contrassegnata in modo che una consultazione di aggiornamento da parte di un IdP possa essere attribuita ad una precedente prima trasmissione.

Il SIE acquisisce i dati di identificazione personale come il nome di una persona, in primo luogo da Infostar e, ad es., i numeri del documento o la foto in via sussidiaria da ISA o SIMIC. La seguente tabella mostra una possibile selezione di dati di identificazione personale con l'indicazione del registro fonte.

| ***Nome dell'attributo*** | **Registro fonte** |
|---|---|
| *IPU* | UPI, SIMIC, ISA |
| *Cognome ufficiale* | Infostar |
| *Nome(i)* | Infostar |
| *Data di nascita* | Infostar |
| *Numero di assicurato (NAVS13)* | Infostar |
| *Sesso* | Infostar |
| *Luogo di nascita* | Infostar |
| *Stato civile* | Infostar |
| *Nazionalità* | Infostar |
| *Status di soggiorno* | SIMIC |
| *Immagine del volto* | ISA, SIMIC |
| *Numero/i documento passaporto* | ISA |
| *Numero/i documento CID* | ISA |
| *Numero/i documento NAA* | SIMIC |
| *Immagine della firma* | ISA, SIMIC |

Tabella 6: Fonti statistiche dei dati di identificazione personale

Prima di introdurre l'eID riconosciuta a livello statale, bisogna procedere all'integrazione dei registri con il NAVS13 e alla loro conseguente migrazione. Per aumentare ulteriormente la qualità dei dati, è opportuno incrociare in modo coerente i registri con i dati di Infostar, come già avviene oggi con ISA.

I dati di identificazione personale possono essere integrati con ulteriori metadati, come l'indicazione di una fonte o la data del rilevamento. Essi sono inoltre sempre collegati all'IPU in modo crittografato. La prima trasmissione dei dati di identificazione personale all'IdP deve avvenire solo con il consenso esplicito e documentato dell'interessato.

Gli IdP sono tenuti ad aggiornare periodicamente i dati di identificazione personale riferiti ad un IPU. Anche questo avviene attraverso l'interfaccia del SIE, ma non serve più un'altra autorizzazione esplicita della persona per questioni di semplicità d'uso. A seconda del livello di garanzia, gli IdP devono eseguire gli aggiornamenti ogni anno (Argento), trimestre (Oro) o settimana (Platino). L'aggiornamento può essere avviato dall'IdP sulla base dell'IPU, nel cui caso il SIE verifica se vi sia effettivamente stata una prima trasmissione per l'IPU all'IdP concreto, con conferma espressa da parte della persona.

Per poter bloccare rapidamente l'eID in speciali circostanze, il SIE predispone sulla propria

interfaccia un elenco degli IPU bloccati. Può costituire una circostanza speciale, ad esempio, la morte di una persona. Gli IdP sono tenuti a bloccare immediatamente tutte le eID rilasciate per gli IPU nell'elenco. L'elenco può essere consultato gratuitamente dall'IdP attraverso l'interfaccia. È tenuto a procedere in tal senso regolarmente (ogni giorno).

### 3.2.3 Organizzazione

Il SIE ha compiti giuridici e in particolare operativi. Per l'elaborazione e poi la cura dei requisiti giuridici, organizzativi e tecnici per i sistemi di eID, il SIE necessita di corrispondenti risorse.

Il SIE è anche responsabile della gestione dell'interfaccia per la trasmissione dei dati di identificazione personale. Funge da Single Point Of Contact (SPOC) per tutte le questioni specialistiche e tecniche dei registri collegati ed IdP in relazione all'interfaccia.

I chiarimenti relativi a dati di identificazione personale che si presume siano incoerenti o falsi o che lo siano effettivamente non sono forniti dal SIE stesso ma dall'organismo di compensazione dell'UCC-UPI, che svolge già oggi questo compito nell'ambito del NAVS13 [40].

Per l'assolvimento di questi compiti il SIE necessita, secondo le stime attuali, di una percentuale di impiego del 300 percento a tempo indeterminato (cura permanente e adeguamento periodico delle disposizioni tecniche agli sviluppi, cura dello SPOC). Visto che le banche dati rilevanti per le eID riconosciute a livello statale (ad eccezione del registro UPI) sono di competenza del DFGP, il SIE andrà ragionevolmente costituito in seno al DFGP.

## 3.3 Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)

### 3.3.1 Riconoscimento

Gli IdP costituiti (privati e pubblici) possono farsi riconoscere a livello statale dal SRGI assieme ai propri sistemi di eID ad uno dei livelli di garanzia previsti. Un IdP può far riconoscere più sistemi di eID ad un diverso livello di garanzia.

Sia l'IdP che il sistema concreto di eID devono ottenere il riconoscimento per almeno il livello di garanzia desiderato. A tal fine il SIE, d'intesa con il SRGI, definisce condizioni giuridiche, organizzative e tecniche e il SRGI verifica che l'IdP le soddisfi. Le certificazioni e i riconoscimenti esistenti (ad es. nel quadro di FieLe o di piattaforme di messaggistica) sono integrati nel processo di riconoscimento quanto più possibile, in modo da evitare duplicazioni.

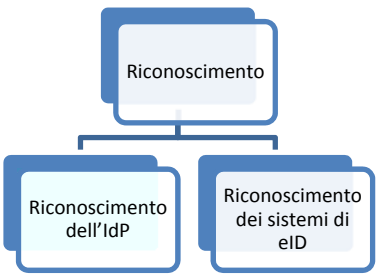



Figura 15: Riconoscimento dell'IdP e del sistema di eID

Il riconoscimento deve sostanzialmente poggiare su prove di conformità con le norme internazionali e i profili nazionali di protezione. L'IdP deve perciò dimostrare al SRGI la

conformità della propria organizzazione e dei propri sistemi di eID mediante certificazioni. Il SRGI verifica i documenti forniti inerenti la certificazione e decide in merito al riconoscimento statale.

Un caso particolare di riconoscimento è l'eventuale notifica di un sistema di eID nei confronti dell'EU. Con la notifica, un sistema di eID viene riconosciuto nell'UE, dove potrà essere utilizzato al relativo livello di garanzia. Reciprocamente, tutti i sistemi di eID degli Stati membri dell'UE già riconosciuti devono essere riconosciuti anche in Svizzera al corrispondente livello di garanzia. La Svizzera deve concludere un trattato bilaterale con l'UE per la notifica.

Inoltre, il SRGI pubblica un elenco degli IdP e dei sistemi di eID riconosciuti, col quale le parti facenti affidamento sulla certificazione e le persone fisiche possono verificare lo status di uno specifico IdP o sistema di eID.

### 3.3.2 Vigilanza

Il SRGI effettua la vigilanza sugli IdP e sui sistemi di eID riconosciuti e interviene in caso di scostamenti rispetto ai requisiti o di casi concernenti il campo della sicurezza delle TIC. A tal fine il SRGI vigila sul mercato, raccoglie e valuta segnalazioni concernenti la sicurezza delle TIC nell'ambito dell'eID e, se necessario, le inoltra al SIE. Inoltre il SRGI richiede agli IdP riconosciuti le necessarie prove di conformità nei tempi stabiliti e le verifica. Come ultima ratio, il SRGI può revocare ad un IdP o ad un sistema di eID il riconoscimento statale.

### 3.3.3 Organizzazione

Il SRGI riconosce e vigila sui sistemi di eID riconosciuti a livello statale. I suoi compiti presentano sinergie con altri compiti della Confederazione nel settore delle TIC:

DFF: l'ODIC è responsabile dell'organizzazione della IAM Confederazione. In tale ambito sono altresì necessarie la vigilanza e la direzione dei sistemi IAM collegati.

Inoltre, in relazione alla legge sulla sicurezza delle informazioni si potrebbe creare un'unità organizzativa che si faccia carico di tali compiti di vigilanza.

DATEC: l'UFCOM già dispone di competenze ed esperienze di alto livello nel campo della sorveglianza del mercato. Inoltre l'UFCOM è già impegnato nel campo delle firme elettroniche (FiEle).

DEFR: anche la SECO, in collaborazione con la Federazione svizzera d'identità, che sostiene, dovrà svolgere una funzione di vigilanza.

Sulla base di una prima analisi, appare opportuno costituire il SRGI presso il DFF (ODIC), poiché IAM Confederazione e sicurezza TIC sono fortemente legate nei contenuti ai sistemi di eID riconosciuti a livello statale. Per l'adempimento dei compiti indicati è necessaria per il SRGI una percentuale di impiego del 100 percento a tempo indeterminato.

## 3.4 Effetti finanziari per la Confederazione

### 3.4.1 Presupposti del modello

Se si analizza il beneficio finanziario per il mercato derivante dall'eID, si nota come esso riguardi principalmente le parti facenti affidamento sulla certificazione, perché queste ultime, utilizzando l'eID, possono semplificare e rendere più vantaggiosi i propri processi (ad es. meno sportelli, meno carta e interruzioni di supporto dell'informazione, maggiore rapidità, modelli operativi innovativi, identificatore personale univoco ecc.). Il modello di finanziamento deve tenere conto di questa informazione essenziale.

Per questo il modello del „pay per use" si qualifica come il modello migliore per addebitare le prestazioni statali agli operatori del mercato. Il modello prevede che tutti gli enti interessati si facciano carico dei propri costi di investimento e gestione (e assumano quindi di fatto una garanzia del deficit), ma che le spese possano essere pareggiate dalle entrate nel medio termine. S'intende con ciò che risultano più promettenti dei pagamenti legati all'utilizzo concreto dell'eID rispetto a pagamenti ex ante. La Confederazione dovrebbe addebitare agli IdP delle commissioni solo se gli IdP richiedono effettivamente degli attributi. Si potrebbe prevedere come ulteriore incentivo che la Confederazione rinunci a riscuotere oneri per la prima trasmissione dei dati di identificazione personale qualora un IdP a sua volta rilasci gratuitamente l'eID.

Saranno poi gli IdP a stabilire come addebitare tali costi all'utente (ad es. "pay per use" o „flat rate"). Gli IdP possono risparmiare in modo significativo sui costi se si può evitare un colloquio con la persona in occasione del rilascio dell'eID. Si potrebbe pensare ad esempio che gli IdP utilizzino per la verifica biometrica dell'identità l'immagine del viso trasmessa dalla Confederazione al livello di garanzia Oro e Platino.

Nel quadro dei lavori si sono verificati anche altri modelli, poi però esclusi, come il modello „prepaid", che ha adottato ad esempio SuisseID. In tale modello si richiede agli utenti un pagamento anticipato che dovrebbe possibilmente coprire i costi per l'emittente. Dalla verifica di tale modello è però risultato che dover pagare una commissione, senza che vi siano evidenti ed ampie possibilità di utilizzo dell'eID, rappresenterebbe un ostacolo significativo per l'accettazione della soluzione. Si è verificato ed escluso anche un modello „promotion", in cui la Confederazione offrirebbe i servizi del SIE senza limiti temporali e gratuitamente, perché tale modello ignora completamente la realtà dei costi. Tale modello avrebbe comunque il vantaggio di abbassare ulteriormente la soglia d'ingresso per le altre parti e verrebbe meno l'onere dell'incasso di quanto dovuto.

Per le stime dei costi per la Confederazione si deve partire da un modello il cui parametro è difficile da prognosticare. Come stima approssimativa, si presuppone che nel medio termine circa la metà della popolazione svizzera disponga di un'eID riconosciuta a livello statale e che quindi arrivino alla Confederazione circa 10 milioni di richieste di attributi. Non si ritiene in questo momento che il carico che queste richieste comportano renda necessario ampliare la capacità delle banche dati esistenti.

### 3.4.2 Spese d'investimento e di gestione del SIE e del SRGI

Sulla base dei presupposti di cui al capitolo 3.4.1**Fehler! Verweisquelle konnte nicht gefunden werden.**, si calcolano per la creazione del SIE costi complessivi per la Confederazione pari a circa 6,5 milioni di CHF. I costi operativi annuali, inclusi i costi relativi al personale, sono stimati in circa 2,2 milioni di CHF.

Per il funzionamento del SIE serve una percentuale di impiego del 300 percento a tempo

indeterminato e per il SRGI una percentuale di impiego del 100 percento a tempo indeterminato. Presso il SIE sono previste queste risorse a livello di personale per lo svolgimento dei seguenti compiti: a) supporto tecnico agli uffici che forniscono i dati internamente alla Confederazione, b) supporto tecnico agli IdP riconosciuti a livello statale, c) responsabilità applicativa e cura dell'infrastruttura TIC necessaria presso il SIE (interfaccia B2B e collegamento delle fonti di dati come ISA, Infostar ecc.), d) elaborazione e cura delle disposizioni organizzative e tecniche per il riconoscimento degli IdP e dei sistemi di eID riconosciuti a livello statale, e) acquisto (gara pubblica) dei servizi degli IdP necessari presso la Confederazione, f) cura e pubblicazione dell'elenco degli IdP riconosciuti e g) reperimento delle informazioni sugli attuali sviluppi tecnologici nel campo dell'eID e relative questioni inerenti la sicurezza delle TIC. Presso il SRGI le risorse del personale sono usate per a) il riconoscimento degli IdP (verifica delle prove di conformità) e b) controllo della conformità costante degli IdP riconosciuti e dei sistemi di eID impiegati.

L'entità dei costi operativi potrà variare in occasione della futura elaborazione del piano dettagliato concernente le TIC.

### 3.4.3 Spese della Confederazione per i servizi degli IdP

Visto che la Confederazione deve procurarsi i servizi identitari necessari per i propri portali presso gli IdP riconosciuti a livello statale, vi sono delle spese.

Queste spese sono più che compensate dai risparmi derivanti dal venir meno delle soluzioni isola IM attuali e future della Confederazione e dai risparmi sui costi dovuti alla semplificazione dei processi operativi.

### 3.4.4 Entrate eID della Confederazione

Visto che il SIE, a partire dall'inizio delle operazioni, riscuote commissioni per la trasmissione e l'aggiornamento dei dati di identificazione personale trasmessi agli IdP, si generano entrate per la Confederazione. A fronte di circa 10 milioni di consultazioni l'anno, la commissione richiesta sarà probabilmente un importo modesto a due cifre per ciascuna trasmissione, nell'ordine di centesimi. Per quattro aggiornamenti degli attributi l'anno i costi per un'eID al livello di garanzia Oro saranno quindi decisamente inferiori ad un franco. Inoltre la Confederazione può riscuotere commissioni per il riconoscimento e la verifica periodica delle prove di conformità degli IdP e dei loro sistemi di eID.

### 3.4.5 Conto economico di gestione

L'introduzione di sistemi di eID riconosciuti a livello statale rappresenta un progetto strategico pluriennale. Per quanto concerne la diffusione dell'eID non si devono quindi esprimere aspettative irrealistiche, come mostrano anche le esperienze di altri Paesi. L'eID, così come fu per il voto per corrispondenza, è uno strumento innovativo che deve innanzitutto guadagnarsi la fiducia della popolazione.

Oltre alla creazione dell'eID, bisogna che le parti facenti affidamento sulla certificazione predispongano un numero sufficiente di applicazioni online accattivanti. A livello legislativo si potrebbe prevedere, come misura di protezione dell'investimento, che tutte le autorità che applicano le leggi federali e richiedono un'autenticazione sui loro portali Internet, siano sostanzialmente tenuti ad accettare anche i sistemi di eID riconosciuti a livello statale.

I costi operativi della Confederazione saranno interamente compensati nel medio termine dalle

entrate derivanti dalle commissioni per la trasmissione degli attributi e per il riconoscimento degli IdP in modo che il progetto risulti neutrale per il bilancio federale. All'inizio però saranno necessari un „finanziamento iniziale" ovvero la sopra citata „garanzia del deficit".

# 4 L’eID in pratica

## 4.1 Introduzione

Il capitolo esamina le possibili future applicazioni delle eID riconosciute a livello statale. Nel capitolo si utilizzano consapevolmente termini parzialmente semplificati (come ad es. „dati personali ufficiali“ al posto di „dati di identificazione personale registrati presso la Confederazione“ o „rilasciante“ al posto di „gestore di servizi identitari / IdP“).

## 4.2 Rilascio di un’eID

In una prima fase il cliente può decidere liberamente quale prodotto tra quelli offerti risponda meglio alle sue esigenze. Le eID offerte si differenziano in base al livello di garanzia, al supporto (smartphone, chiavetta USB, smartcard ecc.) o ai servizi aggiuntivi che eventualmente le accompagnano, come la firma elettronica o la protezione della transazione. È consentito possedere contemporaneamente più eID riconosciute a livello statale.

In una seconda fase, il cliente acquisisce l’eID che ha scelto. Questo comporta un processo di registrazione presso il rilasciante che, nel caso più semplice, può avvenire online; di norma sarà però necessario un colloquio personale presso il rilasciante o perlomeno una videoidentificazione. Il cliente viene identificato mediante un documento ufficiale, si richiedono, con la sua autorizzazione, i suoi dati personali ufficiali alla Confederazione, si personalizza l’eID, la si consegna al cliente e il rilasciante la attiva.

In una terza fase, il titolare può già utilizzare l’eID. Visto che le eID riconosciute a livello statale, grazie ai requisiti di standardizzazione sui portali funzionano in larga misura allo stesso modo, i titolari acquisiscono presto familiarità col sistema. Ciò vale, in particolare, anche nel caso in cui si cambi il rilasciante.

## 4.3 Restituzione o perdita di un’eID

Qualora un’eID vada persa o non possa più essere utilizzata per altre ragioni, il titolare può farla bloccare o cancellare in qualsiasi momento dal rilasciante. Chi rilascia un’eID riconosciuta a livello statale è tenuto ad offrire i relativi servizi per le segnalazioni e ad inserire le eID bloccate in una lista di blocco. Questa lista di blocco è consultata dalle parti facenti affidamento sulla certificazione, nel momento in cui una persona accede con un’eID.

## 4.4 Utilizzo di un’eID

### 4.4.1 Democrazia elettronica e partecipazione elettronica

Lo sviluppo di internet influenza anche la formazione delle opinioni politiche e della volontà popolare. Nel 2011, la Cancelleria federale, su incarico del Consiglio federale, ha elaborato un rapporto sulla democrazia e la partecipazione elettroniche [41]. Nel testo si analizza l’influsso di Internet sui diritti popolari e si delineano gli scenari futuri. Gli ambiti in cui i titolari di eID possono partecipare nel medio termine alla vita politica sono:

- Votazioni popolari
- Elezioni federali

- Iniziative popolari federali e referendum
- Petizioni federali[28]
- Consultazioni e indagini conoscitive[29]
- Parlamenti - autorità – tribunali

Nel processo della formazione democratica della volontà popolare, la fase della decisione fa seguito a quelle dell'informazione e della consultazione. La Cancelleria federale e i Cantoni stanno lavorando per estendere in modo graduale le modalità del voto elettronico (vote électronique) [42]: lo fanno dal 19 gennaio 2003, giorno in cui ad Anières (GE) si è svolto il primo scrutinio di questo tipo. Dopo una prima tappa, caratterizzata dai test pilota effettuati dai Cantoni di Ginevra, Neuchâtel e Zurigo in stretta collaborazione con la Confederazione, il 31 maggio 2006 il Consiglio federale si è espresso a favore di un'introduzione a tappe del voto elettronico. In occasione della votazione popolare del 05.06.2016, cinque Cantoni hanno offerto il canale elettronico per il voto.

Nel 2009 ha suscitato scalpore il referendum contro l'introduzione obbligatoria del passaporto biometrico: il referendum, infatti, non era stato preannunciato da un partito organizzato e quindi non è stato indetto secondo le modalità convenzionali; gli oppositori al passaporto biometrico hanno infatti mobilitato gli elettori utilizzando Facebook. Già nel corso dell'anno precedente una consigliera nazionale aveva depositato una mozione[30] in cui invitava il Consiglio federale "a creare le basi legali necessarie per svolgere progetti pilota di raccolta elettronica di firme per iniziative e referendum. Questi progetti vanno eseguiti parallelamente ai progetti di voto elettronico e di governo elettronico".

Rispondendo alla mozione, il Consiglio federale ha ribadito la propria proposta di procedere a tappe alla digitalizzazione dei diritti popolari. Prima tappa: votare elettronicamente; seconda tappa: eleggere elettronicamente; terza tappa: raccolta di firme digitali; quarta tappa: proposte di candidatura elettroniche.

### 4.4.2 eGovernment

Sebbene il concetto di eGovernment in parte si sovrapponga ad altri ambiti del capitolo 4, si citano qui brevemente le possibilità di utilizzo di un'eID riconosciuta a livello statale che già oggi sono in parte online, con una propria procedura di accesso:

- Compilazione di moduli online di autorità, ad es. per un cambio d'indirizzo, per ottenere permessi o richiedere documenti.
- Accesso a dossier fiscali e rendiconti IVA
- Accesso a portali come eVera per gli svizzeri all'estero
- Accesso a portali per controlli dei veicoli a motore
- Richiesta di un estratto del casellario giudiziale

I titolari di un'eID riconosciuta a livello statale possono accedere in modo sicuro a tutti i portali delle autorità che supportano il pianificato identificatore personale univoco, senza dover prima

[28] Tutte le persone, e quindi non solo gli aventi diritto al voto, hanno il diritto di rivolgersi per iscritto alle autorità competenti per presentare richieste, proposte e reclami in relazione a qualsiasi attività statale.

[29] Nell'ambito di una procedura di consultazione, la Cancelleria federale rende accessibile la documentazione in forma elettronica. I pareri possono essere inoltrati anche in forma elettronica; per quanto riguarda invece lo svolgimento dell'intera procedura e la valutazione dei pareri, non è ancora possibile procedere per via elettronica.

[30] 08.3908. Mozione Jacqueline Fehr. Rafforzare la democrazia grazie alla raccolta elettronica di firme. 17.12.2010 Tolto dal ruolo poiché pendente da più di due anni.

procedere ad onerose registrazioni. In base all'attuale disegno di legge, si tratterà, presso la Confederazione, di tutti i portali che richiedono accessi elettronici.

### 4.4.3 eHealth

L'introduzione della cartella informatizzata del paziente è programmata già per il 2017 [9]. i titolari di una cartella informatizzata del paziente o i loro rappresentanti legali devono potersi iscrivere in sicurezza. Ciò sarà possibile con un'eID riconosciuta a livello statale.

Si prevede che per ogni bambino si apra tale cartella alla nascita o nel quadro del primo controllo medico e che essa venga poi costantemente aggiornata. In caso di ricovero ospedaliero, i professionisti della salute avranno accesso alla cartella informatizzata e, dopo le dimissioni, il medico di famiglia avrà a disposizione i dati medici per i controlli. Con un'app eHealth il paziente in futuro potrebbe registrare i dati sanitari e fornirli al bisogno ai professionisti della salute.

È ipotizzabile che il paziente in futuro riceva una ricetta elettronica con la quale richiedere i farmaci necessari per le terapie presso una farmacia online. Inoltre, si potrebbe aggiungere anche la possibilità di consulti medici online (eConsultation).

### 4.4.4 eEducation

Da molto tempo ormai la digitalizzazione è entrata nelle scuole del livello primario, secondario e terziario. Oggi sono disponibili sempre più materiali didattici digitali, a cui spesso si accede dopo essere entrati nel portale della scuola o della casa editrice. Anche le schede di valutazione o le informazioni scolastiche vengono offerte sempre più spesso in via elettronica. Con un'eID gli alunni possono accedere a queste risorse della scuola.

I genitori, entrando con la propria eID, hanno accesso alle informazioni della scuola e confermano in modo digitale di aver preso visione della scheda di valutazione dei figli, per godere dei propri diritti e assolvere i propri obblighi nel periodo scolastico e formativo.

Al livello terziario, già oggi è possibile iscriversi e scegliere i corsi in modalità elettronica. Anche in tal caso è necessario un accesso elettronico, che può avvenire in modo sicuro con un'eID riconosciuta a livello statale. Nell'istruzione terziaria è probabile anche che l'eID venga utilizzata a livello internazionale.

### 4.4.5 eCommerce

I titolari possono utilizzare l'eID negli shop online, per registrarsi e per poi accedere di nuovo in seguito. Gli shop online non possono e non devono essere tenuti per legge ad accettare le eID riconosciute a livello statale. Tuttavia, dal punto di vista dei titolari, è molto pratico che lo facciano. In questo modo non dovranno infatti gestire svariati user name e password diverse ma potranno usare ovunque la propria eID riconosciuta a livello statale. Visto poi che viene creato un quadro giuridico trasparente per le eID riconosciute a livello statale, anche i diritti e i doveri sono regolamentati in modo chiaro. Agli shop online sarà ad esempio vietato, in quanto parte facente affidamento sulla certificazione, commerciare i dati statali di identificazione personale trasmessi dall'IdP. Questi dati vengono trasmessi dall'IdP rilasciante solo se il titolare vi acconsente espressamente.

Inoltre, con l'eID è possibile, in modo semplice ed affidabile, provare la propria età, sia che si tratti di un'età massima nel caso delle offerte per i giovani che di un'età minima nel caso di offerte per gli adulti o magari i pensionati.

### 4.4.6 ePayment

Il pagamento in modalità Mobile Payment è sempre più diffuso. Con l'eID è ancora più semplice fornire il documento d'identità digitale per una soluzione di pagamento digitale. In fase di registrazione si può provare l'identità attraverso il canale digitale senza interruzioni del supporto dell'informazione e ciò consente di attivare ed utilizzare rapidamente l'applicazione. Il mobile payment è possibile sia online che offline e rappresenta una soluzione promettente per l'intero settore dell'eCommerce.

### 4.4.7 eBanking

L'eBanking diventa sempre più importante. Secondo l'Ufficio federale di statistica, nel 2015 oltre il 49% della popolazione si è avvalsa delle possibilità offerte dall'eBanking [1]. Anche in questo caso la registrazione e l'accesso sicuri al portale sono obbligatori ai fini di una gestione operativa affidabile. Un'eID riconosciuta a livello statale al livello di garanzia Oro o Platino potrebbe sostituire le soluzioni proprietarie delle banche e quindi dare grossi risparmi nel medio periodo.

### 4.4.8 Documenti elettronici

I documenti ufficiali elettronici, o eDocument, sono una soluzione più del futuro, anche se già alcune aziende [43] [44] li offrono in via sperimentale. Si tratta quasi dell'equivalente elettronico di un documento ufficiale materiale, come il passaporto, la carta d'identità o il permesso di condurre.

I documenti elettronici possono essere utilizzati per provare la propria identità quando si incontra fisicamente una parte facente affidamento sulla certificazione, ad esempio per provare la propria età presso un punto vendita o anche in occasione di un controllo dell'identità. Il titolare visualizza sul display di un idoneo dispositivo di supporto un'immagine leggibile del documento elettronico, che può essere verificata con un'idonea applicazione di lettura via IdP. Questo contribuisce a creare un legame concettuale tra l'eID elettronica e i documenti tradizionali.

Ovviamente non sono semplicemente „immagini" di documenti quelle che si controllano nel caso dei documenti elettronici: dietro ci sono le procedure e i meccanismi di sicurezza di una classica eID riconosciuta a livello statale. Le funzioni aggiuntive necessarie per i documenti elettronici possono però essere attuate dagli IdP e dalle parti facenti affidamento sulla certificazione in modo poco dispendioso.

### 4.4.9 Firme elettroniche

Con la revisione della legge federale sulla firma elettronica (FiEle) [45] è possibile offrire online le firme elettroniche come „servizio fiduciario". Il titolare di un'eID riconosciuta a livello statale può quindi registrarsi online presso un prestatore ed avvalersi direttamente del servizio, ad es. per firme elettroniche qualificate basate su server. Visto che l'eID riconosciuta a livello statale è disponibile al livello di garanzia necessario, è superfluo un colloquio preliminare col prestatore del servizio di firma e questo fa risparmiare tempo e denaro.

### 4.4.10 Abbonamenti

Visto che la pianificata eID riconosciuta a livello statale, a partire dal livello di garanzia Oro, consente anche di trasmettere l'immagine del volto garantita a livello statale (foto del documento), si possono ordinare online anche i documenti che richiedono una fotografia. Ciò potrebbe risultare interessante, ad esempio, per i prestatori di servizi nel campo dei trasporti pubblici ma anche in ambito turistico. I titolari di eID non dovranno quindi presentarsi ad uno

sportello ma potranno acquistare online i documenti con foto di cui necessitano e riceverli a casa, ad esempio, per posta o tramite una app.

All'eID potrebbero essere collegate funzioni aggiuntive mediante una mobility app. Per la registrazione e l'accesso si può usare l'eID ed acquistare e certificare abbonamenti e biglietti online attraverso la mobility app, risparmiando sui costi legati all'emissione a parte di abbonamenti o biglietti.

### 4.4.11 Sharing economy

La sharing economy, altrimenti detta collaborative economy [46], è in continua crescita e ha ancora grandi potenzialità. La collaborative economy (car sharing, flat sharing, piattaforme freelance ecc.) spesso richiede l'identificazione sicura della controparte. Questa esigenza può essere soddisfatta con un'eID riconosciuta a livello statale ai diversi livelli di garanzia.

### 4.4.12 Cloud computing

Come la virtualizzazione, il cloud computing promette vantaggi economici rispetto ai sistemi tradizionali. Con il cloud computing, i sistemi TIC possono essere utilizzati in modo molto più efficiente rispetto ai sistemi individuali, consentendo di pianificare ed utilizzare le risorse TIC in modo sostenibile. Per proteggersi da accessi non autorizzati ai dati nel cloud, si possono usare le eID in combinazione con procedure crittografiche.

### 4.4.13 Social Media

Anche se le persone possono essere presenti sui Social Media con uno pseudonimo, vi sono delle applicazioni, come ad esempio i forum con particolari regole per i membri, che richiedono una registrazione affidabile. I forum destinati a bambini e ragazzi, per esempio, devono essere "protetti" nei confronti degli adulti. Con un'eID riconosciuta a livello statale questo è possibile e molto semplice, perché si può fornire con l'eID una prova certa della propria età.

# 5 Protezione delle informazioni e dei dati

## 5.1 Introduzione

La protezione delle informazioni e dei dati e la sicurezza delle TIC in generale sono importanti per la fiducia nell'eID riconosciuta a livello statale. Attualmente il comportamento dei consumatori sul mercato indica però anche che la semplicità d'uso di una soluzione è decisiva affinché sia accettata. L'industria sta compiendo grossi sforzi per mettere sul mercato dispositivi sicuri ma semplici da usare per gli utenti, che siano idonei anche come supporto dell'eID (ad es. cellulari con il Trusted Execution Environment [47]). Si tratta quindi di trovare il giusto equilibrio tra la sicurezza e la semplicità d'uso.

Questo piano presuppone una suddivisione dei compiti tra Stato e mercato, partendo dall'assunto che vi sia, implicitamente, una fiducia di fondo nei servizi identitari forniti dal mercato. Anche se la sicurezza di tutte le componenti, dei sistemi e delle organizzazioni coinvolte nell'ambiente eID è importante, lo Stato non può implementare misure di sicurezza contro ogni minaccia nell'ambiente eID nel suo complesso e risponderne. Un IdP riconosciuto a livello statale, ad esempio, può rilevare ed amministrare, oltre ai dati di identificazione personale, anche altri attributi di fonti diverse. La responsabilità deve essere però a carico dell'IdP stesso.

Sulla base della legge federale sulla protezione dei dati (LPD), dell'ordinanza sulla protezione delle informazioni della Confederazione (ordinanza sulla protezione delle informazioni, OPrI), dell'ordinanza concernente l'informatica e la telecomunicazione nell'Amministrazione federale (OIAF), le istruzioni del Consiglio federale sulla sicurezza dell'informatica nell'Amministrazione e le linee direttrici sulla sicurezza TIC nell'Amministrazione federale, andranno quindi definiti rischi e minacce nell'ambiente eID e si attueranno le misure necessarie. Allo scopo si effettuano per i sistemi coinvolti un'analisi del bisogno di protezione (incl. RINA) e piani SIPD e si attua quanto previsto dalla protezione di base TIC.

Con la creazione di una base legislativa formale per le eID riconosciute a livello statale andranno emanate direttive integrative sulla sicurezza e la protezione dei dati per le organizzazioni coinvolte e i sistemi tecnici.

## 5.2 Identificatore personale univoco

Nell'ambiente eID, l'identificatore personale univoco è molto importante per l'integrità dei dati – qui intesa come la corretta attribuzione alla persona dei dati di identificazione personale – e per la sicurezza dell'eID. L'UCC[31] ha già raggiunto questo obiettivo nel campo delle assicurazioni sociali, creando l'UPI („Unique Person Identification", NAVS13) e può così garantire un corretto svolgimento delle operazioni.

Da un lato, gli IPU possono essere usati al bisogno come identificatori settoriali, mediante una funzionale unidirezionale o anche un'attribuzione tabellare, come già avviene nel caso del numero elettronico del paziente, memorizzato presso l'UCC assieme al NAVS13.

Riteniamo che un IPU, contrariamente all'opinione talvolta espressa, non diminuisca la protezione dei dati personali. Al contrario: riduce il rischio di scambi o incoerenze dei dati di

[31] L'Ufficio centrale di compensazione UCC (UCC) è una divisione principale dell'Amministrazione federale delle finanze. Gestisce il servizio „UCC-UPI", che attribuisce alle persone fisiche il NAVS13, nonché un "organismo di compensazione" per la correzione dei dati.

identificazione personale, che potrebbero danneggiare la persona. Inoltre un IPU evita che si debbano rivelare, perché l'identificazione sia univoca, altri dati di identificazione personale come cognome, nome e data di nascita, che di solito sono altrimenti necessari e che chiunque può direttamente associare nella vita di ogni giorno ad una persona fisica.

## 5.3 Bisogno di protezione

L'analisi del bisogno di protezione mostra come i sistemi di eID riconosciuti a livello statale elaborino, in conformità con la LPD, i dati che possono essere particolarmente degni di protezione nel caso specifico, segnatamente nel caso in cui, dalla foto di una persona, trasmessa al livello di garanzia Oro e Platino, si possono derivare informazioni sulla razza o l'appartenenza religiosa o le condizioni di salute della persona.

In base all'OPrl, i dati di identificazione personale devono essere classificati non come segreti o confidenziali ma ad uso interno. Per quanto concerne invece la disponibilità dell'infrastruttura confederale, non vi sono esigenze più restrittive in materia di integrità e tracciabilità. Visto che la Confederazione, secondo questo piano, acquisirà per i propri portali servizi IAM dagli IdP riconosciuti a livello statale e che questi potranno essere rilevanti anche per il BCM a seconda del portale, in base a RINA vanno prese misure di sicurezza speciali, che sono inserite anche nella legislazione.

## 5.4 Oggetti da proteggere

Nell'ottica della protezione dei dati, la persona è l'oggetto da proteggere e la tecnologia il rischio. Dal punto di vista della sicurezza delle TIC, la tecnologia è l'oggetto da proteggere e la persona il rischio. La priorità nel definire le misure di protezione nel primo caso va dal diritto all'organizzazione alla tecnologia, e nel secondo esattamente il contrario.

La figura sottostante fornisce un'idea di massima degli oggetti da proteggere dei sistemi di eID riconosciuti a livello statale, per i quali vanno definite misure in relazione alla protezione dei dati e della sicurezza delle TIC (legenda in basso):

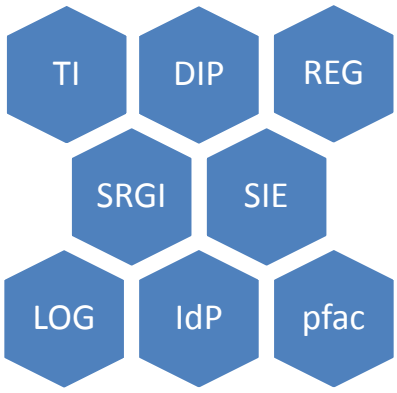



Figura 16: Oggetti da proteggere

| Abbr. | Dettagli |
|---|---|
| TI | Titolare di un'eID riconosciuta a livello statale, inclusa l'infrastruttura che utilizza come smartphone, tablet o PC. |

| Abbr. | Dettagli |
|---|---|
| REG | Registri delle persone che a livello confederale contengono dati di identificazione personale (Infostar, ISA, SIMIC, UCC-UPI), inclusi il personale e i sistemi tecnici. |
| DIP | Singolo record di dati con dati di identificazione personale come cognome, nome, data di nascita ecc. |
| LOG | Dati di protocollo sulla trasmissione di dati di identificazione personale e l'utilizzo di eID riconosciute a livello statale che vengono (obbligatoriamente) raccolti dagli enti coinvolti. |
| SRGI | Servizio di riconoscimento per i gestori dell'identità elettronica inclusi il personale e i sistemi tecnici. |
| SIE | Servizio svizzero per l'identità elettronica inclusi il personale e i sistemi tecnici. |
| IdP | Prestatore di servizi identitari inclusi il personale e i sistemi tecnici, utilizzati per l'emissione di un'eID riconosciuta a livello statale |
| pfac | Parti facenti affidamento sulla certificazione, inclusi il personale e i sistemi tecnici, coinvolte nell'utilizzo di un'eID riconosciuta a livello statale. |

Tabella 7: Legenda degli oggetti da proteggere

## 5.5 Rischi

Dalle minacce e dai punti di debolezza nascono dei rischi, che possono causare un danno. Un rischio è la probabilità che una minaccia si realizzi, moltiplicato per il danno potenziale. Le minacce per la sicurezza TIC sono ad esempio atti intenzionali di autori di reati interni o esterni, la forza maggiore, il guasto tecnico e le carenze nei comportamenti delle persone, come la negligenza o l'errore. Le minacce per la sicurezza dei dati sono ad esempio norme giuridiche insufficienti, atti intenzionali di autori di reati esterni ed interni e malfunzionamenti dei sistemi TIC.

I maggiori rischi per i sistemi di eID riconosciuti a livello statale sono:

| Abbr. | Rischio |
|---|---|
| TI | Violazione dell'obbligo di diligenza e abuso dell'identità<br>Anche le eID riconosciute a livello statale devono essere utilizzate secondo le direttive e con la necessaria cautela. Una violazione dell'obbligo di diligenza sarebbe, ad es., annotare il PIN su un'eID o rinunciare a qualsiasi scanner antivirus. Un abuso dell'identità sarebbe l'utilizzo della propria eID da parte di terzi, ad es. perché se ne è concesso loro l'uso (ad es. il convivente). |
| REG | Furto di dati<br>I dati presenti nei registri delle persone presso la Confederazione devono essere particolarmente protetti contro il furto di dati in massa e, nel singolo caso, la falsificazione dei dati. |
| DIP | Falsificazione di dati<br>La falsificazione di un record di dati con dati di identificazione personale può causare un danno. |

| Abbr. | Rischio |
|---|---|
| LOG | Abuso di dati<br>Quando si usano le TIC, tra cui anche le eID, ne derivano dei dati di protocollo che possono essere utilizzati. Questi dati di protocollo devono essere protetti da usi abusivi, come ad es. la creazione non autorizzata di profili. |
| SRGI | Violazione dell'obbligo di diligenza<br>Il riconoscimento e la vigilanza sugli IdP devono avvenire con la necessaria diligenza e indipendenza. Questo richiede che SIE elabori con cura profili di protezione. |
| SIE | Il furto di dati e la falsificazione di dati, mancata conoscenza della sicurezza TIC<br>I dati elaborati dal SIE devono essere protetti dal furto e dalla falsificazione. Per furto di dati si intende anche la trasmissione illecita di dati di identificazione personale ad un IdP. I profili di protezione predisposti dal SIE per il riconoscimento dei sistemi di eID devono essere idonei rispetto alle tecnologie e alle minacce attuali. |
| IdP | Furto di dati<br>I sistemi di eID degli IdP riconosciuti a livello statale devono essere protetti in particolare dal furto di dati in massa e, nel caso singolo, dalla falsificazione di dati. Per falsificazione di dati s'intende anche un malfunzionamento tecnico dell'eID o la scorretta registrazione di una persona. |
| pfac | Furto di dati e abuso di dati<br>I processi tecnici ed organizzativi presso la pfac devono consentire un uso senza errori di un'eID riconosciuta a livello statale. Un errore sarebbe, ad es., un'autenticazione non svolta correttamente. I dati presso la pfac devono essere protetti, in particolare, contro il furto di dati in massa e l'abuso di dati. |

Tabella 8: Principali rischi

Costituiscono altri rischi di ordine generale:

| Abbr. | Rischio |
|---|---|
| NUL | Nessun prestatore di servizi identitari<br>Se nessun prestatore di eID riconosciute a livello statale si afferma sul mercato, viene meno la pianificata suddivisione dei compiti tra Stato e mercato. Visto però che deve essere comunque introdotta un'eID riconosciuta a livello statale, dovrà esserci una soluzione di riserva. |
| FIN | Monopolio di un prestatore di servizi identitari<br>Il piano si basa sul presupposto che nell'ambiente eID si affermino più prestatori di eID statali e che si crei quindi concorrenza tra loro. Se non si sviluppa una concorrenza, bisogna evitare che i prezzi per le eID riconosciute a livello statale si sviluppino in modo scorretto. |
| CAT | Concatenazione di incidenti<br>Ad un'eID riconosciuta a livello statale partecipano numerosi sistemi singoli (come Infostar, ISA, IdP ecc.) che devono essere collegati a livello organizzativo e tecnico. Bisogna impedire che il guasto di un sottosistema faccia cadere anche gli altri. |

| Abbr. | Rischio |
|---|---|
| PCO | Perdita di controllo dei sistemi di eID riconosciuti a livello statale<br>Il controllo dei sistemi di eID riconosciuti a livello statale da parte di enti stranieri non sarebbe politicamente sostenibile. Devono essere „in mano“ alla Svizzera. |
| SPIO | Spionaggio dei sistemi di eID riconosciuti a livello statale<br>Le eID riconosciute a livello statale non dispongono, in quanto tali, oltre ai dati di identificazione personale, di altre caratteristiche di una persona. In particolare, non forniscono informazioni su appartenenze associative, funzioni, opinioni politiche e capacità delle persone.<br>Le eID possono però essere usate per procurarsi tali informazioni, in particolare nel caso di un abuso di identità. |

Tabella 9: Altri rischi

Un’analisi approfondita del rischio in base alle direttive dell’"Handbuch Risikomanagement Bund vom 29. April 2013" viene svolta nel quadro dell’elaborazione del piano dettagliato e delle disposizioni esecutive della legge sull’eID.

## 5.6 Misure di sicurezza

Sulla base dell’analisi del bisogno di protezione (capitolo 5.3**Fehler! Verweisquelle konnte nicht gefunden werden.**), dell’elenco degli oggetti da proteggere (capitolo 5.4) e anche dei rischi (capitolo 0), si riportano di seguito le principali misure di sicurezza da intraprendere per i sistemi di eID riconosciuti a livello statale:

| Abbr. | Misure di sicurezza |
|---|---|
| TI | Contro la violazione dell’obbligo di diligenza e l’abuso di identità<br>Direttive giuridiche (ad es. trattamento, obbligo di segnalazione); informazione attiva dei titolari. |
| REG | Contro il furto di dati<br>Nessuna misura aggiuntiva. Già oggi i registri delle persone sono gestiti conformemente alle direttive della Confederazione. |
| DIP | Contro la falsificazione di dati<br>Introduzione coerente di un identificatore personale univoco; firma dei dati di identificazione personale. |
| LOG | Contro l’abuso di dati<br>Direttive giuridiche (ad es. divieto del commercio dei profili); audit nel quadro del riconoscimento e della vigilanza. |
| SRGI | Contro la violazione dell’obbligo di diligenza<br>Processi controllati (event. certificazione ISO27000); controllo di sicurezza relativo alle persone. |

| Abbr. | Misure di sicurezza |
|---|---|
| SIE | Contro il furto di dati e la falsificazione dei dati, mancata conoscenza della sicurezza TIC<br>Dati di identificazione personale aggiornati; processi controllati (event. certificazione ISO27000); controllo di sicurezza relativo alle persone; firma digitale; canale di comunicazione sicuro; minimizzazione dei dati; liste di blocco (che riportano ad es. i titolari deceduti); coerente formazione continua e collaborazione con specialisti della sicurezza TIC. |
| IdP | Contro il furto di dati<br>Dati di identificazione personale aggiornati; utilizzo di un identificatore personale univoco; direttive giuridiche (ad es. profili di protezione secondo ISO/IEC 15408, tenuta dei dati in Svizzera, responsabilità, termini di cancellazione, liste di blocco); riconoscimento statale e vigilanza; direttive per il riconoscimento aggiornate a livello tecnologico; processi controllati (event. certificazione ISO 27000); controllo di sicurezza relativo alle persone. |
| pfac | Contro il furto di dati e l'abuso di dati<br>Direttive giuridiche (ad es. responsabilità, direttive per la tutela dei dati di identificazione personale); trasmissione controllata dei dati di identificazione personale dall'IdP (ad es. il NAVS13 sulla base di una white list). |
| NUL | Contro la mancanza di prestatori di servizi identitari<br>Condizioni quadro interessanti per gli IdP; soluzione di riserva (emissione di un'eID da parte della Confederazione). |
| FIN | Contro un monopolio dei prestatori<br>Condizioni quadro interessanti per gli IdP; direttive giuridiche sui prezzi. |
| CAT | Contro la concatenazione di incidenti<br>Collegamento lasco dei sistemi; analisi del rischio e BCM; responsabilità regolamentate. |
| PCO | Contro la perdita di controllo sui sistemi di eID riconosciuti a livello statale<br>Sistemi user-centered (ad. es consenso espresso per la trasmissione di dati di identificazione personale); direttive giuridiche e criteri d'idoneità per la sicurezza („Diritto e foro svizzeri, „Elaborazione dati in Svizzera", „Nessun obbligo di rivelare dati"); responsabilità regolamentate. |
| SPIO | Contro lo spionaggio di sistemi di eID riconosciuti a livello statale<br>Direttive giuridiche (ad es. minimizzazione dei dati, divieto di creazione di profili, termini di cancellazione); criteri d'idoneità per la sicurezza („Nessun obbligo di rivelare dati") |

Tabella 10: Misure di sicurezza

# 6 Legislazione

## 6.1 Aspetti generali

La creazione di un quadro giuridico trasparente è finalizzata al conseguimento dei seguenti obiettivi:

- riduzione o prevenzione di abusi d'identità e falsificazioni dell'identità nel mondo digitale;
- promozione di comunicazioni elettroniche sicure tra privati e con le autorità e
- interoperabilità e continuità dei sistemi di eID all'interno della Svizzera e con l'UE (notifica).

Le disposizioni sono sancite dalla legge sull'eID, che deve essere ancora stilata, dalle relative disposizioni esecutive e dai necessari standard e comprendono le direttive giuridiche, organizzative e tecniche concernenti

- i contenuti, il rilascio, il funzionamento, l'amministrazione, il ritiro e l'impiego di eID riconosciute a livello statale;
- il riconoscimento a livello statale degli IdP e la vigilanza sugli IdP riconosciuti nonché sui loro sistemi di eID;
- l'interfaccia per la trasmissione agli IdP dei dati statali di identificazione personale;
- l'interoperabilità dei sistemi di eID.

La regolamentazione nel suo complesso deve essere configurata in modo tale da consentire che vi sia una base di fiducia per un ambiente sostenibile per le eID, su cui fondare l'ulteriore sviluppo dei mercati digitali. Laddove possibile ed opportuno, ci si baserà sugli standard internazionali o sulle direttive già consolidate sul mercato. Nell'ambiente tecnico delle eID, che è dinamico, è sicuramente opportuno regolamentare i dettagli tecnici ed organizzativi a livello di disposizioni esecutive. La legge definirà quindi solo gli obiettivi delle categorie di eID, qui chiamati livelli di garanzia. Il Consiglio federale dovrà poter decidere l'impostazione tecnica ed organizzativa, ivi incluse le limitazioni concernenti l'inoltro di attributi (ad es. il NAVS13) a determinate parti facenti affidamento sulla certificazione. La legge dovrà invece regolamentare le conseguenze in caso di abuso da parte degli enti coinvolti, ad es. potrà essere possibile revocare l'autorizzazione ad un IdP riconosciuto.

Saranno sostanzialmente le parti facenti affidamento sulla certificazione a definire quale livello di garanzia considerare per quale tipo di applicazione. Per il vote électronique si potrà scegliere un livello di garanzia dell'eID diverso rispetto a quanto prescritto per le applicazioni eHealth o a quanto necessario per l'eEducation.

## 6.2 Rapporto con altre leggi

Nell'ambito dei lavori concernenti l'attività legislativa, si verificano e documentano nel dettaglio i punti di contatto con altre leggi. Eventualmente verranno effettuati anche degli adeguamenti nel quadro della „modifica di altri atti normativi". Si auspicano regole chiare in materia di responsabilità dell'IdP e/o di servizi di certificazione.

# 7 Allegato

## 7.1 Definizioni concettuali

Nel contesto del piano 2016 concernente l'eID e quindi anche per il disegno di legge (legge federale sulle unità d'identificazione elettronica riconosciute) utilizziamo una serie di termini il cui significato viene qui definito e contestualizzato a livello semantico e logico. Le sezioni che seguono spiegano i termini utilizzati per quanto necessario, senza riportare tutti i dettagli del discorso scientifico.

### A. Concetti fondamentali

Il concetto fondamentale di identità è estremamente sfaccettato ed è stato e viene analizzato nei suoi tanti significati a livello filosofico, psicologico, giuridico e tecnico. Una buona visione d'insieme è stata offerta, ad esempio, dalla Network of Excellence europea FIDIS [48]. Nel contesto del processo legislativo, il concetto di identità viene usato in un'accezione più specifica, giuridica e tecnica, come ad esempio da parte del NIST [49] e dell'UE [2]. Il nostro schema per la sua definizione si basa sul modello di informazione degli standard eCH [50][7][51].

### 1. Entità, insieme di entità ed attributi

In questo approccio, il punto di partenza è la prospettiva esterna, dalla posizione di un'amministrazione[32], rispetto ad un complesso di unità materiali o immateriali del mondo reale, denominate **entità**. L'insieme delle entità rilevanti è definito dal contesto amministrativo e viene chiamato **insieme di entità**[33]. Un'**entità,** dal punto di vista e nel contesto dell'amministrazione, avrà una serie di caratteristiche, che da essa possono essere stabilite con una certa sicurezza e che quindi rappresentano un'entità come record di **attributi** in un sistema informativo dell'amministrazione.

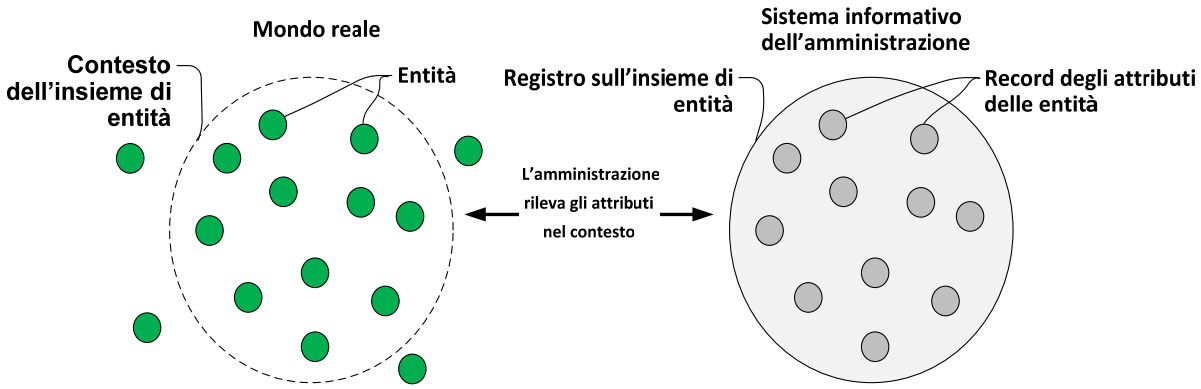



Figura 17: Attributi come caratteristiche dell'entità rilevanti per l'amministratore

Un attributo è composto dal **nome dell'attributo**, dal **valore dell'attributo** ed eventualmente da altri metadati come ad esempio una tipizzazione dei dati o una data di validità. Il nome definisce il significato semantico dell'attributo e con esso il campo dei possibili valori degli attributi. Il valore dell'attributo è il risultato della definizione degli attributi per una singola entità.

---

[32] L'amministrazione è un'istanza che amministra le entità e può attribuire loro ruoli o diritti, tipicamente una parte facente affidamento sulla certificazione, un gestore dell'identità elettronica o un'organizzazione statale.

[33] Negli standard eCH [7] [51] [50] l'entità viene intesa solo come persona e definita *soggetto*. L'insieme di entità e la relativa amministrazione corrispondono a *spazio dei nomi* e *risorsa.*

Implicitamente, al valore dell'attributo è associata anche la sicurezza con la quale si è definito un valore dell'attributo e sulla quale si basa la fiducia dell'amministrazione nella correttezza dell'assegnazione. La fiducia dell'amministrazione deriva dalla forza del collegamento della caratteristica all'entità, dalla garanzia che il corrispondente valore dell'attributo è stato rilevato correttamente, ovvero dall'affidabilità della fonte dal quale è stato acquisito l'attributo, e dal tempo trascorso dalla definizione dell'attributo. Così, ad esempio, la determinazione dell'autenticità di una determinata carta SIM sarà molto sicura, mentre il collegamento del cellulare come supporto della carta SIM alla persona non sarà molto forte. D'altra parte, una caratteristica biometrica è legata stabilmente alla persona ma nella misurazione permane una certa insicurezza sul fatto che il valore dell'attributo riscontrato sia stato rilevato correttamente. A seconda del contesto, la conseguente fiducia dell'amministrazione nella correttezza del valore dell'attributo e nella sua associazione ad una persona sarà sufficiente o meno. In generale, la fiducia nella definizione una tantum di un attributo diminuisce col tempo. Per questo di tanto in tanto gli attributi vengono rilevati di nuovo, per conservare l'intensità della fiducia.

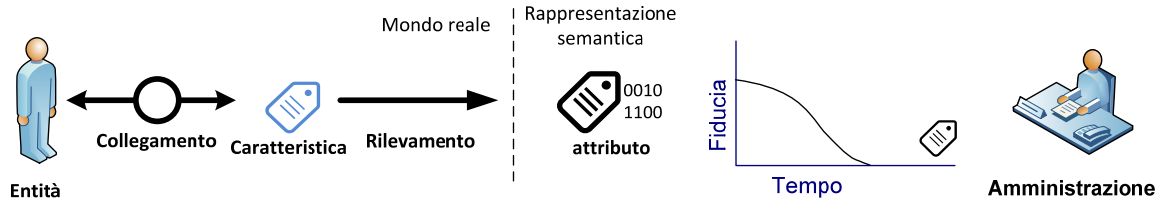



Figura 18: La sicurezza di un attributo e la fiducia in funzione del tempo

Se il valore di un attributo è definito con sufficiente sicurezza per tutte le entità, si può suddividere l'insieme di entità sottostante in sottoinsiemi, nei quali è assegnato lo stesso valore dell'attributo a tutte le entità [34]. Un esempio è la partizione di un insieme di persone in base all'attributo *data di nascita*. I singoli sottoinsiemi di questo partizionamento sono formati dalle persone che hanno la stessa data di nascita come valore dell'attributo. Attributi diversi e tra loro indipendenti o solo debolmente correlati portano a partizioni diverse dell'insieme di entità. Vi sono attributi che partizionano in modo forte un insieme di entità e altri che separano l'entità solo in misura limitata o non offrono informazioni nuove, come ad esempio l'anno di nascita, se la data di nascita è già nota.

## 2. Combinazione di attributi

Quindi, con più attributi il più possibile indipendenti, è possibile partizionare più volte un insieme di entità, o meglio l'insieme dei record di dati appartenenti alle entità con gli attributi rilevati. Solo quando nelle intersezioni di queste partizioni di attributi resta al massimo un solo record di attributi associato ad un'entità, è possibile distinguere tutte le entità nell'insieme di entità attraverso i record di dati che le rappresentano con gli attributi rilevati. In questo caso, la combinazione degli attributi accertati al corrispondente livello di sicurezza è **identificativa**. In generale, un record di attributi per un'entità è denominato **identità parziale**. Se gli attributi sono identificativi, si tratta di un'identità parziale identificativa.

Qualora in un'identità parziale vi siano solo attributi le cui intersezioni non separano tutte le

[34] Formalmente una definizione di attributi è una rappresentazione dell'insieme di entità nello spazio dei valori degli attributi. Una partizione univoca dell'insieme di entità si ha solo quando è definito in modo univoco per ciascuna entità un valore dell'attributo al livello di garanzia richiesto. La partizione dell'insieme di entità risulta allora dalle preimmagini dei singoli valori degli attributi.

entità, permane un certo anonimato che corrisponde al sottoinsieme maggiore non separato. Ad esempio, con l'identità parziale *cognome* e *data di nascita* permane un certo anonimato nell'insieme di entità degli abitanti della Svizzera perché vi sono più persone con lo stesso cognome e la stessa data di nascita. Se c'è un singolo attributo che già risolve completamente l'anonimato, lo si chiama **identificatore[35].**

La figura 19 offre una rappresentazione simbolica di A) un insieme di entità con le singole entità (rappresentate dai loro record di attributi) e B) una partizione di tale insieme mediante un attributo nominale e il sottoinsieme definito da un determinato valore dell'attributo. C) è la combinazione di attributi (intersezioni di partizioni di un'identità parziale). Un singolo attributo che separa tutte le entità nell'insieme di entità è D) un identificatore.

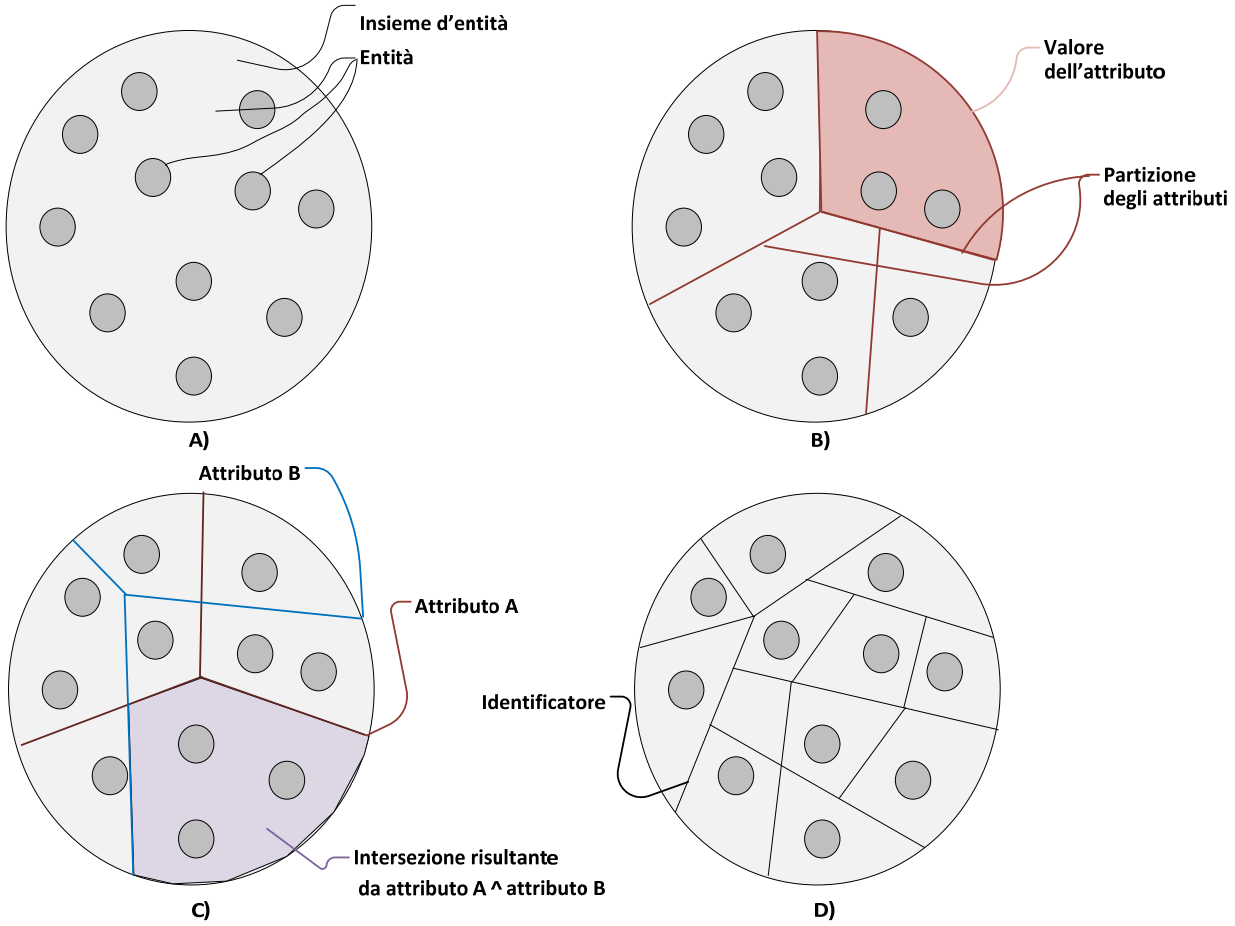



Figura 19: Record di dati di insiemi di entità ed identità parziali.

Spesso un identificatore viene assegnato da un'amministrazione ad un insieme di entità e può essere utilizzato come attributo pienamente identificativo da altri amministratori, nel cui contesto d'interesse siano rilevanti sottoinsiemi dell'insieme di entità più ampio. Tra gli abitanti della Svizzera, ad esempio, è un identificatore di questo tipo il NAVS13, assegnato dall'UCC alle persone in Svizzera e poi usato come identificatore da diverse istanze.

[35] Un'identità parziale identificativa come rappresentazione di un'entità sotto forma di attributi con un identificatore viene definita *eIdentity* negli standard eCH. Spesso però il termine eIdentity viene utilizzato con significati semantici diversi. Per questo preferiamo il termine ‚identità parziale identificativa'.

## 3. Classi di insiemi di entità

Sulla base del quadro giuridico, le entità possono essere suddivise in soggetti giuridici ed oggetti giuridici. **I soggetti giuridici** sono portatori di diritti e doveri. Invece gli **oggetti giuridici** sono beni di cui un soggetto giuridico dispone e che può rivendicare per sé. I soggetti giuridici sono le **persone fisiche** (esseri umani) e le **persone giuridiche** (ad es. le imprese o le istituzioni). Gli oggetti giuridici sono **beni materiali** (ad es. immobili o beni mobili) e **beni immateriali** (ad es. brevetti, diritti d'autore, crediti pecuniari ma anche software).

Anche se, in linea di principio, l'identificazione elettronica nel contesto dell'Internet of things (IoT) è rilevante per ogni tipo di entità, la legge sull'eID si limita, in linea col mandato, ai soggetti giuridici costituiti dalle persone (fisiche). Di conseguenza nella discussione ci si concentrerà da ora in poi sulle *persone fisiche*, che costituiscono nel contesto dell'eID svizzera gli insiemi di entità rilevanti.

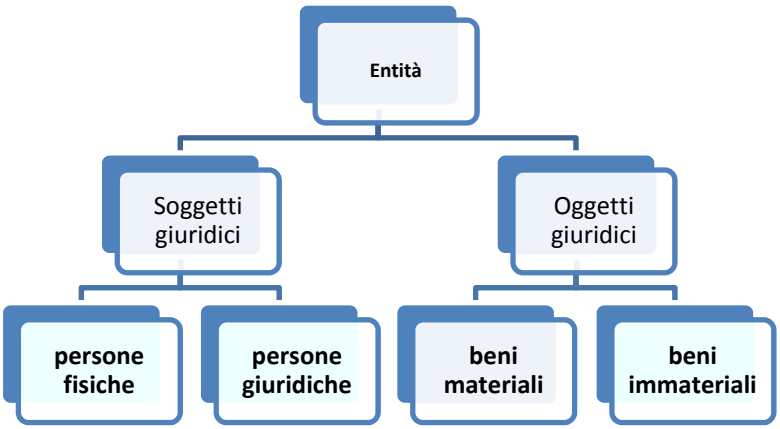



Figura 20: Categorizzazione delle entità in soggetti ed oggetti giuridici.

## 4. Persona – base di persone, ambiente eID

Ogni persona appartiene, in base alle sue attività sociali ed economiche, ad insiemi di entità specifici del contesto, che chiameremo **basi di persone**, mutuando il termine dalle basi di clienti che costituiscono la clientela[36]. Una **persona** può essere il cittadino di uno Stato, il collaboratore di un'azienda, il cliente di un negozio, il membro di un partito, di un club o di altri gruppi. Tutti questi gruppi sono accomunati dal fatto che la base di persone è definita da una serie di regole (una legge, un contratto, statuti ecc.) ed è amministrata dall'organizzazione che definisce il contesto. Se l'organizzazione è uno Stato e le regole sono definite dalla Costituzione, dalle leggi e da regole di applicazione, chiamiamo la base di persone così definita **popolazione.** Per una certa popolazione, il complesso di tutte le persone e delle istanze amministratrici, che all'interno della popolazione definiscono tali basi di persone che dipendono dal contesto, viene denominato **ambiente dell'identità** o **ambiente eID**.

## 5. Identificatore personale, dati di identificazione personale

In uno specifico contesto, una persona è definita in modo univoco da un'identità parziale ad un determinato livello di sicurezza. Un attributo, che identifica di per sé tutte le persone in una base di persone, è un **identificatore personale**. Se tale identificatore si riferisce all'intera popolazione di uno Stato, lo chiamiamo **identificatore personale univoco (IPU)**. Il NAVS13 è

[36] Una base di persone è definita stabilmente in un determinato momento dall'insieme dei record di dati delle identità parziali che la rappresentano presso l'amministrazione. Nel corso del tempo i record di dati per le persone possono essere rilevati ex novo o cancellati. La base di persone si sviluppa di conseguenza.

un esempio di attributo che identifica la popolazione rilevata dall'UCC e che quindi è un IPU.

Gli attributi rilevati e gestiti dallo Stato vengono denominati **dati di identificazione personale (DIP)**. Attraverso i dati di identificazione personale è possibile identificare in modo univoco una persona tra la popolazione. Basta nella maggior parte dei casi una piccola parte di tali dati, come ad esempio il *cognome*, il *nome* e la *data di nascita*, che di fatto in Svizzera è identificativa, come identità parziale[37].

Se per una popolazione, come base di persone definita a livello statale, è definito un IPU, è possibile derivare da tale IPU diversi identificatori personali per ogni base di persone subordinata (identificatori settoriali) o persino limitarne la durata (identificatori transitori). Gli identificatori derivati possono poi servire ad impedire un'identificazione, per motivi di protezione dei dati, in modo trasversale rispetto a diverse basi di persone subordinate. I sistemi di identificatori derivati devono essere amministrati o perlomeno sorvegliati dall'amministrazione della base di persone statale, perché solo questa istanza può sciogliere l'anonimato relativo tra basi di persone con identificatori derivati in modo diverso.

## 6. Identità di una persona

L'**identità** di una persona è una generalizzazione idealizzata delle identità parziali di una persona. In linea di principio, è composta da tutti gli attributi che si potrebbero assegnare in tutti i possibili contesti e per i quali, complessivamente, si ha sufficiente fiducia che al momento della determinazione essi descrivano esattamente la persona giusta. Nel contesto di un ambiente eID con dati dell'identità rilevati a livello statale per l'intera popolazione, l'identità viene spesso usata come sinonimo di identità parziale rilevata a livello statale con i dati di identificazione personale, più precisamente denominata **identità civile** o **statale**.

## 7. Classi di attributi

Bisogna distinguere tra gli attributi che vengono assegnati dall'amministrazione di una base di persone alle persone, quelli che la persona possiede come caratteristica personale indipendentemente da un insieme di regole e quelli che le sono associati, spesso per tutta la vita, da una regolamentazione statale superiore che definisce la popolazione e l'identità civile delle persone.

i. Attributi assegnati

Si tratta degli attributi di una persona che in linea di principio sono pubblicamente noti ma che dipendono dal contesto della base di persone, come ad esempio la tessera di un'associazione, il codice cliente presso una parte facente affidamento sulla certificazione, il numero personale, la procura di una società, la user-id per l'accesso ad un servizio ecc. Servono ad identificare, in relazione al contesto, i membri rilevati nella base di persone e ad assegnare loro dei ruoli. Le organizzazioni professionali tengono per i propri soci dei registri delle persone, con questi attributi assegnati, come ad esempio la qualifica, le specializzazioni, gli accreditamenti, le autorizzazioni ecc. Tali attributi possono essere assegnati da tutte le organizzazioni amministratrici alle proprie basi di persone. Perlopiù integrano i dati di identificazione personale e spesso hanno un significato solo nel contesto specifico.

ii. Attributi personali come fattori di autenticazione

Si tratta degli attributi appartenenti alla persona, come ad esempio le caratteristiche biometriche, i dati segreti inventati o acquisiti come ad es. il codice PIN o il possesso di un tipo di strumento

[37] Il tasso di scambio con questi tre attributi nelle popolazioni svizzere è al livello di ppm.

personale, come potrebbe essere una smartcard personalizzata o un documento. Questi attributi sono sostanzialmente privati e possono essere rilevati e aggiunti ad un'identità parziale identificativa da parte di un'amministrazione solo col consenso e con il concorso della persona[38]. Servono in particolare per verificare l'autenticità di una persona. Per un'autenticazione, la persona rende noto l'attributo personale all'amministrazione della base di persone, che poi potrà effettuare una verifica della presenza dell'attributo personale. Gli attributi personali così rilevati sono perlopiù definiti verificabili solo all'interno della base di persone per la quale sono rilevati. Il rilevamento e la verifica possono avvenire anche in modo indiretto attraverso un dispositivo che rileva e verifica solo gli attributi personali originali e trasmette unicamente il risultato della verifica. Un autenticatore dell'eID è una realizzazione tipica di questo tipo di dispositivo. Nel caso dell'autenticatore dell'eID, l'identificatore e gli elementi di sicurezza dell'apparecchio fanno parte dell'identità parziale del titolare dell'autenticatore registrata presso l'amministrazione (IdP). Costituiscono altri esempi di tali apparecchi gli autenticatori distribuiti dalle banche, che rilevano la presenza della persona con il codice PIN o a livello biometrico e che generano un codice valido una tantum come conferma di una verifica andata a buon fine. Un attributo così assegnato rappresenta poi gli attributi personali sottesi.

Spesso gli attributi personali sono definiti anche **fattori di autenticazione** e suddivisi in tre categorie: **biometrici, basati sulle conoscenze** e **basati sul possesso**. Gli attributi a se stanti, che si basano su una caratteristica misurabile, come ad esempio le caratteristiche biometriche, perlopiù non sono utilizzabili come identificatori per le basi di persone più grandi, perché quasi sempre ci sono persone con valori degli attributi non distinguibili entro i limiti di precisione della misurazione e di sicurezza auspicata[39]. Per basi di persone più piccole e circoscritte a priori, gli attributi misurabili possono invece essere molto identificativi. Normalmente, però, servono a confermare un'identità parziale asserita, alla quale appartengono, con un ulteriore rilevamento e una verifica. Ad esempio, un'amministrazione verifica se la password che una persona inserisce al momento dell'accesso corrisponda alla password che ha registrato assieme allo user-id della persona. Oppure il poliziotto verifica visivamente se l'immagine del volto della persona coincida con quella dell'identità parziale presente sulla CID.

iii. Attributi dell'identificazione statale delle persone

La terza categoria è quella degli attributi che sono assegnati ad una persona in base alle regole statali e ad un processo di amministrazione statale dell'identità, per lo più direttamente fin dalla nascita[40] e che identificano l'individuo come identità civile nella totalità della popolazione. Questi dati di identificazione personale vengono gestiti nei registri statali delle persone. Costituiscono un esempio di attributi amministrati dallo Stato il *cognome, il nome, la data di nascita, il luogo di nascita* ecc. Nel contesto della discendenza, della località e della data di calendario, sono assegnati alla nascita ad una nuova entità *persona*, sono verificati ad ogni rilascio di documenti e sono adeguatamente contrassegnati alla morte. Ma anche la *nazionalità*, il *numero di passaporto* o i *dati dell'indirizzo* rientrano in questo tipo di attributi. Contrariamente alla maggior parte degli altri dati di identificazione personale, però, essi non sono necessariamente validi per tutta la vita o hanno persino una durata espressamente limitata.

---

[38] In ambito forense, il concorso della persona non è consapevole, ma richiede alla polizia, come istanza amministratrice, sforzi aggiuntivi significativi per collegare un'identità parziale identificativa agli attributi personali rilevati.

[39] Vi sono delle eccezioni: ad esempio l'immagine dell'iride di una persona come attributo identificativo all'interno della popolazione mondiale. Ciò vale anche per il DNA, con limitazioni in alcuni casi di gemelli.

[40] Vi sono naturalmente Stati che rilevano pochi dati di identificazione personale o non li rilevano affatto o persone che, per varie ragioni, cercano di interrompere il collegamento con i loro dati di identificazione personale e quindi con la loro identità civile. In tali casi, uno Stato può assegnare ad una persona nuovi dati di identificazione personale, che varranno all'interno della sua popolazione.

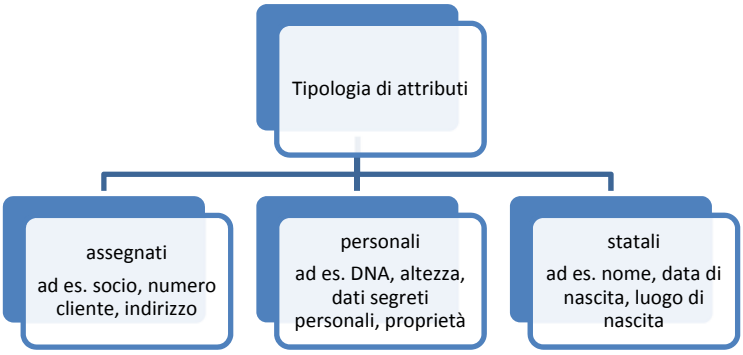



Figura 21: Categorie di attributi che possono essere rilevati nelle identità parziali

## 8. Gerarchia delle basi di persone

La base di persone definita da un amministratore nel suo contesto è nella maggior parte dei casi un sottoinsieme di una base di persone più vasta, per la quale sono già determinati o assegnati determinati attributi. Al vertice della gerarchia di basi di persone c'è l'intera popolazione di un ambiente d'identità, con i dati di identificazione personale dell'identità civile. Gli attributi dell'identità civile sono amministrati attraverso il registro dello stato civile e la fiducia nella corretta assegnazione degli attributi rilevati alla persona viene costantemente alimentata in Svizzera verificando ripetutamente i dati, in occasione del rilascio di ogni documento.

Gli attributi dei dati di identificazione personale vengono spesso rilevati anche in basi di persone subordinate, cosicché l'identità civile dello Stato e l'identità parziale nella base di persone subordinata definisce la stessa persona. Un'azienda di eCommerce, ad esempio, vorrà inserire la propria base di clienti, per quanto possibile, all'interno del quadro giuridico statale e pertanto rileverà, in particolare, gli attributi importanti per tale inserimento ed identificherà il cliente come persona con la sua identità civile nello Stato.

Le diverse basi di clienti possono sovrapporsi e vengono quindi in parte rappresentante da identità parziali identiche, con attributi identici. Il cognome e la data di nascita di una persona, ad esempio, in molti registri di basi di clienti fanno parte dell'identità parziale rilevata. Per motivi legati alla protezione dei dati, può risultare opportuno che le identità parziali di determinate basi di clienti non si sovrappongano, se possibile, in modo che tra loro non possano essere stabiliti dei collegamenti. Si potrebbe ottenere questo, ad esempio, riducendo gli attributi statali ad un identificatore personale settoriale derivato. L'IPU introdotto in questo piano è alla base di tale opzione. In ogni caso, un IPU offre una migliore tutela della sfera privata rispetto all'alternativa odierna, rappresentata da *cognome*, *nome e data di nascita*, che all'atto pratico può essere assegnata da chiunque ad una determinata persona, ad esempio attraverso i social network. La figura 22 mostra degli esempi di basi di dati diverse che inseriscono dati di identificazione personale nei propri record di attributi. Queste basi di dati in parte si sovrappongono e le loro identità parziali hanno come nucleo nella maggior parte dei casi attributi provenienti dai dati di identificazione personale dello Stato.

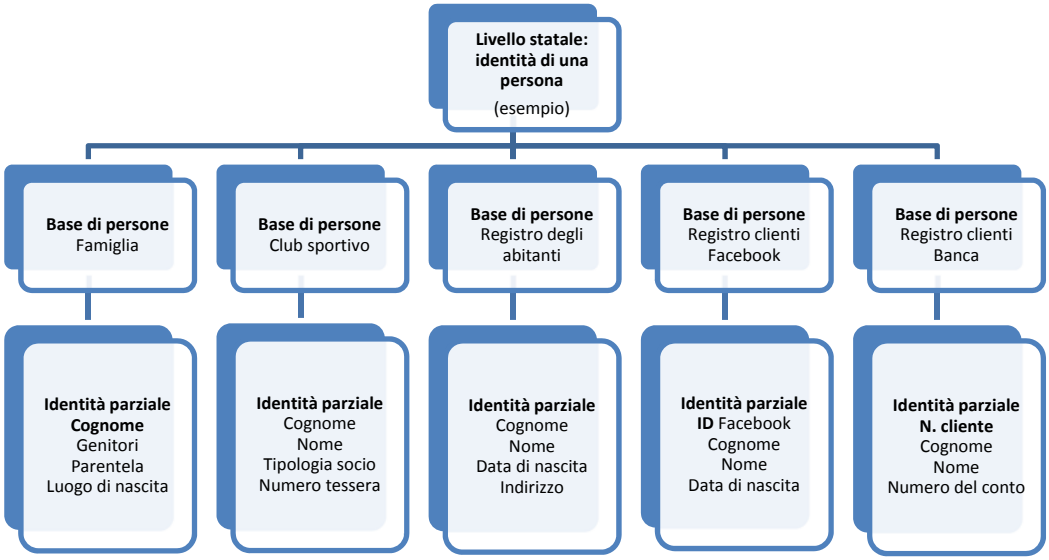



Figura 22: Esempi di diverse basi di dati

## B. Gestione dell'identità (IdM), sistema di gestione dell'identità (IdMS)

L'amministrazione dei dati dell'identità parziale di una base di persone, la loro tutela e manutenzione e l'esecuzione dell'identificazione e dell'autenticazione di singole persone sono definiti **gestione dell'identità (IdM)**. L'insieme degli strumenti per lo svolgimento di questi compiti è un **sistema di gestione dell'identità (IdMS)**. Il nucleo centrale di un IdMS è costituito dal registro delle persone con gli attributi dell'identità parziale rilevati e con processi definiti su come il registro viene curato, usato ed amministrato.

## 9. Ciclo di vita di un'identità parziale nell'IdM

Le fasi principali del ciclo di vita di un'identità parziale di una persona in un IdM sono la **registrazione** di una nuova persona, il **log-in** di una persona già rilevata e la **cancellazione** delle persone eliminate. L'attribuzione di ruoli e diritti non rientra più direttamente nei compiti fondamentali di un IdM ma spesso è comunque considerata parte di un sistema complessivo[41]. I registri degli abitanti, i registri delle imposte o i registri dello stato civile delle autorità, i registri dei clienti dei social media, delle aziende e delle banche ma anche gli elenchi di associati o gli elenchi scolastici sono esempi di IdMS.

### i. Registrazione di una persona nell'IdM

Per la registrazione di una nuova persona, la sua identità parziale deve essere creata nel contesto dell'organizzazione amministratrice oppure deve essere acquisita da un IdMS di una base di persone sovraordinata. Parte dell'identità parziale è un identificatore specifico del

[41] Spesso l'assegnazione di ruoli e quindi la concessione dei diritti di utilizzo dei servizi dell'organizzazione che gestisce un IdM, sono descritti come parte di un sistema complessivo chiamato sistema di Identity and Access Management (IAM). Ai fini di una corretta assegnazione dei ruoli, in base alle direttive dell'organizzazione, è necessaria prima una registrazione e, per l'esercizio di un ruolo, di un precedente accesso e quindi, necessariamente, della funzionalità di un IdM. L'amministrazione dei diritti di accesso sono però compiti aggiuntivi, che si possono riassumere in termini di access management. Per un design del sistema efficiente si raccomanda però di separare l'amministrazione dei diritti di accesso dall'IdM [7].

contesto, che rappresenta l'intera identità parziale della persona nella base di persone. Anche l'identificatore può essere definito specificatamente per l'IdMS o può essere acquisito da una base di persone sovraordinata.

In sede di registrazione si rileva l'identità parziale di una persona nell'IdMS al livello di garanzia rilevato definito dall'amministrazione. Ciò include almeno un attributo personale (segreto) come fattore di autenticazione referenziante (**collegamento**), che viene rilevato in modalità protetta o ridefinito assieme alla persona**.** Certi fattori di autenticazione, come ad esempio gli attributi biometrici, non devono essere rivelati ogni volta dalla persona ma possono essere forniti in forma indiretta in un dispositivo chiuso (autenticatore) come dati di riferimento[42]. Oltre ai fattori di autenticazione, sono rilevati altri attributi come ad es. determinati dati di identificazione personale che vengono comparati con gli attributi noti di una base di persone sovraordinata o già esistente (**identificazione iniziale)**. Perlopiù si tratta di attributi dell'identità civile. A registrazione avventa, il sistema viene attivato per l'utilizzo da parte della persona autorizzata.

ii. Login presso l'IdM

Se una persona registrata desidera in un secondo momento dimostrare la propria appartenenza ad una base di persone gestita dall'IdM, si connette con l'identificatore personale attribuitole o con il relativo pseudonimo (user-id ecc.) e in questo modo afferma di essere la persona giusta. L'IdMS eseguirà quindi un'**autenticazione** con i fattori di autenticazione rilevati, appartenenti all'identità parziale della persona asserita. Per l'autenticazione, la persona deve dimostrare di disporre in quel momento degli stessi fattori di autenticazione (attributi personali) che sono stati rilevati in sede di registrazione per la sua identità parziale. A seconda del numero di fattori indipendenti, che vengono verificati, si parla di uno, due o tre fattori di autenticazione.

iii. Cancellazione o blocco temporaneo

Se una persona non appartiene più alla base di persone amministrata nell'IdM, va cancellata l'identità parziale rilevata in sede di registrazione. Rientra nei compiti di un IdM anche il controllo del regolare utilizzo dell'identità parziale rilevata. Qualora vi siano dei dubbi circa il sussistere della sicurezza di un'identità parziale, l'utilizzo può essere bloccato in via transitoria o permanente.

## 10. Processi di base di un sistema di gestione dell'identità elettronica (IdMS)

L'identificazione e l'autenticazione di una persona sono i processi di base della gestione dell'identità. Il gestore di un IdM può eseguire tali processi anche come servizio a terzi che amministrano una base di persone subordinata.

La differenza tra i due processi può essere illustrata in modo semplice dall'esempio dell'accesso online ad un portale. Un utente effettua al primo contatto col portale una registrazione, con cui crea nell'IdMS del portale un'identità parziale. Essa contiene, in particolare, un identificatore scelto autonomamente (pseudonimo) o assegnato (user-id, numero di accesso). Al contempo deve rivelare all'IdMS almeno un attributo personale come parte dell'identità parziale (ad esempio una password personale), direttamente o attraverso un mezzo che funge da tramite (ad es. gli elementi di sicurezza attivati con il codice PIN di una carta SIM).

Quando, successivamente, la persona accede di nuovo al portale, si identifica con l'identificatore personale che nell'IdMS indica la sua identità parziale (**identificazione**). In questo modo asserisce di essere l'utente rilevato nell'IdMS. In una fase successiva lo prova

[42] Tale dispositivo fa parte dell'IdMS e fornisce con un grado definito di sicurezza il risultato della verifica dei fattori di autenticazione.

dimostrando l'attributo personale registrato nell'IdMS per la stessa identità parziale e così si autentica (**autenticazione**). Anche in questo caso, tale prova avviene direttamente o indirettamente, così come avvenuto per il rilevamento dell'attributo personale in sede di registrazione. L'autenticazione è quindi un processo in cui si ottiene la conferma dell'identità asserita di una persona. Rispetto all'identificazione iniziale con rilevamento dell'identità parziale nel quadro della registrazione, il log-in con identificazione mediante identificatore personale e con successiva autenticazione è un processo molto frequente.

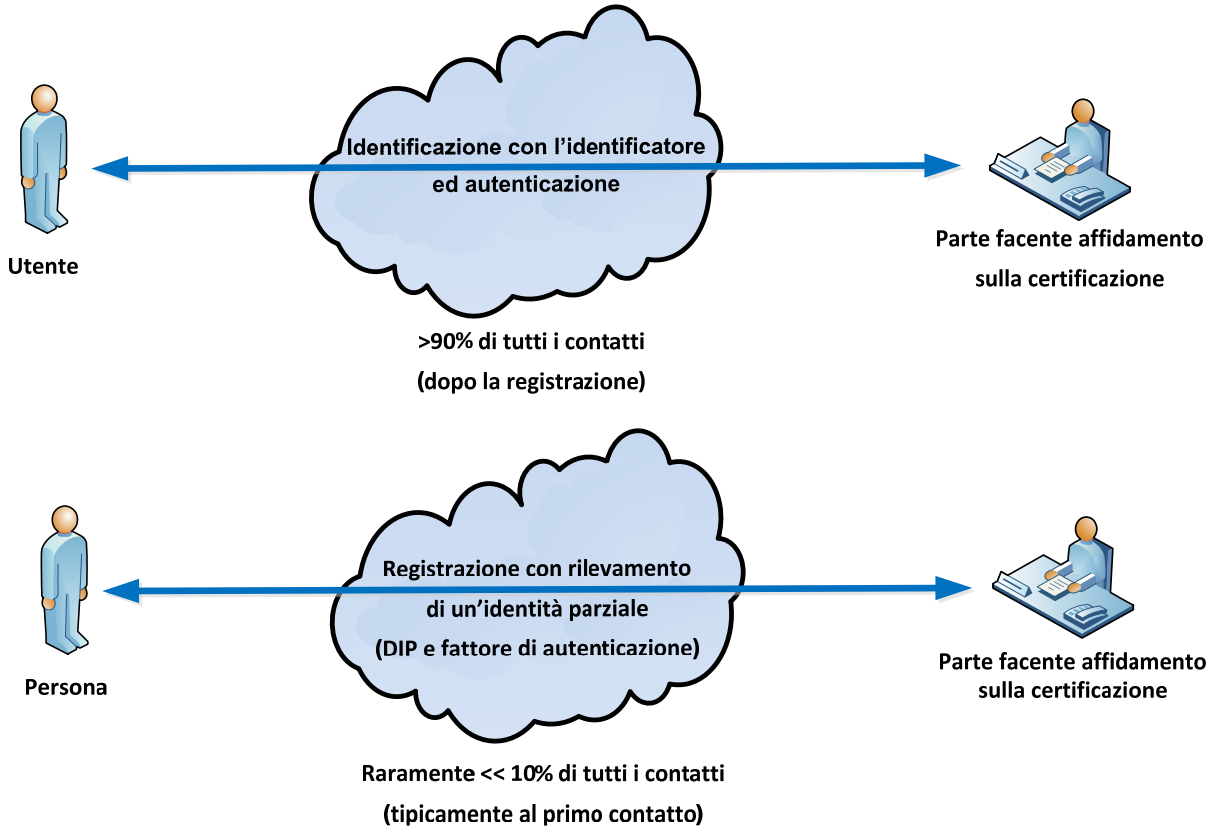



Figura 23: Frequenza del log-in rispetto alla registrazione.

## 11. Identificazione di una persona

La base dell'identificazione è il processo di determinazione ed attribuzione sicura di un'identità parziale ad una persona, nel cui ambito va rilevato anche ed almeno un attributo personale della persona come fattore di autenticazione. Attingendo ai dati statali di identificazione personale, l'identificazione può anche avvenire in relazione ad una base di persone (statale) sovraordinata. Una base di persone sovraordinata può fornire, nel quadro di un'identificazione, i dati corrispondenti direttamente alla base di persone subordinata. Questo avviene, ad esempio, quando in sede di identificazione viene richiesto di presentare un documento statale che contiene i principali dati di identificazione personale, come il *cognome, il nome, la data di nascita* ecc. Di norma, in un'identità parziale identificativa viene rilevato anche un identificatore personale univoco nella base di persone. Esso, nella base di persone, è quindi rappresentativo dell'intera identità parziale e può essere utilizzato per l'accesso online e quindi per l'identificazione. Se lo Stato definisce per tutte le basi di persone subordinate un identificatore personale univoco (IPU), esso può essere utilizzato per l'identificazione nella popolazione nel suo complesso e, per molte parti facenti affidamento sulla certificazione, come identificatore nei loro IdMS.

## 12. Autenticazione di una persona

L'autenticazione è il processo di verifica dell'appartenenza di un'identità parziale ad una persona, che la rivendica. Si verifica che gli attributi personali rilevati dell'identità parziale (fattori di autenticazione) effettivamente appartengano con un certo grado di sicurezza alla persona richiedente nella base di persone. La verifica avviene confrontando gli attributi personali, che la persona fornisce al momento dell'autenticazione, con i fattori di autenticazione rilevati durante la registrazione della persona. La forza di un'autenticazione dipende dal collegamento degli attributi personali verificati alla persona e dal numero e dal tipo di attributi verificati. La verifica dell'iride di una persona, ad esempio, avrà così una significatività molto maggiore per il collegamento rispetto alla richiesta di un codice PIN a quattro cifre o di una password. In base alle conoscenze attuali, l'iride è infatti assolutamente unico. Molte persone invece usano codici PIN o password semplici, spesso facili da indovinare. Ad ogni ulteriore fattore di autenticazione indipendente verificato aumenta la forza di un'autenticazione. La fiducia in un'autenticazione risulta dalla forza dell'autenticazione e dalla sicurezza che il processo non sia stato falsificato da un attacco. Un'autenticazione è un'istantanea, ad un determinato livello di garanzia, e la fiducia in essa diminuisce col tempo.

## 13. Gestione dell'identità elettronica

Se la gestione dell'identità avviene con mezzi elettronici, si parla di **gestione dell'identità elettronica (eIDM)** e del relativo **sistema elettronico di gestione dell'identità (sistema di eID)**. Nell'eIDM, oltre al ruolo della persona che viene identificata con un mezzo di identificazione elettronica (eID) e che viene denominata **titolare**, e al ruolo dell'amministrazione, che identifica ed autentica le persone e che è denominata **parte facente affidamento sulla certificazione (pfac)**, vi sono altri due ruoli: quello del **prestatore di servizi identitari (Identity Provider - IdP),** che rilascia l'eID e gestisce il sistema di eID e quello dello **Stato regolatore**. La parte facente affidamento sulla certificazione, che deve avere fiducia nell'IdP, incarica l'IdP di svolgere i processi di identificazione ed autenticazione elettronica delle persone. La pfac gestisce a tal fine un'applicazione informatica, chiamata **servizio facente affidamento sulla certificazione**, collegata al sistema di eID dell'IdP mediante un'interfaccia eID.

L'IdP gestisce un sistema di eID e rileva una base di persone il più ampia possibile, in modo che siano coperte le basi di persone di quante più pfac possibile e da poter quindi erogare servizi identitari per una vasta cerchia di clienti. Fa parte del sistema di eID un mezzo d'identificazione elettronica (eID), che l'IdP emette per tutte le persone registrate presso di lui e che gli consente di autenticare tutti i titolari di tale eID, ovunque nello spazio virtuale. Lo **Stato regolatore** definisce le condizioni quadro giuridiche, processuali, organizzative e tecniche nel cui ambito si svolge l'eIDM, con la collaborazione degli IdP e dei loro sistemi di eID. In particolare, definisce anche chi e come possa usare ed elaborare quali dati di identificazione personale. Definisce così la base di fiducia necessaria per lo sviluppo di un ambiente di eID funzionante.

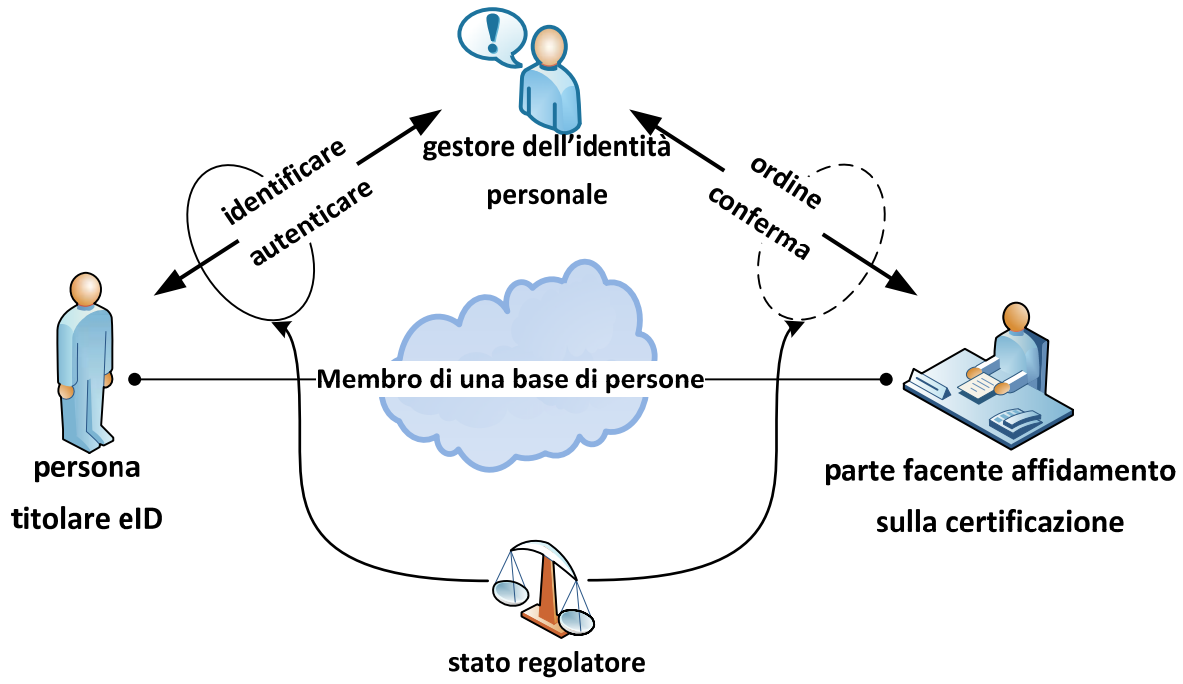



Figura 24: Distribuzione dei compiti nella gestione elettronica dell'identità

## 14. Mezzo d'identificazione elettronica (eID)

Un mezzo d'identificazione elettronica (eID) è un'unità elettronica materiale e/o immateriale (autenticatore)[43] che appartiene ad un sistema di eID e che viene usata, una volta completato il processo di registrazione, per l'identificazione e l'autenticazione di una persona nella base di persone del gestore del sistema di eID. L'eID ha delle interfacce che consentono una comunicazione sicura diretta con il server centrale del sistema di eID e contiene un identificatore, che viene assegnato al titolare in sede di registrazione. L'eID può contenere una funzione di autenticazione collegata in modo sicuro all'unità, con incapsulati dati di riferimento per i fattori di autenticazione personali del titolare. Tale funzione di autenticazione confronta, in sede di autenticazione, i fattori di autenticazione del titolare rilevati durante la registrazione con gli attributi personali della persona rilevati in quel momento e decide se coincidano e se quindi provengano dal titolare registrato. L'eID può contenere, oltre all'identificatore eventualmente dipendente dal collegamento, anche altri attributi identitari della persona o è connessa in modo univoco ad essi attraverso l'eIDM della base di persone dell'IdP.

i. Livello di garanzia di un'eID

I mezzi d'identificazione elettronica possono essere concepiti per livelli di garanzia diversi. Nel quadro del regolamento europeo eIDAS [2] si definiscono tre livelli di garanzia (basso, significativo, elevato), che corrispondono nella sostanza ai tre livelli di garanzia più alti degli standard ISO/IEC 29115 [52] e ai livelli di garanzia definiti dal NIST per l'autenticazione digitale [6]. Nel piano per l'eID svizzera, questi livelli di garanzia coincidono con i tre livelli di garanzia introdotti (Argento, Oro, Platino). Le eID dei tre livelli di garanzia si differenziano specialmente per il processo di rilascio in sede di registrazione di una persona, per la forza dell'autenticazione

[43] Un autenticatore è per il momento solo un'unità funzionale elettronica. Diventa un'eID dopo che, nel processo di registrazione, l'unità è collegata mediante la funzione di autenticazione ad una persona e i suoi dati identitari all'identificatore dell'unità.

della funzione di autenticazione integrata nell'eID, per i diversi record di dati di identificazione personale, trasmessi dallo Stato, e per il loro diverso grado di applicabilità.

ii. Le eID riconosciute a livello statale

La pianificata *legge federale sulle unità d'identificazione elettronica riconosciute (legge sull'eID)* costituisce il fondamento giuridico per il riconoscimento a livello statale di sistemi di eID ed eID offerti sul mercato da gestori dell'identità elettronica per le persone autorizzate della popolazione della Svizzera. Il riconoscimento statale si basa su un processo di riconoscimento col quale si verifica che gli aspetti della sicurezza tecnica ed organizzativa in base al livello di garanzia dell'eID, l'affidabilità dell'IdP rilasciante e l'interoperabilità del sistema di eID rispettino i criteri di riconoscimento stabiliti dalla legge.

iii. Interoperabilità

Con un'adeguata standardizzazione delle interfacce e dei protocolli, un'eID ovvero il relativo sistema di eID può essere utilizzato in linea di principio da tutte le parti facenti affidamento sulla certificazione per l'identificazione e l'autenticazione di titolari. A tal fine, i sistemi di eID devono essere interoperabili tra loro. Grazie all'interoperabilità, una parte facente affidamento sulla certificazione può ordinare l'identificazione o l'autenticazione di un titolare per tutte le eID di un determinato livello di garanzia, indipendentemente dall'IdP riconosciuto a livello statale che le ha rilasciate.

## 15. Interoperabilità in sistemi di eID

Basta realizzare l'interoperabilità tra tutti i gestori di sistemi di eID per ottenere un utilizzo trasparente di un'eID nell'intero ambiente eID. Un titolare con un'eID dell'IdP A può usarla presso una parte facente affidamento sulla certificazione, il cui servizio facente affidamento sulla certificazione è connesso al sistema di eID dell'IdP B. A tal fine accede con l'identificatore dell'eID al portale del servizio facente affidamento sulla certificazione, che inoltra la richiesta al sistema di eID del suo IdP B. Quest'ultimo determina la presenza degli elementi di sicurezza dell'eID nel sistema di eID dell'IdP A e invia l'ordine di autenticazione o identificazione al sistema di eID dell'IdP A, che o esegue da sé l'ordine e comunica il risultato attraverso lo stesso canale o fornisce gli elementi di sicurezza necessari all'IdP B, in modo che quest'ultimo possa eseguire l'ordine con l'eID del titolare. Tecnicamente, questo può avvenire in modo analogo al roaming della telefonia mobile. Affinché ciò funzioni, tutti i sistemi di eID riconosciuti a livello statale devono usare un unico sistema identificatore per le loro eID. Esso potrebbe consistere, ad esempio, in indirizzi IPv6, un sistema di e-mail standardizzato o un'altra forma di identificatori dell'eID definiti in modo unitario.

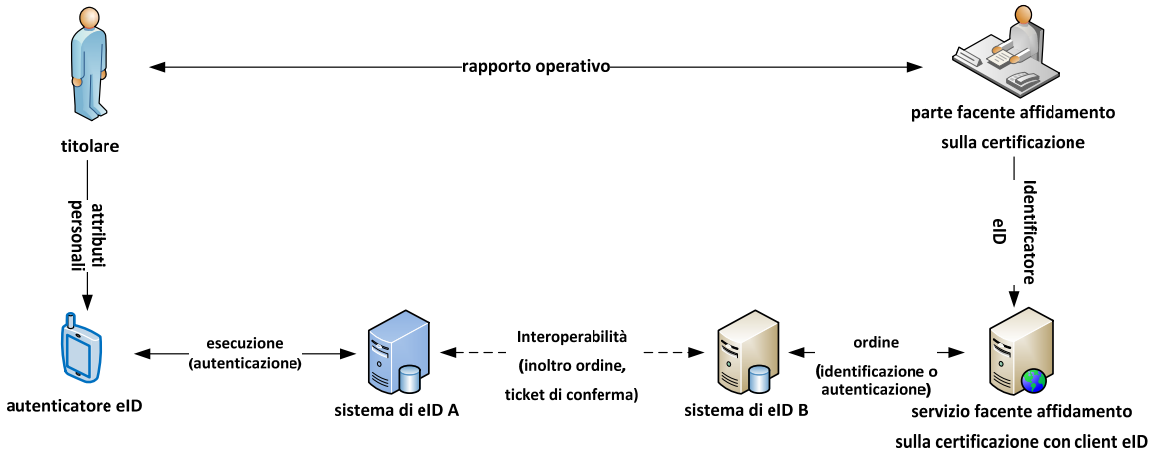



Figura 25: Iter di un'autenticazione o identificazione interoperabile

i. Utilizzo interoperabile di dati di identificazione personale

Sulla base dell'interoperabilità tra i sistemi di eID degli IdP riconosciuti a livello statale, ciascuna pfac, il cui servizio facente affidamento sulla certificazione sia connesso ad almeno un sistema di eID riconosciuto, può usare per la propria base di persone i meccanismi di identificazione ed autenticazione di tutte le eID riconosciute a livello statale. La pfac definisce il livello minimo di garanzia. Nel processo di registrazione, la pfac può, col consenso del titolare dell'eID, anche ricavare dati dell'identità da basi di persone sovraordinate degli IdP riconosciuti a livello statale e con essi gli attributi dell'identità civile registrati a livello statale. Si raggiunge così la completa interoperabilità dei dati di identificazione personale nell'ambiente eID svizzero per tutti i titolari di un'eID riconosciuta a livello statale. L'interoperabilità dell'identificazione e dell'autenticazione con incrocio degli attributi registrati a livello statale si estende per tutta la filiera: dallo Stato ai gestori dell'identità elettronica (IdP) fino alle parti facenti affidamento sulla certificazione (pfac).

Se una parte facente affidamento sulla certificazione registra una persona nella propria base di persone, la necessaria identificazione viene svolta dal servizio per l'identità e il risultato è comunicato alla pfac. Se l'eID è riconosciuta a livello statale, l'IdP, se così desidera il titolare, può trasmettere alla parte facente affidamento sulla certificazione anche dati di identificazione personale e in particolare anche un IPU derivato da registri statali. Anche nel caso in cui un titolare desideri accedere ad una pfac, l'IdP effettuerà la necessaria autenticazione da sé o la delegherà all'IdP competente e poi comunicherà il risultato alla pfac.

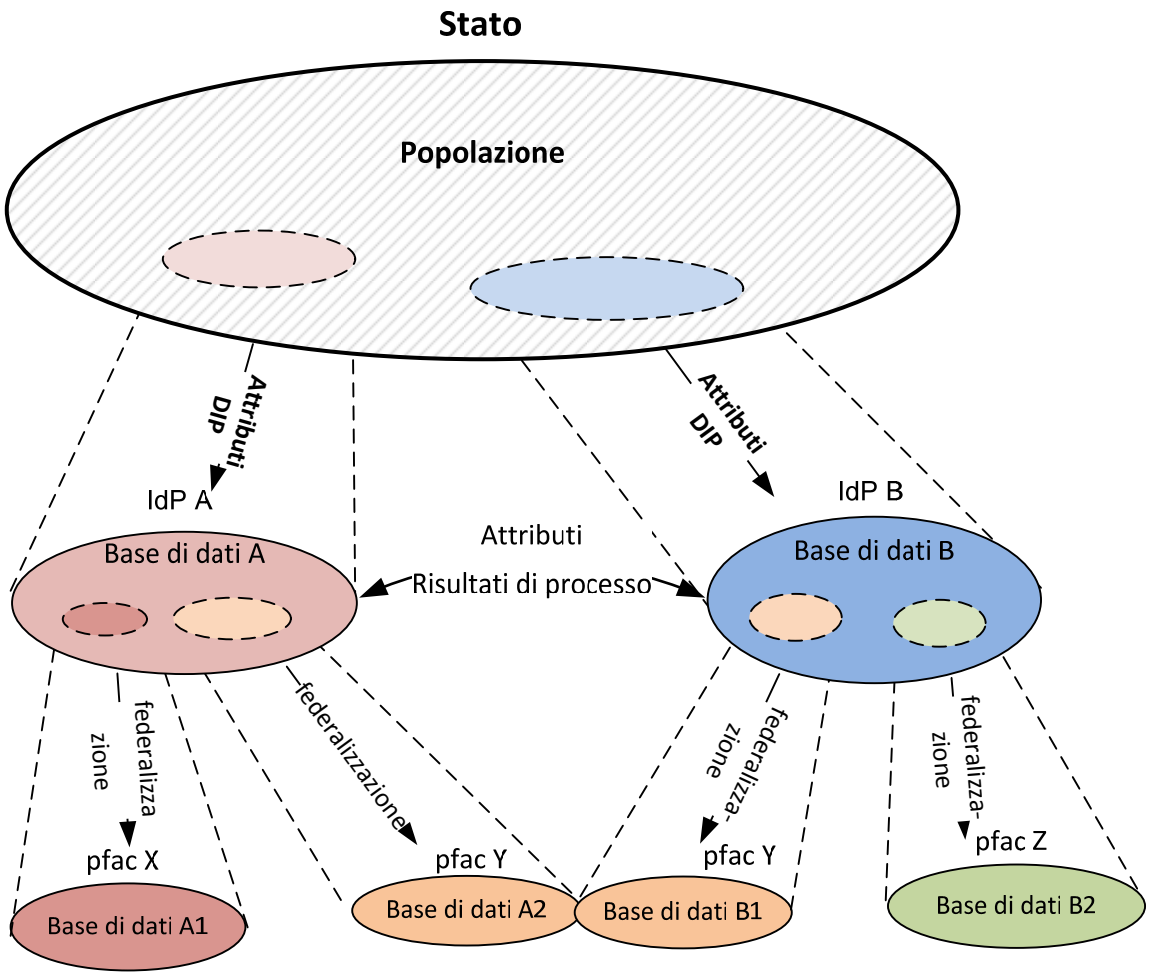



Figura 26: Filiera di trasmissione degli attributi

La figura illustra la filiera di trasmissione degli attributi da una base di persone sovraordinata a basi di persone subordinate, nell'esempio: Stato - gestori dell'identità elettronica (IdP) – parti facenti affidamento sulla certificazione (pfac). Al vertice c'è la base di persone dell'intera popolazione, con i dati di identificazione personale (DIP). Grazie all'interoperabilità, con l'aiuto di un'eID, tra gli IdP si trasmettono non solo gli attributi ma anche i risultati di processo dell'identificazione e dell'autenticazione.

## 16. Lo Stato come gestore degli attributi e il Servizio di riconoscimento per l'eIDM

La Confederazione si occupa dell'IdM statale per tutte le persone registrate in Svizzera che hanno un documento valido rilasciato dalle autorità svizzere. L'identificazione e l'autenticazione supportate dallo Stato con questi documenti sono possibili già oggi per tutte le basi di persone subordinate e i loro IdMS. Con l'introduzione di IdP riconosciuti a livello statale come prestatori di sistemi di eID, si consente anche la trasmissione elettronica di dati di identificazione personale da registri statali attraverso un servizio proxy statale. Gli IdP che offrono sistemi di eID riconosciuti a livello statale possono avvalersi di quest'offerta. Per l'ambito dei **sistemi di eID riconosciuti a livello statale,** la base di persone del livello più alto è l'intera popolazione svizzera, i cui dati di identificazione personale sono amministrati nei registri statali Infostar, ISA, ISR, UCC e SIMIC.

i. Servizio svizzero per l'identità elettronica (SIE)

Il SIE è un'unità amministrativa del DFGP che, col consenso esplicito del titolare di un'eID, trasmette un record di dati di identificazione personale a seconda del livello di garanzia dell'eID al sistema di eID dell'IdP. Ha accesso ai relativi registri delle persone della Svizzera (ISA, Infostar, SIMIC, UPI-UCC).

ii. Servizio di riconoscimento per i gestori dell'identità elettronica (SRGI)

Affinché un IdP possa gestire un sistema di eID riconosciuto a livello statale, deve eseguire un processo di riconoscimento per sé e per i propri sistemi di eID. Questo include la verifica dei requisiti di riconoscimento di natura tecnica, organizzativa e giuridica. In particolare, ciò comprende anche la verifica del rispetto degli standard e la presenza di interfacce per l'inserimento interoperabile del sistema di eID da riconoscere nell'ambiente eID svizzero.
Il SRGI è un'unità amministrativa in seno al DFF. Gli competono il riconoscimento a livello statale degli IdP e dei loro sistemi di eID nonché la vigilanza sul rispetto dei requisiti per tale riconoscimento.

## 7.2 Glossario

Sulla base dei termini e dei contesti sopra illustrati, si utilizzano per la legislazione e per il piano per un'eID riconosciuta a livello statale le seguenti definizioni.

| Termine | Abbr. | Definizione |
|---|---|---|
| Attivazione | | Attivazione di un'eID per la gestione da parte dell'IdP dopo il rilascio con registrazione del titolare. |
| Accesso | | Accesso / log-in di un titolare al sistema eIDM (o IAM) di una pfac o all'IdP con l'eID. |
| Servizio di riconoscimento per gestori dell'identità elettronica | SRGI | Vedi 3.3. |
| Attributo | | Caratteristica di un'entità definita nominalmente. Un attributo ha un nome dell'attributo, un valore dell'attributo ed altre caratteristiche, come ad esempio un tipo di dati o una data di validità. |
| Nome dell'attributo | | Nome semantico della caratteristica che viene rilevata come attributo. |
| Valore dell'attributo | | Valore stabilito di un attributo di un'entità specifica (persona). |
| Servizio attributi | | Servizio per la trasmissione di attributi identitari per persone rilevate nei registri del servizio. Gli IdP riconosciuti a livello statale agiscono da servizio attributi per i dati di identificazione personale, resi loro disponibili dal SIE. Anche il SIE è un servizio attributi. |
| Autenticatore | | Un'unità elettronica materiale e/o immateriale appartenente ad un sistema di eID. Ha interfacce che consentono una comunicazione diretta sicura con il server centrale del sistema di eID e contiene un identificatore che viene attribuito al titolare al momento della registrazione. Contiene una funzione di autenticazione, collegata in modo sicuro con l'unità, con dati di riferimento per i fattori di autenticazione personale del titolare. |
| Funzione di autenticazione | | Funzione di un'eID, che consente di rilevare attributi personali (fattori di autenticazione) del titolare e confrontarli con i valori memorizzati a livello locale. La funzione di autenticazione decide se un titolare sia la persona corretta. |
| Autenticazione<br>Autenticare | | Vedi allegato sezione 12. |
| Fattori di autenticazione | | Attributi personali che possono essere usati per l'autenticazione di una persona. Si distingue spesso tra tre categorie: biometrici, basati sulle conoscenze e basati sul possesso. |
| Popolazione | | Qui le persone rilevate ed amministrate nei registri statali nella giurisdizione di uno Stato. |
| Identificatore personale univoco | IPU | Identificatore attribuito in modo univoco dallo Stato alle persone della popolazione. Il NAVS13 è un IPU in Svizzera. |
| Gestione elettronica dell'identità | eIDM | Gestione dell'identità con sistemi digitali elettronici. |

| | | |
|---|---|---|
| Mezzo d'identificazione elettronica | eID | Autenticatore, assegnato ad un'identità parziale del titolare presso l'IdP, la cui funzione di autenticazione è inizializzata in modo tale da consentire l'autenticazione del titolare. |
| Sistema di gestione dell'identità elettronica | Sistema di eID | Sistema in cui l'eID viene rilasciata, gestita ed amministrata. |
| Interfacce elettroniche applicazioni e processi | Interfaccia eID | Componente standardizzata di sistemi di eID, che viene gestita presso i servizi che fanno affidamento sulla certificazione come interfaccia al sistema di eID. Garantisce moduli e formati unitari nell'utilizzo dell'eID. |
| Ambiente eID | | Insieme di tutte le istanze che impiegano l'eID per la popolazione di uno Stato o che contribuiscono alla loro gestione. |
| Entità | | Un'unità identificabile sulla base di determinati attributi. |
| Insieme di entità | | Insieme di unità a seconda del contesto. |
| Identificatore | | Designazione univoca di un'entità nel sistema informativo di un amministratore di identità parziali. |
| Attributi identitari | | Vedi attributi. |
| Attributi identitari identificativi | | Identità parziale con attributi che identificano in modo univoco un'entità all'interno di un insieme di entità. |
| Identificazione<br>Identificare | | Vedi allegato sezione 11. |
| Identità ambiente | | Vedi ambiente eID. |
| Identità,<br>identità civile | | Complesso degli attributi che si possono rilevare per una persona (entità). L'identità civile corrisponde agli attributi di una persona rilevati nei registri statali delle persone. |
| Gestore dell'identità elettronica<br>Identity Provider | IdP | Prestatore di servizi identitari che gestisce e/o utilizza un sistema di eID. |
| Gestione dell'identità | IdM | Vedi allegato capitolo B. |
| Sistema di gestione dell'identità | IdMS | Vedi allegato capitolo B. |
| Gestione dell'identità e dell'accesso | IAM | IdM con annessa amministrazione di ruoli e diritti per le persone rilevate nella base di persone. |
| Sistema di gestione dell'identità e dell'accesso | IAMS | Sistema elettronico per IAM. |
| Servizio identitario | | Con questo termine s'intende sempre qui un'autenticazione o un'identificazione con la trasmissione di dati di identificazione personale. |
| Disattivazione | | Inattivazione di un'eID nel sistema di eID di un IdP. |
| Titolare | | Persona alla quale è stata rilasciata da un IdP un'eID riconosciuta a livello statale. |
| Interoperabilità | | Rete di sistemi di eID che si riconoscono e fanno reciprocamente affidamento, con un livello di garanzia minimo definito. |
| Cancellazione | | Disattivazione definitiva di un'eID. |
| Persona fisica | | Persona che costituisce un soggetto che agisce |

| | | |
|---|---|---|
| | | autonomamente. |
| Identità parziale | | Set di dati con attributi concernenti un'entità. |
| Persona | | Soggetto giuridico, qui usato principalmente nel senso di persona fisica. |
| Identificatore personale | | Un nome definito in un contesto che designa in modo univoco, in quel contesto, una persona. |
| Dati di identificazione personale | DIP | Attributi dell'identità civile di una persona inseriti in registri di persone statali. I dati di identificazione personale sono qui limitati ad una parte di tali attributi, definita dalla legge. |
| Attributi personali | | Attributi utilizzabili per l'autenticazione di una persona, vedi fattori di autenticazione. |
| Base di persone | | Insieme di persone le cui identità parziali sono rilevate nell'IdM di un gestore. |
| Soggetto giuridico | | Portatore di diritti e doveri che agisce autonomamente; comprende le persone fisiche e giuridiche. |
| Registrazione | | Registrazione presso IdP:<br>collegamento di una persona ad un'eID, identificazione della persona da parte dell'IdP, trasmissione dei DIP della persona da parte del SIE all'IdP in occasione del rilascio di un'eID.<br>Registrazione presso la pfac:<br>primo accesso di un titolare presso una pfac, nel suo IdMS, con trasmissione dei dati di identificazione personale da parte dell'IdP, che ha rilasciato l'eID. |
| Servizio svizzero per l'identità elettronica | SIE | Vedi 3.2. |
| Livello di garanzia | | Vedi 2.6.1. |
| Supporto di un'eID | | Unità elettronica in cui è integrata un'eID. |
| Protezione della transazione | | Verifica degli accordi di una transazione. |
| Parte facente affidamento sulla certificazione | pfac | Persona fisica o giuridica o unità IDI che gestisce per la propria attività un servizio facente affidamento sulla certificazione. |
| Servizio che fa affidamento sulla certificazione | | Un'applicazione informatica che utilizza il servizio identitario del sistema di eID e predispone le necessarie interfacce tra la prestazione di servizio della pfac e il sistema di eID. |
| Attributi assegnati | | Attributi che dipendono dal contesto, assegnati ad una persona nella sua identità parziale nella base di persone di una pfac o IdP da questi ultimi. |

## 7.3 Riferimenti bibliografici

La bibliografia riporta innanzitutto i documenti citati e poi altre fonti di contenuti elaborati nel piano.


[1] Bundesamt für Statistik, «Informationsgesellschaft,» Schweizerische Eidgenossenschaft, 2016. [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04.html. [Consultato il giorno 20 Juli 2016].

[2] EU, «Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung),» 23. Juli 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&qid=1422521123960&from=EN. [Consultato il giorno 29. Oktober 2015].

[3] E. Kommission, «Technical Specifications and procedures for Assurance for eID,» in *2015/1502*, 2015.

[4] FIDO Alliance, «UAF Architectural Overview, Review Draft,» 09. Februar 2014. [Online]. Available: https://fidoalliance.org/specifications/download/. [Consultato il giorno 12. April 2015].

[5] Lindemann, R., FIDO Alliance and Nok Nok Labs Inc., «The evolution of authentication,» 2013. [Online]. Available: http://www.springer.com/cda/content/document/cda_downloaddocument/9783658033705-c1.pdf. [Consultato il giorno 12. April 2015].

[6] D. N. S. P. 800-63-3, «Digital Authentication Guideline,» 12 Mai 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3. [Consultato il giorno 15 Juni 2016].

[7] eCH, «eCH-0107 IAM Gestaltungsprinzipien v2.0,» 04. Dezember 2013. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0. [Consultato il giorno 12. April 2015].

[8] N. 8149, «Developing Trust Frameworks to Support Identity Federations,» NIST - National Institute of Standards and Technology; US DoC, 2016.

[9] Bundesamt für Gesundheit, «Bundesgesetz über das elektronische Patientendossier,» [Online]. Available: http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/index.html?lang=de. [Consultato il giorno 23 07 2016].

[10] Schweizer Parlament, «Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03,» 19. Dezember 2003. [Online]. Available: http://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Consultato il giorno 12. April 2015].

[11] eCH Verein, «eCH - E-Governement Standards,» [Online]. Available: http://www.ech.ch. [Consultato il giorno November 2015].

[12] J. Fromm e et al., «3-Jahre Online Ausweisfunktion – Lessons Learned,» *Fraunhofer Fokus,* Oktober 2013.

[13] Belgische Regierung, «Portal belgium.be - Online Dienste der Belgischen Behörden,» [Online]. Available: http://www.belgium.be/de/online_dienst/. [Consultato il giorno 12. April 2015].

[14] BRZ-Presseservice, «Handy-Signatur gräbt der Bürgerkarte langsam das Wasser ab (Seite 54),» 27. März 2014. [Online]. Available: https://www.brz.gv.at/presse/pressespiegel/Pressespiegel-2014-03.pdf. [Consultato il giorno 12. April 2015].

[15] International Civil Aviation Organisation (ICAO), «Document 9303,» [Online]. Available: http://www.icao.int/Security/mrtd/pages/Document9303.aspx. [Consultato il giorno 26 07 2016].

[16] Bundesministerium des Innern, «Personalausweis,» [Online]. Available: http://www.personalausweisportal.de/DE/Home/home_node.html. [Consultato il giorno 26 07 2016].

[17] Government Technology, «Louisiana Considers Electronic Driver's License,» [Online]. Available: http://www.govtech.com/state/Louisiana-Considers-Electronic-Drivers-License.html. [Consultato il giorno 26 07 2016].

[18] CNET, «The driver's license of the future is coming to your smartphone,» [Online]. Available: http://www.cnet.com/news/your-future-drivers-license-could-go-digital/. [Consultato il giorno 26 07 2016].

[19] Gemalto, C. Mesnard, «Trusted National Mobile ID Schemes,» in *Secure Document World Conference, London 2016*, London, 2016.

[20] H. Steier, «Uns blieb das Lachen im Hals stecken,» *20 Minuten,* vol. 22. September 2010; 11:14, n. Digital News, Sicherheit, p. http://www.20min.ch/digital/hardware/story/17220624, 2010.

[21] M. Quade e R. Wölfle, SuisseID in der Praxis - Grundlagen und Fallbeispiele zum elektronischen Identitätsnachweis der Schweiz, Basel: edition gesowip, 2010, p. 88.

[22] P. Müller, «Die SuisseID als Unterstützung für E-Voting, eine Analyse der Möglichkeiten und Handlungsoptionen,» Berner Fachhochschule, Wirtschaftsinformatik, Bern, 2011.

[23] S. Strauß e G. Aichholzer, «National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design. International Journal on Advances in Intelligent Systems,» pp. 12-23, Vol. 3, Nrs. 1&2 2010.

[24] Riedl, R., E-Government Institut Bern, BFH, «Von unterschiedlichen nationalen eID-Strategien zum einheitlichen europäischen Identitäts-raum – ein Ländervergleich,» 03. Juni 2014. [Online]. Available: http://e-government.adv.at/2014/pdf/2_1100_Riedl_eGovernmentKonferenz_20140603.pdf. [Consultato il giorno 12. April 2015].

[25] M. Horsch, «Die Open eCard App für mehr Transparenz, Vertrauen und Benutzerfreundlichkeit beim elektronischen Identitätsnachweis,» in *13. Deutscher IT-Sicherheitskongress des BSI*, Bonn, 2013.

[26] Nok Nok Labs Inc., «Four Barriers To Adabpt Strong Authentication,» 2013. [Online]. Available: https://www.noknok.com/sites/default/files/whitepapers/4barrierswhitepaper_0.pdf. [Consultato il giorno 12. April 2015].

[27] M. Richter, «Kriterien der Benutzerfreundlichkeit,» Philosophische Fakultät der Universität Zürich, http://www.michaelrichter.ch/literat_97.pdf, 1997.

[28] NIST, «National Strategy for Trusted Identities in Cyberspace (NSTIC),» [Online]. Available: http://www.nist.gov/nstic/index.html. [Consultato il giorno 26 07 2016].

[29] B. Fachhochschule, F. Wirtschaft e E.-G. Institut, «eID- Ökosystem Modell,» Juni 2015. [Online]. Available: https://www.egovernment.ch/index.php/download_file/force/271/3343/. [Consultato il giorno 8 August 2016].

[30] Bundesrat, «Strategie des Bundesrates für eine digitale Schweiz,» Schweizerische Eidgenossenschaft, 20. April 2016. [Online]. Available: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/strategie.html. [Consultato il giorno 15 Mai 2016].

[31] E-Government Schweiz, «E-Government-Strategie Schweiz,» 24. Januar 2007. [Online]. Available: http://www.egovernment.ch/egov/00833/00834/index.html?lang=de. [Consultato il giorno 12. April 2015].

[32] E-Government Schweiz, «Roadmap E-Government Schweiz,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00852/index.html?lang=de. [Consultato il giorno 12. April 2015].

[33] E-Government Schweiz, «Katalog priorisierter Vorhaben,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00847/index.html?lang=de. [Consultato il giorno 12. April 2015].

[34] Schweizerische Bundeskanzlei, «E-Demokratie und E-Partizipation,» 2011. [Online]. Available: http://intranet.bk.admin.ch/themen/06367/index.html?lang=de. [Consultato il giorno 08 05 2015].

[35] NSTIC- National Strategy for Trusted Identities in Cyberspace, «The Identity Ecosystem: Use Examples;,» [Online]. Available: http://www.nist.gov/nstic/identity-ecosystem.html [Zugriff am 13. April 2015].. [Consultato il giorno 13 April 2015].

[36] EU, «Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185252017&uri=CELEX:32015D0296. [Consultato il giorno 29 07 2017].

[37] EU, «Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185296675&uri=CELEX:32015R1501. [Consultato il giorno 29 07 2016].

[38] EU, «Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185318253&uri=CELEX:32015R1502. [Consultato il giorno 29 07 2016].

[39] EU, «Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185344281&uri=CELEX:32015D1984. [Consultato il giorno 29 07 2016].

[40] Zentrale Ausgleichsstelle, «Verteilter Clearingprozess,» [Online]. Available: http://www.zas.admin.ch/org/00721/00758/00911/index.html?lang=de. [Consultato il giorno 25 07 2016].

[41] Bundeskanzlei, «E-Demokratie und E-Partizipation,» [Online]. Available: https://www.bk.admin.ch/themen/06367/index.html?lang=de. [Consultato il giorno 22 07 2016].

[42] Bundeskanzlei, «Vote électronique,» [Online]. Available: https://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de. [Consultato il giorno 22 07 2016].

[43] Österreichische Staatsdruckerei, «MIA (My Identity App),» [Online]. Available: https://www.staatsdruckerei.at/produkte/identitaetsmanagement/mia-my-identity-app/. [Consultato il giorno 26 07 2016].

[44] MORPHO, «Electronic Driver License,» [Online]. Available: http://www.morpho.com/en/now-your-smartphone-could-be-your-drivers-license-too. [Consultato il giorno 26 07 2016].

[45] Bund, «Bundesgesetz über die elektronische Signatur, ZertES,» [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Consultato il giorno 24 07 2016].

[46] European Commission, «Collaborative economy,» [Online]. Available: http://ec.europa.eu/growth/single-market/strategy/collaborative-economy/. [Consultato il giorno 23 07 2016].

[47] «The Trusted Execution Environment, Delivering Enhanced Security at a lower cost to the mo-bile market,» Februar 2011. [Online]. Available: http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf. [Consultato il giorno 12. April 2015].

[48] K. R. e. a. (Eds), The Future of Identity in the Information Society, Berlin - Heidelberg: Springer-Verlag, 2009.

[49] NIST Hildegard Ferraiolo, Larry Feldman and Greg Witte, «NIST Special Publication 800-157 - Guidelines for Derived Personal Identity Verification (PIV) Credentials,» Dezember 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf. [Consultato il giorno 12. April 2015].

[50] eCH, «eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,» 04. September 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0171. [Consultato il giorno 13. April 2015].

[51] eCH, «eCH-0170 Qualitätsmodell für elektronische Identitäten,» 06. Juni 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170. [Consultato il giorno 12. April 2015].

[52] ISO, «ISO Standard 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework,» 27. März 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138. [Consultato il giorno 13. April 2015].

[53] D. Hühnlein, «Identitätsmanagement-eine visualisierte Begriffsbestimmung,» *Datenschutz und Datensicherheit, Heft 3,* p. 163, 2008.

[54] M. Jakobsson e S. Taveau, «The Case for Replacing Passwords with Biometrics,» 2012. [Online]. Available: http://mostconf.org/2012/papers/3.pdf. [Consultato il giorno 12. April 2015].

[55] J. Grant, «Digital Identity in 2019: a vibrant identity ecosystem,» 2014. [Online]. Available: http://secureidnews.com/news-item/digital-identity-in-2019-a-vibrant-identity-ecosystem/#. [Consultato il giorno 12. April 2014].

[56] M. Schröder e F. Morgner, «Abgeleitete Identitäten,» 2013. [Online]. Available: https://www.bundesdruckerei.de/sites/default/files/documents/2013/08/fachartikel_dud_abgeleitete_identitaeten.pdf. [Consultato il giorno 12 April 2015].

[57] Meister, Gisela, Giesecke & Devrient, «Abgeleitete Identitäten – ein Überblick,» 25. September 2014. [Online]. Available: http://www.cast-forum.de/workshops/programm/194. [Consultato il giorno 12. April 2015].

[58] Global Platform Inc., «A new model: The consumer-centric model and how it applies to the Mobile ecosystem,» März 2012. [Online]. Available: http://www.globalplatform.org/documents/Consumer_Centric_Model_White_PaperMar2012.pdf. [Consultato il giorno 12. April 2015].

[59] «OASIS - Advancing Open Standards for the Information Society,» [Online]. Available: https://www.oasis-open.org/. [Consultato il giorno 12. April 2015].

[60] OASIS, «OASIS - SAML Wiki,» [Online]. Available: https://wiki.oasis-open.org/security/FrontPage. [Consultato il giorno 12. April 2015].

[61] Schweizer Bundesrat, «Informationsgesellschaft in der Schweiz,» März 2012. [Online]. Available: http://www.bakom.admin.ch/themen/infosociety/. [Consultato il giorno 12. April 2015].

[62] EU, «STORK,» 2015. [Online]. Available: https://www.eid-stork.eu/. [Consultato il giorno 12. April 2015].

[63] Schweizer Bundesrat, «Bundesratsbeschluss zur Ausarbeitung eines Gesetzgebungspaketes zur Förderung des elektronischen Geschäftsverkehrs,» 19. Dezember 2012. [Online].

[64] SuisseID, «SuisseID,» 2015. [Online]. Available: http://www.suisseid.ch/de. [Consultato il giorno 12. April 2015].

[65] Mondinis Workshop, «Mondinis Study on Identity Management in eGovernment; Common Terminological Framework for Interoperable Electronic Identity Management; V2.01,» DG Information Society and Media; EU Commission, 23 November 2005. [Online]. Available: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf. [Consultato il giorno 13 April 2015].

[66] D. Miessler, «Daniel Miessler Blog; Security: Identification, Authentication, and Authorization,» [Online]. Available: https://danielmiessler.com/blog/security-identification-authentication-and-authorization/ . [Consultato il giorno 13 April 2015].

[67] G. Doe, «Difference Between Identification & Authentication;,» Demand Media; , [Online]. Available: http://science.opposingviews.com/difference-between-identification-authentication-3471.html . [Consultato il giorno 13 April 2015].

[68] I. 1. Standard, «Common Criteria for Information Technology Security Evaluation».

[69] R. Dholakia, «A question of Scale,» NokNok Labs, 2012.

[70] D. O'Shea, «Fido U2F & UAF Tutorial,» in *World e-ID Congress, Marseille 2014*, Marseille, 2014.

[71] Bundesversammlung, «Ausweisgesetz (AwG, SR 143.1),» 01 Jan 2013. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19994375/index.html. [Consultato il giorno 08 Mai 2015].

[72] SkIDentity, «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Consultato il giorno 09. Mai 2015].

[73] Verein eGov-Schweiz, «Bürgerdossier,» 2015. [Online]. Available: http://www.egov-schweiz.ch/media/archive2/eGov_Flyer_Buergerdossier_def.pdf. [Consultato il giorno 09. Mai 2105].

[74] E-Government Schweiz, «Identititätsverbund Schweiz (IDV Schweiz),» 2015. [Online]. Available: http://www.egovernment.ch/b206/index.html?lang=de. [Consultato il giorno 09. Mai 2015].

[75] «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Consultato il giorno 12. April 2015].

[76] H. STORCK 2.0, «STORK - Secure idenTity acrOss boRders linKed 2.0,» STORK 2.0 project group, [Online]. Available: https://www.eid-stork2.eu/. [Consultato il giorno 9 11 2015].

[77] Bundesamt für Statistik, «Nutzungszwecke,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=302#302. [Consultato il giorno 22 07 2016].

[78] Bundesamt für Statistik, «Nutzungshäufigkeit von Online-Fomularen,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=335#335. [Consultato il giorno 22 07 2016].

[79] Bundesamt für Statistik, «Nutzung des Internets,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/03/key/ind16.indicator.30106.160204.html. [Consultato il giorno 22 07 2016].

[80] FINMA, «FINMA ermöglicht Video- und Online-Identifizierung,» 21 12 2015. [Online]. Available: https://www.finma.ch/de/news/2015/12/20151221-mm-videoidentifizierung/. [Consultato il giorno 15 7 2016].

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Dipartimento federale di giustizia e polizia DFGP**

Berna, 23 febbraio 2017

Destinatari:
i Governi cantonali

**Legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID): indizione della procedura di consultazione**

Onorevoli Presidenti e Consiglieri,

il 22 febbraio 2017 il Consiglio federale ha incaricato il DFGP di indire una procedura di consultazione sulla legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID) presso i Cantoni, i partiti, le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna, le associazioni mantello nazionali dell'economia e le cerchie interessate.

La consultazione durerà fino al **29 maggio 2017.**

Per poter svolgere in rete anche transazioni complesse, i partner commerciali devono poter fare affidamento sull'identità della controparte. Un'eID consente loro di identificare le persone fisiche autorizzate a beneficiare di un servizio.

L'avamprogetto si fonda sulla ripartizione dei compiti tra Stato e mercato. Prevede che lo Stato possa autorizzare i fornitori di servizi identitari (IdP) privati o pubblici che soddisfano i pertinenti presupposti a rilasciare eID riconosciute a livello statale. Sempre secondo l'avamprogetto, le eID riconosciute possono essere rilasciate a persone la cui identità può essere confermata tramite i sistemi d'informazione dello Stato Infostar (il registro informatizzato dello stato civile), SIMIC (il sistema d'informazione centrale sulla migrazione), ISA (il sistema d'informazione sui documenti d'identità) e il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI).

Con la presente legge si crea un quadro giuridico e di standardizzazione per il riconoscimento di sistemi di eID e degli IdP strutturato in modo da consentire, successivamente, il reciproco riconoscimento dei sistemi di eID riconosciuti tra la Svizzera e l'UE o singoli Stati membri dell'UE. A tal scopo sarebbero necessari pertinenti accordi bilaterali.

Nell'ambito dell'eID riconosciuta a livello statale la Confederazione assume cinque compiti:
1. elabora e aggiorna le basi legali, creando in tal modo trasparenza e sicurezza;
2. definisce gli standard nonché i requisiti in materia di sicurezza e interoperabilità da rispettare per gestire un sistema di eID;

3. gestisce una piattaforma elettronica tramite la quale gli IdP riconosciuti possono ottenere dati d'identificazione personale tenuti dallo Stato;
4. riconosce gli IdP e i loro sistemi di eID; e
5. esercita la vigilanza sugli IdP riconosciuti e sui sistemi di eID.

La Confederazione assumerà questi compiti tramite due unità amministrative: il «Servizio svizzero delle identità elettroniche (Servizio delle identità)» e il «Servizio di riconoscimento per i fornitori di servizi identitari (Servizio di riconoscimento)».

Il progetto non avrà ripercussioni sul bilancio dato che i costi d'esercizio saranno coperti dagli emolumenti.

Vi invitiamo a prendere posizione in merito all'avamprogetto di legge e al rapporto esplicativo.

La documentazione per la consultazione è disponibile all'indirizzo Internet: https://www.admin.ch/ch/i/gg/pc/pendent.html.

Ai sensi della legge sui disabili (LDis; RS 151.3) ci adoperiamo per pubblicare documenti accessibili anche ai disabili. Vi invitiamo pertanto a trasmettere elettronicamente (**in formato PDF e Word**) i vostri pareri entro il suddetto termine al seguente indirizzo:

copiur@bj.admin.ch

Vi preghiamo di indicare le coordinate delle persone di contatto responsabili per il parere per eventuali domande.

Per maggiori informazioni potete contattare
Urs Paul Holenstein (tel. 058 463 53 36, urspaul.holenstein@bj.admin.ch) o
Sandra Eberle (tel. 058 465 47 77, sandra.eberle@bj.admin.ch).

Vi ringraziamo sin d'ora per la preziosa collaborazione e cogliamo l'occasione per porgervi, Signore e Signori Consiglieri di Stato, i migliori saluti.

Simonetta Sommaruga
Consigliera federale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Dipartimento federale di giustizia e polizia DFGP**

Berna, 23 febbraio 2017

Destinatari:
i partiti politici
le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna
le associazioni mantello nazionali dell'economia
le cerchie interessate

**Legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID): indizione della procedura di consultazione**

Gentili Signore e Signori,
il 22 febbraio 2017 il Consiglio federale ha incaricato il DFGP di indire una procedura di consultazione sulla legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID) presso i Cantoni, i partiti, le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna, le associazioni mantello nazionali dell'economia e le cerchie interessate.

La consultazione durerà fino al **29 maggio 2017.**

Per poter svolgere in rete anche transazioni complesse, i partner commerciali devono poter fare affidamento sull'identità della controparte. Un'eID consente loro di identificare le persone fisiche autorizzate a beneficiare di un servizio.

L'avamprogetto si fonda sulla ripartizione dei compiti tra Stato e mercato. Prevede che lo Stato possa autorizzare i fornitori di servizi identitari (IdP) privati o pubblici che soddisfano i pertinenti presupposti a rilasciare eID riconosciute a livello statale. Sempre secondo l'avamprogetto, le eID riconosciute possono essere rilasciate a persone la cui identità può essere confermata tramite i sistemi d'informazione dello Stato Infostar (il registro informatizzato dello stato civile), SIMIC (il sistema d'informazione centrale sulla migrazione), ISA (il sistema d'informazione sui documenti d'identità) e il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI).

Con la presente legge si crea un quadro giuridico e di standardizzazione per il riconoscimento di sistemi di eID e degli IdP strutturato in modo da consentire, successivamente, il reciproco riconoscimento dei sistemi di eID riconosciuti tra la Svizzera e l'UE o singoli Stati membri dell'UE. A tal scopo sarebbero necessari pertinenti accordi bilaterali.

Nell'ambito dell'eID riconosciuta a livello statale la Confederazione assume cinque compiti:
1. elabora e aggiorna le basi legali, creando in tal modo trasparenza e sicurezza;
2. definisce gli standard nonché i requisiti in materia di sicurezza e interoperabilità da rispettare per gestire un sistema di eID;

3. gestisce una piattaforma elettronica tramite la quale gli IdP riconosciuti possono ottenere dati d'identificazione personale tenuti dallo Stato;
4. riconosce gli IdP e i loro sistemi di eID; e
5. esercita la vigilanza sugli IdP riconosciuti e sui sistemi di eID.

La Confederazione assumerà questi compiti tramite due unità amministrative: il «Servizio svizzero delle identità elettroniche (Servizio delle identità)» e il «Servizio di riconoscimento per i fornitori di servizi identitari (Servizio di riconoscimento)».

Il progetto non avrà ripercussioni sul bilancio dato che i costi d'esercizio saranno coperti dagli emolumenti.

Vi invitiamo a prendere posizione in merito all'avamprogetto di legge e al rapporto esplicativo.

La documentazione per la consultazione è disponibile all'indirizzo Internet: https://www.admin.ch/ch/i/gg/pc/pendent.html.

Ai sensi della legge sui disabili (LDis; RS 151.3) ci adoperiamo per pubblicare documenti accessibili anche ai disabili. Vi invitiamo pertanto a trasmettere elettronicamente (**in formato PDF e Word**) i vostri pareri entro il suddetto termine al seguente indirizzo:

copiur@bj.admin.ch

Vi preghiamo di indicare le coordinate delle persone di contatto responsabili per il parere per eventuali domande.

Per maggiori informazioni potete contattare
Urs Paul Holenstein (tel. 058 463 53 36, urspaul.holenstein@bj.admin.ch) o
Sandra Eberle (tel. 058 465 47 77, sandra.eberle@bj.admin.ch).

Vi ringraziamo sin d'ora per la preziosa collaborazione e porgiamo distinti saluti.

Simonetta Sommaruga
Consigliera federale

# Liste der ständigen Vernehmlassungsadressaten
# Liste des destinataires consultés systématiquement
# Elenco dei destinatari permanenti della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)



Stand: 2.2.2017

1. Kantone / Cantons / Cantoni

| | |
|---|---|
| Staatskanzlei des Kantons Zürich | Neumühlequai 10<br>Postfach<br>8090 Zürich<br>staatskanzlei@sk.zh.ch |
| Staatskanzlei des Kantons Bern | Postgasse 68<br>3000 Bern 8<br>info@sta.be.ch |
| Staatskanzlei des Kantons Luzern | Bahnhofstrasse 15<br>6002 Luzern<br>staatskanzlei@lu.ch |
| Standeskanzlei des Kantons Uri | Rathausplatz 1<br>6460 Altdorf<br>ds.la@ur.ch |
| Staatskanzlei des Kantons Schwyz | Regierungsgebäude<br>Bahnhofstrasse 9<br>Postfach 1260<br>6431 Schwyz<br>stk@sz.ch |
| Staatskanzlei des Kantons Obwalden | Rathaus<br>6061 Sarnen<br>staatskanzlei@ow.ch |
| Staatskanzlei des Kantons Nidwalden | Dorfplatz 2<br>Postfach 1246<br>6371 Stans<br>staatskanzlei@nw.ch |
| Staatskanzlei des Kantons Glarus | Rathaus<br>8750 Glarus<br>staatskanzlei@gl.ch |
| Staatskanzlei des Kantons Zug | Seestrasse 2<br>Regierungsgebäude<br>am Postplatz<br>6300 Zug<br>info@zg.ch |
| Chancellerie d'Etat du Canton de Fribourg | Rue des Chanoines 17<br>1701 Fribourg<br>chancellerie@fr.ch<br>relations.exterieures@fr.ch |

| | |
|---|---|
| Staatskanzlei des Kantons Solothurn | Rathaus<br>Barfüssergasse 24<br>4509 Solothurn<br>kanzlei@sk.so.ch |
| Staatskanzlei des Kantons Basel-Stadt | Marktplatz 9<br>4001 Basel<br>staatskanzlei@bs.ch |
| Landeskanzlei des Kantons Basel-Landschaft | Regierungsgebäude<br>Rathausstrasse 2<br>4410 Liestal<br>landeskanzlei@bl.ch |
| Staatskanzlei des Kantons Schaffhausen | Beckenstube 7<br>8200 Schaffhausen<br>staatskanzlei@ktsh.ch |
| Kantonskanzlei des Kantons Appenzell Ausserrhoden | Regierungsgebäude<br>9102 Herisau<br>Kantonskanzlei@ar.ch |
| Ratskanzlei des Kantons Appenzell Innerrhoden | Marktgasse 2<br>9050 Appenzell<br>info@rk.ai.ch |
| Staatskanzlei des Kantons St. Gallen | Regierungsgebäude<br>9001 St. Gallen<br>info.sk@sg.ch |
| Standeskanzlei des Kantons Graubünden | Reichsgasse 35<br>7001 Chur<br>info@gr.ch |
| Staatskanzlei des Kantons Aargau | Regierungsgebäude<br>5001 Aarau<br>staatskanzlei@ag.ch |
| Staatskanzlei des Kantons Thurgau | Regierungsgebäude<br>Zürcherstrasse 188<br>8510 Frauenfeld<br>staatskanzlei@tg.ch |
| Cancelleria dello Stato del Cantone Ticino | Palazzo delle Orsoline<br>6501 Bellinzona<br>can-scds@ti.ch |
| Chancellerie d'Etat du Canton de Vaud | Place du Château 4<br>1014 Lausanne<br>info.chancellerie@vd.ch |

| | |
|---|---|
| Chancellerie d'Etat du Canton du Valais | Planta 3<br>1950 Sion<br>Chancellerie@admin.vs.ch |
| Chancellerie d'Etat du Canton de Neuchâtel | Le Château<br>Rue de la Collégiale 12<br>2000 Neuchâtel<br>Secretariat.chancellerie@ne.ch |
| Chancellerie d'Etat du Canton de Genève | Rue de l'Hôtel-de-Ville 2<br>Case postale 3964<br>1211 Genève 3<br>service-adm.ce@etat.ge.ch |
| Chancellerie d'Etat du Canton du Jura | 2, rue de l'Hôpital<br>2800 Delémont<br>chancellerie@jura.ch |
| Konferenz der Kantonsregierungen (KdK)<br>Conférence des gouvernements cantonaux (CdC)<br>Conferenza dei Governi cantonali (CdC) | Sekretariat<br>Haus der Kantone<br>Speichergasse 6<br>Postfach<br>3001 Bern<br>mail@kdk.ch |

2. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell' Assemblea federale

| | |
|---|---|
| Bürgerlich-Demokratische Partei BDP<br>Parti bourgeois-démocratique PBD<br>Partito borghese democratico PBD | Postfach 119<br>3000 Bern 6<br>mail@bdp.info |
| Christlichdemokratische Volkspartei CVP<br>Parti démocrate-chrétien PDC<br>Partito popolare democratico PPD | Generalsekretariat<br>Klaraweg 6<br>Postfach<br>3001 Bern<br>info@cvp.ch |
| Christlich-soziale Partei Obwalden csp-ow | Frau Linda Hofmann<br>St. Antonistrasse 9<br>6060 Sarnen<br>ch.schaeli@gmx.net |
| Christlichsoziale Volkspartei Oberwallis | CSPO<br>Geschäftsstelle<br>Postfach 132<br>3930 Visp<br>info@cspo.ch |

| | |
|---|---|
| Evangelische Volkspartei der Schweiz EVP<br>Parti évangélique suisse PEV<br>Partito evangelico svizzero PEV | Nägeligasse 9<br>Postfach<br>3001 Bern<br>vernehmlassungen@evppev.ch |
| FDP. Die Liberalen<br>PLR. Les Libéraux-Radicaux<br>PLR.I Liberali Radicali | Generalsekretariat<br>Neuengasse 20<br>Postfach<br>3001 Bern<br>info@fdp.ch |
| Grüne Partei der Schweiz GPS<br>Parti écologiste suisse PES<br>Partito ecologista svizzero PES | Waisenhausplatz 21<br>3011 Bern<br>gruene@gruene.ch |
| Grünliberale Partei glp<br>Parti vert'libéral pvl | Laupenstrasse 2<br>3008 Bern<br>schweiz@grunliberale.ch |
| Lega dei Ticinesi (Lega) | Via Monte Boglia 3<br>Case postale 4562<br>6904 Lugano<br>lorenzo.quadri@mattino.ch |
| Mouvement Citoyens Genevois (MCG) | Case postale 155<br>1211 Genève 13<br>info@mcge.ch |
| Partei der Arbeit PDA<br>Parti suisse du travail PST | Postfach 8640<br>8026 Zürich<br>pdaz@pda.ch |
| Schweizerische Volkspartei SVP<br>Union Démocratique du Centre UDC<br>Unione Democratica di Centro UDC | Generalsekretariat<br>Postfach 8252<br>3001 Bern<br>gs@svp.ch |
| Sozialdemokratische Partei der Schweiz SPS<br>Parti socialiste suisse PSS<br>Partito socialista svizzero PSS | Zentralsekretariat<br>Spitalgasse 34<br>Postfach<br>3001 Bern<br>verena.loembe@spschweiz.ch |

3. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni delle città e delle regioni di montagna

| | |
|---|---|
| Schweizerischer Gemeindeverband | Laupenstrasse 35<br>3008 Bern<br>verband@chgemeinden.ch |
| Schweizerischer Städteverband | Monbijoustrasse 8<br>Postfach<br>3001 Bern<br>info@staedteverband.ch |
| Schweizerische Arbeitsgemeinschaft für die Berggebiete | Seilerstrasse 4<br>Postfach<br>3001 Bern<br>info@sab.ch |

4. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national/ associazioni mantello nazionali dell'economia

| | |
|---|---|
| economiesuisse<br>Verband der Schweizer Unternehmen<br>Fédération des entreprises suisses<br>Federazione delle imprese svizzere<br>Swiss business federation | Hegibachstrasse 47<br>Postfach<br>8032 Zürich<br>info@economiesuisse.ch<br>bern@economiesuisse.ch<br>sandra.spieser@economiesuisse.ch |
| Schweizerischer Gewerbeverband (SGV)<br>Union suisse des arts et métiers (USAM)<br>Unione svizzera delle arti e mestieri (USAM) | Schwarztorstrasse 26<br>Postfach<br>3001 Bern<br>info@sgv-usam.ch |
| Schweizerischer Arbeitgeberverband<br>Union patronale suisse<br>Unione svizzera degli imprenditori | Hegibachstrasse 47<br>Postfach<br>8032 Zürich<br>verband@arbeitgeber.ch |
| Schweiz. Bauernverband (SBV)<br>Union suisse des paysans (USP)<br>Unione svizzera dei contadini (USC) | Laurstrasse 10<br>5201 Brugg<br>info@sbv-usp.ch |
| Schweizerische Bankiervereinigung (SBV)<br>Association suisse des banquiers (ASB)<br>Associazione svizzera dei banchieri (ASB)<br>Swiss Bankers Association | Postfach 4182<br>4002 Basel<br>office@sba.ch |

| | |
|---|---|
| Schweiz. Gewerkschaftsbund (SGB)<br>Union syndicale suisse (USS)<br>Unione sindacale svizzera (USS) | Monbijoustrasse 61<br>Postfach<br>3000 Bern 23<br>info@sgb.ch |
| Kaufmännischer Verband Schweiz<br>Société suisse des employés de commerce<br>Società svizzera degli impiegati di commercio | Hans-Huber-Strasse 4<br>Postfach 1853<br>8027 Zürich<br>berufspolitik@kfmv.ch |
| Travail.Suisse | Hopfenweg 21<br>Postfach 5775<br>3001 Bern<br>info@travailsuisse.ch |

5. Weitere Interessierte / Autres intéressés / Altri interessati

| | |
|---|---|
| asut | Schweizerischer Verband der Telekommunikation<br>Klösterlistutz 8<br>3013 Bern<br>info@asut.ch |
| Berner Fachhochschule | Falkenplatz 24<br>3012 Bern<br>office@bfh.ch |
| Interessengemeinschaft Detailhandel Schweiz (IG DHS)<br>Communauté d'intérêt du commerce de détail suisse (CICDS) | Geschäftsstelle IG DHS<br>Postfach 5815<br>3001 Bern<br>info@igdhs.ch |
| Post CH AG | Wankdorfallee 4<br>3030 Bern<br>corporatecenter@post.ch |
| Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten | Henric Petri-Strasse 15<br>Postfach 205<br>4010 Basel<br>praesident@privatim.ch |
| Procivis Daniel Gasteiger | Seestrasse 329<br>8038 Zürich<br>gasteiger@procivis.ch |
| Schweizerische Bundesbahnen SBB | Hilfikerstrasse 1<br>3000 Bern 65<br>meier.bernhard@sbb.ch |

| | |
|---|---|
| Schweizerische Informatikkonferenz | Haus der Kantone<br>Speichergasse 6<br>3011 Bern<br>info@sik.ch |
| Schweizerischer Anwaltsverband SAV | Marktgasse 4<br>Postfach 8321<br>3011 Bern<br>info@sav-fsa.ch |
| Schweizerischer Notarenverband | Schwanengasse 5/7<br>3011 Bern<br>info@schweizernotare.ch |
| Swico | Josefstrasse 218<br>8005 Zürich<br>info@swico.ch |
| Swiss Fintech Innovations | Binzmühlestrasse 14<br>8050 Zürich<br>office@swissfintechinnovations.ch |
| Swisscom (Schweiz) AG | Alte Tiefenaustrasse 6<br>3050 Bern<br>Konzern.Rechtsdienst@swisscom.com |
| Trägerverein SuisseID | Geschäftsstelle<br>Steinerstrasse 37<br>3006 Bern<br>office@suisseid.ch |