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…