Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Documento di discussione degli obiettivi dell'le

Base di discussione per un'idea comune di un'identità elettronica statale in vista della decisione di principio del Consiglio federale

Riassunto

Il presente documento serve da base per il dibattito pubblico. Non mira a prendere una decisione a favore di una delle varianti per una nuova identità elettronica (Ie) statale. La discussione pubblica verte principalmente sulle questioni dell'utilità dell'Ie, dei casi di applicazione e dei requisiti posti a un'Ie statale. Il risultato della discussione pubblica servirà al Consiglio federale per prendere una decisione di principio entro la fine del 2021.

Per la Svizzera riparte la ricerca di una soluzione relativa all'Ie. Il primo passo consiste nel discutere l'idea di una nuova Ie. Si tratta di rispondere soprattutto alle seguenti domande.

- L'Ie è un documento digitale rilasciato dallo Stato per provare la propria identità e può essere usata sia nel mondo analogico che in quello digitale?
- Un ecosistema più ampio con prove digitali di qualsiasi tipo dei più diversi editori pubblici e privati potrebbe implicare una maggiore utilità e quindi anche un uso più ampio da parte degli utenti? Quali sarebbero i rischi?

La discussione deve concentrarsi sull'utilità di un'Ie per il titolare. Il presente documento abbozza alcuni casi di applicazione esemplari, nella consapevolezza che non esiste *un unico caso di applicazione* e che sarà la somma di tutti i casi di applicazione utili a determinare il successo dell'Ie. Nel contempo bisogna tuttavia riconoscere che al momento i più diversi fornitori statali e privati di servizi hanno probabilmente un bisogno maggiore, rispetto ai titolari dell'Ie, di un ecosistema di Ie facilmente integrabile e dalla struttura flessibile. È pertanto di fondamentale importanza che sia spiegata mediante casi di applicazione adeguati anche l'utilità concreta per i titolari. In tale contesto allo Stato spetta il ruolo di promotore, abilitatore (enabler) e garante.

Dall'elaborazione della legge sull'Ie, respinta in votazione, la situazione è mutata in particolare nei seguenti ambiti:

- la protezione dei dati e in particolare la protezione della sfera privata sono divenute un tema ancora più importante nell'opinione pubblica;
- i sistemi d'identità del futuro si basano su approcci incentrati sugli utenti.

Per l'attuazione tecnologica il presente documento illustra e propone di discutere diverse soluzioni:

- Self-Sovereign Identity
- infrastruttura a chiave pubblica
- fornitore d'identità (IdP) centrale dello Stato

Tutte le soluzioni sollevano questioni irrisolte e non ogni soluzione soddisfa in misura uguale tutti i requisiti. La valutazione delle varianti non fa tuttavia parte della presente base di discussione; si svolgerà invece nell'ambito di una discussione pubblica tesa a definire le caratteristiche fondamentali di un'idea comune di Ie, della sua utilizzazione e dei requisiti posti all'ecosistema. Tale discussione sarà determinante per la decisione di principio del Consiglio federale prevista alla fine del 2021. In seguito potranno essere elaborate le basi legali che dovranno essere approvate dal Parlamento.

Glossario

Attributo	Singolo dato, p. es. nome o data di nascita.
Comunicazione peer-to-peer	Comunicazione diretta senza intermediario. Nel contesto della SSI, il flusso di dati tra il servizio di rilascio e il titolare o tra il titolare e il verificatore.
Credenziali (Credentials)	Nel contesto della SSI: set di dati composto da uno o più attributi. Nel contesto IdP: credenziali di login: caratteristiche dell'identità che permettono l'autenticazione del soggetto, sinonimo di fattori d'autenticazione, p. es. nome utente, parola chiave o PIN.
Credenziali verificate (Verified Credentials, VC)	Set di dati composto da uno o più attributi, firmato dal servizio di rilascio come «verificato» e poi consegnato all'utente. Oltre ai dati in sé, anche il servizio di rilascio, la data di rilascio e le prove crittografiche sono parte delle credenziali verificate.
Crittografia a chiave pubblica	Tecnica di criptaggio asimmetrica, nella quale una chiave è resa pubblica e l'altra deve rimanere privata.
Ecosistema di Ie	Cooperazione di diversi attori (statali e privati), con varie possibilità di offerta e di uso, mediante e attorno all'Ie nonché sulla base di un'infrastruttura digitale affidabile.
Elenco delle revoche	Elenco pubblicamente accessibile dei numeri d'identificazione di prove e certificati rilasciati ma poi revocati.
Fornitore d'identità (Identity provider, IdP)	Componente tecnica di sistema presso la quale si svolge un login per «garantire» successivamente l'identità dell'utente. In senso lato, anche un documento d'identità o un wallet può essere inteso come un fornitore d'identità.
Identità autogestita	Traduzione di Self-Sovereign Identity. Nel contesto della SSI l'utente è egli stesso responsabile della gestione delle prove digitali rilasciate dal servizio di rilascio e quindi affidabili.
Identità decentrale	Identità elettronica non gestita da un sistema centrale per il cui tramite esclusivo può essere usata, bensì salvata su un apparecchio dell'utente, ad esempio sullo smartphone, grazie al quale può essere usata direttamente.
Identity Hub «Backup»	Possibilità di salvaguardare elettronicamente prove dell'identità. Mette a disposizione i dati per il loro ripristino e permette la loro trasmissione ad altri apparecchi. Può essere gestito dall'utente sul proprio hardware o messo a disposizione da un fornitore con funzionalità di cloud.
Identity Management	Identity e Access Management sono spessi nominati insieme con la sigla IAM. All'identity management compete la gestione delle identità e l'attribuzione delle caratteristiche (attributi tecnici), a prescindere dai relativi ruoli e dalle autorizzazioni. Per identità si può intendere, semplificando, anche un login o un conto.
Ie	Identità elettronica statale – un tipo di prova digitale che può essere impiegata dall'utente per provare la sua identità.
Infrastruttura a chiave pubblica (Public Key Infrastruktur, PKI)	Sistema globale di una rete di fiducia allestita sulla base di una tecnica di criptaggio asimmetrica.
Infrastruttura digitale fiduciaria	Una serie di regole, processi, piani ed elementi infrastrutturali che garantiscono la fiducia nei processi digitali e l'affidabilità di questi ultimi e che sono accettati e usati da un folto numero di utenti.
Institutional Agent	Termine usato nel contesto della SSI e introdotto dal progetto pilota di SSI tedesco IDunion. Software per il rilascio e il controllo di credenziali verificate.
Livello di ambizione	Termine ripreso dalla rielaborazione del Regolamento eIDAS. Chiarisce la portata dell'uso di un'infrastruttura Ie.
Memorizzazione decentrale dei dati	I dati non sono conservati in un'unica memoria centrale, bensì in una rete di sistemi di memorizzazione oppure sugli apparecchi terminali degli utenti.
Node	Nodo di memorizzazione in una rete di memorizzazione distribuita (Distributed Ledger [registro distribuito], DLT).
Parsimonia di dati	Il termine riunisce due aspetti: ridurre al minimo gli attributi necessari alla trasmissione di dati a terzi e evitare flussi inutili di dati e dei relativi metadati.
Privacy by design	Principio secondo cui la protezione dei dati e in particolare la parsimonia di dati è assicurata dal tipo di infrastruttura. Permette di creare fiducia senza dover garantire la sicurezza mediante basi legali e i relativi controlli.
Public Key Directory (PKD)	Registro centrale nel quale sono depositate le chiavi pubbliche (public key) dei servizi di rilascio delle prove. Nelle PKI gerarchiche con un'unica ancora di fiducia non è necessaria una PKD.
Registry	Termine usato nel contesto della SSI: memoria leggibile pubblicamente con le necessarie prove crittografiche per controllare la validità di credenziali verificate.
Regolamento eIDAS	eIDAS sta per «electronic identification, authentication and trust services». Si tratta di un regolamento dell'Unione europea che definisce regole univoche nei settori dell'identificazione elettronica e dei servizi elettronici fiduciari.
Relying Party (RP)	Termine analogo a verificatore, usato nel contesto dell'IdP: partecipante all'ecosistema Ie che se ne serve per verificare prove dell'identità e l'uso dei dati personali rappresentanti l'Ie.
Self-Sovereign Identity (SSI)	Una serie di principi improntati alla protezione dei dati e all'utente che negli ultimi anni ha portato a un approccio tecnologico per un'identità elettronica dedotta da tali principi.

Servizio di rilascio (Issuer)	Istituzioni, organizzazioni e anche persone private che rilasciano una prova digitale e la consegnano all'utente.
Titolare (Holder)	Nel contesto della SSI e della PKI il titolare del wallet con le prove digitali.
Trust over IP (ToIP) Framework	Direttive per la definizione di livelli decisionali relativi a questioni di attuazione della governance e della tecnologia, elaborate da gruppi di lavoro della Trust over IP Fundation.
Verificatore (Verifier)	Termine analogo a Relying Party usato nel contesto della SSI: partecipante all'ecosistema Ie che se ne serve per verificare prove dell'identità e l'uso dei dati personali rappresentanti l'Ie.
Wallet	Applicazione, spesso concepita per smartphone, che salva prove digitali e garantisce la comunicazione con i servizi di rilascio e di verifica.

Indice

1 Scopo del documento

Il presente documento costituisce la base per discutere una visione comune di un'identità elettronica statale (Ie), la sua impostazione, la portata del relativo ecosistema e molti altri aspetti. Rinuncia consapevolmente a descrivere e valutare una soluzione definitiva. Un'ampia discussione permetterà di precisare le linee generali per l'Ie. Il risultato di tale discussione consentirà al Consiglio federale di prendere una decisione di principio in merito a una nuova soluzione per un'Ie statale.

2 Situazione di partenza

2.1 Votazione popolare relativa alla legge sull'Ie

Il 27 settembre 2019 il Parlamento ha adottato a netta maggioranza la legge federale sui servizi d'identificazione elettronica (Legge sull'Ie, LSIe), contro la quale è poi riuscito il referendum. Nella votazione del 7 marzo 2021 il Popolo ha respinto chiaramente la legge.

2.2 Mozioni

Dopo il rifiuto della LSIe, il 10 marzo 2021 sono state presentate sei mozioni dal tenore identico:[1]

Il Consiglio federale è incaricato di creare uno strumento d'identificazione elettronica statale, comparabile alla carta d'identità o al passaporto nel mondo reale e che consenta ai cittadini di comprovare la loro identità (autentificazione) nel mondo virtuale, osservando in particolare i principi della «privacy by design», della minimizzazione dei dati e della registrazione decentralizzata dei dati (come la registrazione dei dati dei documenti d'identità presso gli utenti). Questa identità elettronica (Ie) può fondarsi su prodotti e servizi sviluppati dall'economia privata. La procedura di rilascio e la gestione complessiva della soluzione devono tuttavia competere ad autorità statali specializzate.

Le richieste principali delle sei mozioni:

- strumento d'identificazione elettronica statale comparabile al passaporto
- parsimonia dei dati e «Privacy by Design»
- registrazione decentrale dei dati
- processo di rilascio e gestione complessiva di competenza delle autorità statali

2.3 Chiarimento della visione di un'Ie

Le idee relative all'Ie sono per ora poco precise, ognuno ne ha una visione propria. Il presente documento intende dare impulsi per consolidare e sviluppare la visione di base. Occorre ad esempio chiarire se l'Ie può essere utilizzata anche nel mondo reale (analogamente ai certificati di vaccinazione digitali), se all'Ie si può attribuire la stessa forza probatoria dei documenti cartacei e se essa, in quanto fattore di identificazione, deve essere parte di un login statale su scala nazionale.

[1] https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213129

La prova dell'identità per via digitale è il compito principale di un'Ie. Quest'ultima può quindi essere intesa come un «documento» e il login come *una* sua possibile applicazione. Inoltre, lo Stato assume il ruolo di sevizio di rilascio e di gestione. Ne risulta pertanto la definizione seguente:

«Un'Ie è un documento digitale rilasciato dallo Stato che permette di provare la propria identità.»

Per non restringere troppo la portata della visione, il presente documento lega l'Ie all'idea di un'infrastruttura digitale affidabile della Svizzera che potrebbe essere definita come segue:

«La Svizzera possiede un'infrastruttura digitale di fiducia gestita dallo Stato che permette e promuove processi sicuri ed esclusivamente digitali.»

Un'Ie statale potrebbe fornire un contributo importante per una siffatta infrastruttura digitale di fiducia, ma non sarebbe l'unico tassello per realizzarla (cfr. cap. 2.4). Come già nella legge sull'Ie, hanno diritto a un'Ie i cittadini svizzeri e stranieri titolari di un documento o una carta di legittimazione riconosciuti in Svizzera. Nel presente documento per gli aventi diritto si usa la designazione «utenti». Le persone giuridiche agiscono sempre per mezzo dei loro organi, composti da persone fisiche, e non possono pertanto essere titolari di un'Ie propria. Sono identificate mediante un numero d'identificazione delle imprese (IDI)[2] univoco.

2.4 Esigenze poste alla digitalizzazione

Le esigenze poste nell'ambito della digitalizzazione sono spesso molto elevate, mentre le aspettative e idee in merito divergono notevolmente. Oggi la tecnica non è più considerata un fattore che limita la trasmissione di dati e notizie: «tecnicamente quasi tutto è possibile». La mancanza di una tangibilità fisica rende tuttavia a volte più difficile una comprensione comune e univoca dei fatti, delle funzioni e dei ruoli.

La digitalizzazione è sempre connessa all'esigenza di ripensare i processi e i ruoli. Una buona digitalizzazione con processi efficienti non si raggiunge trasferendo i processi esistenti in modo incontrollato su canali digitali. Nel caso ideale si possono evitare alcune fasi necessarie nel processo analogico. L'automatizzazione connessa a una digitalizzazione dei processi (nel senso che i processi sono reimpostati secondo principi digitali) porta al risparmio di risorse e permette un'elevata scalabilità del sistema, che con pressoché i medesimi mezzi può sbrigare con qualità e velocità maggiori una mole molto più importante di processi.

Lo sviluppo della digitalizzazione deve porre in primo piano gli utenti. Oltre che di cittadini privati, si tratta anche di rappresentanti dell'economia (che agiscono per le imprese) che possono trarre un profitto notevolmente maggiore dai processi digitalizzati. Una buona digitalizzazione migliora quindi direttamente le condizioni quadro dell'economia, permette di semplificare le procedure e da parte sua l'economia è in grado di offrire nuove possibilità ai cittadini. Ne trae quindi profitto l'intera economia nazionale.

La richiesta di un'Ie statale può essere intesa come un conferimento di compiti alla Confederazione. Le competenze precise della Confederazione e quindi le possibilità di far progredire la digitalizzazione mediante un'infrastruttura statale devono essere tuttavia esaminate in maniera più approfondita. L'Ie non è tuttavia la bacchetta magica che tutti aspettano nella spe-

[2] Cfr. https://www.bfs.admin.ch/bfs/it/home/registri/registro-imprese/numero-identificazione-imprese.html

ranza che risolva tutti i problemi della digitalizzazione. L'Ie non porterà direttamente alla digitalizzazione della Svizzera, ma ne sosterrà il progresso perché costituisce un'importante componente infrastrutturale del Paese.

Infine, occorre osservare che molte esigenze sono in un rapporto dialettico. Non c'è *la soluzione giusta* e la discussione deve portare a una via consensuale. È necessario trovare un equilibrio tra:

- fruibilità per gli utenti ↔ protezione dei dati ↔ sicurezza dei dati
- autoresponsabilità ↔ possibilità di sostegno
- focalizzazione sull'utente ↔ fiducia
- ambiente controllato con accesso difficile ↔ sistema aperto con accesso facile
- pochi casi di applicazione controllati ↔ molti casi di applicazione incontrollati
- velocità di attuazione ↔ perfezione
- flessibilità ↔ protezione degli utenti

3 Sviluppo nel settore delle identità digitali

3.1 Sviluppi tecnologici

Viste le richieste di un'elevata protezione dei dati e di una registrazione decentrale dei dati, avanzate anche dalle mozioni menzionate nel capitolo 2.2, negli ultimi anni si è sviluppata una discussione su scala mondiale sul tema «identità decentrale». Ciò ha portato a tutta una serie di tecnologie, nuove procedure crittografiche e standard che possono essere impiegati per ottenere sistemi affidabili. La Self-Sovereign Identity (SSI), costituita da principi focalizzati sull'utente e mezzi tecnologici, è probabilmente al momento l'approccio più discusso, in ragione della semplicità del sistema, della vicinanza della tecnologia alla realtà fisica e della sua applicabilità universale.

Una pietra miliare tecnologica della SSI è la crittografia a chiave pubblica, che da anni è usata per la prova tecnica decentrale della provenienza sotto forma di certificati (p. es. X.509). Si applica in particolare nell'ambito della firma di dati del passaporto biometrico, del rilascio del certificato COVID, della firma elettronica o dell'installazione di una comunicazione protetta con un sito Internet.

Su scala internazionale è ravvisabile la tendenza all'Ie sugli smartphone, poiché questi ultimi sono molto diffusi. Le soluzioni precedenti sviluppate con carte munite di microchip sono sostituite con soluzioni basate sugli smartphone. I «wallet» digitali usati come luogo di conservazione di prove digitali gestite in modo decentrale sono all'ordine del giorno sull'agenda digitale dell'UE. Tuttavia, al momento in Europa molte soluzioni Ie sono soluzioni «IdP tradizionali», anche se con caratteristiche assai differenti (fornitori d'identità statali, privati, federati).

Il rilancio dell'Ie offre alla Svizzera l'opportunità di approfittare delle conoscenze e delle tendenze più recenti. Poiché la tecnologia si evolve con grande rapidità, è necessario un sistema la cui realizzazione tecnica è flessibile. Su scala internazionale il ciclo di rinnovamento delle soluzioni per le identità digitali va dai 5 ai 10 anni. Una soluzione definitiva perfetta non è possibile e pertanto non costituisce neppure un obiettivo da raggiungere. Dovrebbe tuttavia essere scelta una soluzione in grado di fungere da base per molti processi di creazione di

valore aggiunto nonché di promuovere la digitalizzazione della Svizzera. Il futuro quadro giuridico per un'Ie dovrebbe essere per quanto possibile neutrale sotto il profilo tecnologico e quindi permetterne esplicitamente l'ulteriore sviluppo.

3.2 Sviluppi nel diritto europeo

Il 3 giugno 2021 la Commissione europea ha presentato una proposta di modifica[3] del Regolamento eIDAS[4] al fine di istituire il contesto giuridico per un'identità digitale europea (idUE). Se dovesse essere adottato conformemente al progetto, il nuovo regolamento obbligherebbe gli Stati membri a mettere a disposizione dei cittadini portafogli digitali in cui essi possono connettere la propria identità digitale nazionale con la prova di altri attributi personali (p. es. licenza di condurre, diplomi, conto bancario, ecc.). Dall'identità digitale nazionale viene dedotta un'idUE. I portafogli possono essere messi a disposizione dalle autorità o da istituzioni private riconosciute da uno Stato membro.

Per permettere di attuarla quanto prima, la proposta è completata da una raccomandazione in cui la Commissione esorta gli Stati membri a creare entro settembre 2022 strumenti comuni e ad avviare senza indugio i lavori preliminari necessari. Gli strumenti devono comprendere l'architettura tecnica, le norme, le direttive e le procedure consolidate.

Il quadro prescritto dalla Commissione è neutrale sotto il profilo tecnologico ma si fonda sui principi della SSI. A partire da settembre 2021, gli Stati membri negozieranno gli standard tecnici. Affinché la futura Ie svizzera possa essere notificata conformemente al Regolamento eIDAS conviene fondarsi sul quadro previsto dalla Commissione europea.

4 Ecosistema Ie

4.1 Uso quotidiano

Tutte le iniziative tese a introdurre un'identità elettronica nazionale devono affrontare il problema dell'uovo e della gallina: senza Ie non si creano casi di applicazione e senza casi di applicazione non è necessaria un'Ie. Per favorirne la diffusione e l'uso frequente in Europa, oltre che ai servizi del governo elettronico, si punta spesso all'uso dell'Ie per scopi secondari quali l'autorizzazione alla firma elettronica o l'accesso a operazioni bancarie in Internet (e-banking). L'uso frequente migliora la padronanza e la competenza e crea la possibilità di un uso quotidiano massiccio (ognuno conosce l'Ie, l'apprezza ed è in grado di usarla).

Se s'intende permettere il numero più elevato possibile di usi per scopi diversi, è necessario un ecosistema funzionante: un'infrastruttura usata collettivamente, con regole definite di comune accordo e con molte possibilità per i diversi attori del sistema. Nel caso ideale l'Ie funziona in un ecosistema che dispone di interfacce aperte e standardizzate nonché di un sistema di gestione armonizzato, non implica regole burocratiche ostacolanti e consente un aggiornamento semplice e automatico dei dati dell'Ie. In tal modo si creerebbero anche i presupposti per coinvolgere le imprese dell'economia privata, che su tale base potrebbero sviluppare nuovi processi e scambi commerciali, il che permetterebbe di usare l'Ie per ulteriori scopi. Se sono

[3] Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica il Regolamento (UE) n. 910/2014 e mira a creare le condizioni per un'identità digitale europea

[4] 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

a disposizione scopi di utilizzazione concreti ed è visibile un beneficio individuale, si suscita l'interesse dei potenziali utenti.

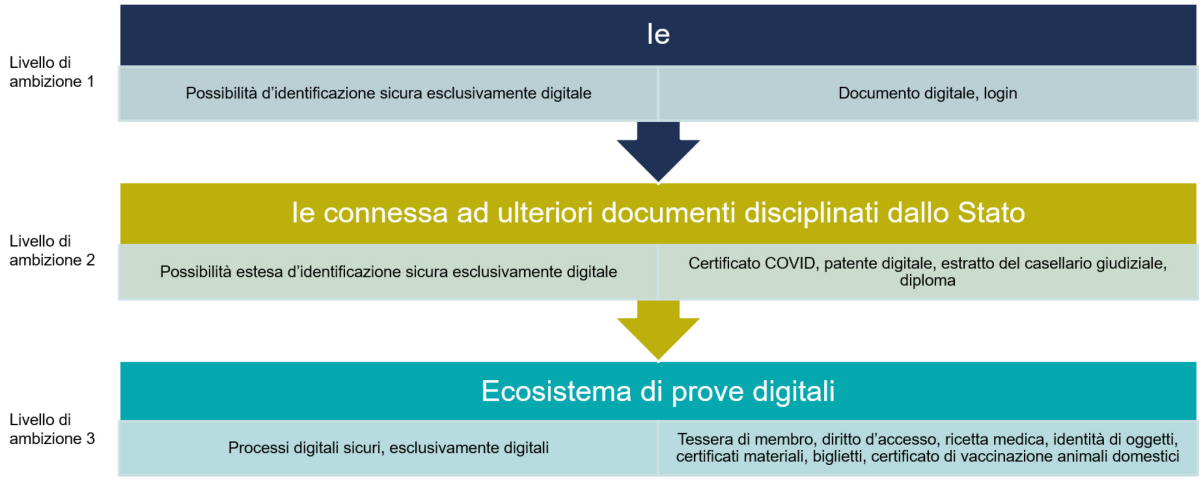
Tra i criteri più importanti devono figurare la facilità d'utilizzazione e il grado di soddisfazione degli utenti. Le interazioni nell'ecosistema Ie devono essere comode, trasparenti e comprensibili. Nel contempo occorre creare fiducia nel sistema, nei partecipanti e nella forza probatoria dell'Ie. Inoltre, l'utilizzo non dovrebbe richiedere l'impiego di apparecchi tecnici supplementari e dovrebbe probabilmente essere gratuito per gli utenti, poiché anche importi esigui possono essere scoraggianti. Occorre evitare consapevolmente ostacoli troppo alti all'utilizzo e l'IE deve soddisfare le aspettative degli utenti in merito alla protezione e alla sicurezza.

Questi criteri sono sufficienti affinché l'Ie diventi di uso quotidiano? È sufficiente istituire un ecosistema specifico per l'Ie oppure occorre creare un ecosistema più ampio in cui l'Ie costituirebbe soltanto *una tra le tante prove digitali*? Il capitolo seguente illustra questo aspetto.

4.2 Portata dell'ecosistema

Prima di affrontare la discussione tecnologica è opportuno affrontare anche la questione della portata della futura utilizzazione dell'Ie (i cosiddetti livelli di ambizione) e quindi del relativo ecosistema. Sussiste un'interazione tra i livelli di ambizione, l'istituzione e la struttura dell'ecosistema e le tecnologie impiegabili. La scelta della tecnologia dipende in linea di massima dal risultato desiderato, ma è importante sapere che diverse attuazioni tecniche di complessità analoga permettono di ottenere risultati differenti.

Come base per la discussione sono definiti – in analogia alla discussione nell'UE[5] – i tre livelli di ambizione seguenti:



Livello di ambizione 1: Ie

Il livello di ambizione 1 prevede lo scopo minimo di un'Ie: l'Ie è un documento che può essere usato nel mondo digitale per provare la propria identità. È rilasciata esclusivamente dalla Confederazione. L'Ie potrebbe essere integrata *con* un login oppure usata *per* un login. L'utilità immediata di un'Ie in quanto possibilità di documento d'identità digitale consiste principalmente nei seguenti casi di applicazione:

[5] Anche l'UE definisce tre «livelli di ambizione» per l'UEid

- conferma dell'identità (p. es. conto bancario, abbonamento del cellulare, ordinazione dell'estratto del casellario giudiziale, sportello postale, controllo della persona)
- conferma dell'età (con attributi dedotti)

Dalla votazione sulla legge sull'Ie risulta l'impressione che una maggioranza non è convinta dell'utilità di questi casi di applicazione.

Livello di ambizione 2: Ie connessa a ulteriori prove disciplinate dallo Stato

Il livello di ambizione 2 mira a un ecosistema in cui l'Ie statale costituisce un'identità di base su cui si fondano molte altre prove disciplinate dallo Stato, ad esempio la licenza di condurre digitale. L'identità di base fornisce le informazioni di base relative alla persona, quali il nome, la data di nascita e l'immagine del viso. In aggiunta la licenza di condurre si limiterebbe a fornire le ulteriori indicazioni, quali la categoria di veicolo e la data di validità.

Per mezzo di connessioni crittografiche si creerebbe una dipendenza dall'identità di base. Nel caso di connessioni logiche un'ulteriore prova statale potrebbe funzionare anche in modo indipendente e non sarebbe toccata da un'eventuale revoca dell'identità di base.

La portata dell'ecosistema è molto più ampia rispetto al livello 1 e le utilizzazioni possibili sono molto più numerose. Al rilascio sarebbero autorizzati i più diversi attori statali che garantirebbero anche la correttezza delle connessioni.

Livello di ambizione 3: ecosistema di prove digitali

Il livello di ambizione 3 offre il potenziale maggiore per risolvere il problema dell'uovo e della gallina. Nell'intero ecosistema, l'Ie costituisce soltanto una delle tante prove digitali. È possibile una connessione all'Ie, ma una prova digitale può anche essere indipendente da essa, ad esempio un biglietto per un evento o per i trasporti pubblici, una tessera di membro, un certificato di vaccinazione di un animale domestico, una licenza di condurre o l'attestato del collaudo periodico di un'automobile.

Con il livello di ambizione 3 possono rilasciare prove digitali sia lo Stato che privati. La possibilità di rilascio dei privati è decisiva, poiché nella quotidianità le prove rilasciate da privato a privato sono numerose. Ciò consente di eseguire molti processi esclusivamente per via digitale, per esempio nell'ambito della gestione dei clienti, dei fornitori o dei collaboratori e in tutti i casi in cui sono in gioco documenti, giustificativi e certificati. Per l'utente ciò ha il vantaggio che l'applicazione (ricevere, memorizzare, presentare) è sempre uguale di modo che si afferma un'idea collettiva di cosa sia una prova digitale. Invece dell'Ie, al centro dell'ecosistema vi è un luogo di conservazione disciplinato e garantito dallo Stato, un «wallet statale» dal quale possono essere ricevute informazioni di alta affidabilità.

L'UE si esprime per il livello di ambizione 3, un cosiddetto «Highly Secure Personal Digital Identity Wallet».

L'Ie è senza dubbio un elemento chiave di un siffatto ecosistema, nel quale potrebbe contribuire all'istituzione di un'infrastruttura di fiducia nazionale, digitale e flessibile. È in linea di massima ipotizzabile un'evoluzione a tappe, ma il livello di ambizione finale dovrebbe essere definito sin dall'inizio, poiché non tutte le tecnologie sono adeguate per un ecosistema aperto di prove digitali (livello di ambizione 3). Ogni livello di ambizione è realizzabile con una o più tecnologie. Ogni implementazione comporta determinate conseguenze. Prima di descrivere

possibili soluzioni è tuttavia opportuno passare in rassegna alcuni casi di applicazione esemplari.

4.3 Casi di applicazione

Per poter confrontare soluzioni diverse il presente capitolo descrive alcuni casi di applicazione esemplari. Per ogni caso è abbozzata la situazione attuale e quella auspicata. Ogni caso è esemplare per un determinato tipo di applicazione e mette pertanto in evidenza aspetti specifici che permettono di discutere ulteriori questioni.

I casi di applicazione trattati nel presente capitolo non hanno la pretesa di costituire un elenco esaustivo. È invece fondamentale cercare casi di applicazione rilevanti per il criterio dell'utilità per i cittadini e valutarli secondo tale parametro. Come già illustrato, ciò non sarà possibile in modo definitivo in un determinato momento, poiché si tratta di un processo in continua evoluzione. Pertanto, a seconda del livello di ambizione, vanno stabiliti processi pilotati e agili. In tale contesto, lo Stato – come chiesto in alcune mozioni – assolve il ruolo di autorità abilitante proattiva (enabler).

I casi di applicazione intendono permettere di illustrare e analizzare criticamente in modo esemplare l'utilità diretta e concreta per gli utenti dell'Ie. Implicitamente occorre tenere sempre in considerazione le possibilità di semplificare il processo, il che implica un vantaggio indiretto per gli utenti grazie alla velocizzazione delle procedure, a prestazioni più vantaggiose o a nuovi servizi. A seconda del livello di ambizione, i fornitori di servizi stessi (relying party) possono considerarsi non solo destinatari o verificatori della prova bensì anche servizi di rilascio.

Molte discussioni sull'argomento mettono in risalto che non esiste *un unico caso di applicazione;* decisiva è la somma e la molteplicità delle applicazioni. Quanto più elevato è il livello di ambizione tanto più numerose e molteplici saranno le applicazioni possibili. Nel caso di un «ecosistema aperto di prove digitali», l'economia innovativa svizzera potrebbe notevolmente aumentare il numero e la molteplicità delle applicazioni e quindi aumenterebbe anche la probabilità dell'uso nella vita di tutti i giorni.

4.3.1 Verifica dell'età nel mondo analogico e in quello digitale

Nella verifica dell'identità si tratta di verificare che una persona abbia passato un determinato limite di età e quindi l'età precisa e la data di nascita sono irrilevanti. L'utilità dell'Ie per l'utente consiste nell'applicazione semplice e parsimoniosa sotto il profilo dei dati, possibile sia nel mondo analogico che in quello digitale.

Situazione attuale nel mondo analogico, p. es. all'entrata di una discoteca:

- all'entrata della discoteca, il personale addetto alla sicurezza controlla il documento cartaceo per verificare se la persona in questione ha ad esempio già 18 anni ed è quindi autorizzata a entrare;
- il documento contiene in particolare l'immagine del viso, la data di nascita, il nome e il cognome e la nazionalità.

Situazione attuale nel mondo digitale, p. es. commercio elettronico:

- in molti casi si rinuncia alla verifica dell'età e ci si basa su un'autodichiarazione dell'utente. Questo tipo di misura non impedisce a minorenni di acquistare articoli non idonei alla loro età;

- la verifica mediante una foto o un video di un documento è relativamente complicata e quindi è richiesta solo raramente.

Aspetti centrali:

- nel caso di una verifica dell'età con un documento la parsimonia dei dati non è rispettata;
- metadati che possono risultare dalle procedure di verifica;
- protezione dei giovani insufficiente a causa di difficoltà tecniche elevate.

Situazione auspicata nel mondo analogico, p. es. all'entrata della discoteca:

- nel mondo reale l'Ie può essere usata alla stregua di un documento cartaceo;
- per la verifica dell'età sono necessarie soltanto due informazioni: la conferma di aver superato l'età minima richiesta e l'immagine del viso. Tali informazioni devono essere dedotte dall'Ie statale e trasmesse per la verifica senza rivelare altri dati. La protezione dall'uso illecito dell'immagine del viso è disciplinata nella legge sulla protezione dei dati.

Situazione auspicata nel mondo digitale, p. es. commercio elettronico:

- l'editore dell'Ie non viene a sapere quando essa è impiegata;
- per ottenere informazioni affidabili sull'età nella consultazione delle informazioni dell'Ie è integrato il processo «conferma dell'età minima richiesta», alla stregua di un processo di pagamento.

Utilità concreta per l'utente dell'Ie:

- il nome e la data di nascita non devono essere rivelati, il che contribuisce alla sicurezza in generale;
- per entrare in una discoteca non occorre un documento cartaceo;
- negli acquisti online la protezione dei giovani è migliore.

4.3.2 Apertura di un conto bancario

Il settore finanziario è uno dei settori più regolamentati. L'apertura di un conto bancario è disciplinato da numerose leggi e norme. È pertanto necessario avere certezza della persona che intende aprire un conto (know your customer). L'utilità per l'utente consiste nella trasmissione semplice della conferma dell'identità. È inoltre possibile inoltrare altre prove senza scansione e invio per mail, un'operazione critica dal punto di vista della protezione dei dati.

Situazione attuale:

- verifica dell'identità in loco: presentazione della carta d'identità o del passaporto; viene allestita una copia del documento e inserita negli atti;
- verifica dell'identità nelle procedure online, p. es. mediante fotografie di documenti e successiva identificazione video in processi online in parte automatizzati;
- verifica dell'identità mediante il versamento di un importo da un conto bancario esistente intestato allo stesso nome.

Aspetti centrali:

- onere elevato (di personale, finanziario, tecnico) per l'identificazione
- affidabilità molto elevata nell'associare identità e titolare in modo da attribuire le operazioni dell'identità senza ombra di dubbio al titolare (utilizzabilità in giudizio).

Situazione auspicata:

- l'Ie permette un'identificazione semplice, esclusivamente digitale e sicura;
- a seconda delle circostanze restano necessarie procedure di confronto a causa di prescrizioni settoriali, ad esempio le banche devono controllare la persona davanti allo schermo per mezzo dell'immagine del viso del documento digitale trasmesso in occasione dell'identificazione.

4.3.3 Estratto del registro delle esecuzioni

A chi si candida per un appartamento o per un impiego è di norma richiesto un estratto del registro delle esecuzioni, che deve essere ottenuto presso il competente ufficio d'esecuzione. Per l'utente l'utilità dell'Ie consiste nella semplicità della prova dell'identità quando ordina l'estratto presso uno dei 400 uffici di esecuzione e nel ricevere un estratto digitale del registro delle esecuzioni (prova) che successivamente può essere presentato un numero indeterminato di volte.

Situazione attuale:

- prima occorre trovare il competente ufficio d'esecuzione. Un sistema di ricerca è ad esempio offerto dalla piattaforma della Confederazione «EasyGov», che sostiene i richiedenti anche nel compilare correttamente la richiesta;
- successivamente la richiesta di estratto è di norma stampata, firmata e inoltrata per posta insieme a una copia del documento d'identità. A seconda dell'ufficio d'esecuzione è necessario pagare in anticipo l'emolumento;
- l'ufficio invia un estratto cartaceo al richiedente;
- l'utente invia l'estratto (originale o copia) al destinatario desiderato;
- sono offerti anche processi digitali se il richiedente dispone di una firma qualificata o incarica un terzo di procurare l'estratto facendo valere il proprio interesse;
- in questi casi l'ufficio d'esecuzione invia un documento pdf con firma digitale. Il destinatario può verificare l'autenticità del documento pdf mediante un'applicazione di validazione.

Aspetti centrali:

- trasmissione dell'estratto: spesso è necessario un documento originale;
- i processi presso il destinatario sono onerosi poiché non sono esclusivamente digitali e la validità della firma di un documento pdf deve essere verificata mediante un'applicazione di validazione;
- estratti cartacei manipolati, nel caso di destinatari che non chiedono un'originale riconoscibile.

Situazione auspicata:

- l'identità del richiedente può essere verificata mediante Ie;
- l'estratto digitale, in quanto prova, è trasmesso all'utente mediante un canale sicuro;
- l'utente può trasmettere direttamente l'estratto digitale a un destinatario;
- il sistema del destinatario può automatizzare i processi di verifica.

Utilità concreta per l'utente dell'Ie:

- non è necessario recarsi in un ufficio di esecuzione o alla posta;
- l'attestato originale può essere presentato un numero indeterminato di volte e pertanto non risultano ulteriori spese se lo stesso documento deve essere inoltrato a diversi servizi.

4.3.4 Login statale

Per usare i servizi di governo elettronico è spesso necessario un login per accedere alle relative piattaforme. L'autenticazione potrebbe essere affidata a un servizio statale e l'Ie potrebbe fungere da fattore d'autenticazione. L'utilità dell'Ie per l'utente consisterebbe nell'uso dei medesimi dati di login per diverse piattaforme di governo elettronico.

Situazione attuale:

- IdP o sistemi di gestione dell'identità divergenti di portali differenti implicano una moltitudine di credenziali per il login;
- molti Cantoni non dispongono ancora di una gestione dell'identità per possibili servizi di governo elettronico;
- non esiste un login statale usato su tutto il territorio nazionale.

Aspetti centrali:

- rendere possibile l'esercizio parallelo con soluzioni produttive esistenti;
- autenticazione sicura per mezzo di fattori d'autenticazione aggiuntivi.

Situazione auspicata:

- l'Ie costituisce un fattore (multiplo) d'autenticazione (elemento di possesso, eventualmente anche sapere segreto ed elemento biometrico);
- un servizio d'autenticazione statale garantisce un meccanismo d'autenticazione sicuro per tutti i portali statali di governo elettronico;
- l'identità e i diritti di accesso possono essere separati, il che conduce a notevoli semplificazioni nella costruzione e manutenzione delle applicazioni.

Utilità concreta per l'utente dell'Ie:

- uso dei medesimi dati di login per differenti piattaforme di governo elettronico;
- procedura di login sicura e quindi elevata protezione dell'accesso.

4.3.5 Firme elettroniche

Le firme elettroniche, disciplinate dal 2005 dalla legge sulla firma elettronica, sono state finora poco usate dai cittadini. L'utilità dell'Ie consiste nel semplificare l'accesso a una firma elettronica qualificata.

Situazione attuale:

- fornitori riconosciuti mettono a disposizione i servizi necessari per le firme elettroniche;
- all'inizio il fornitore procede all'identificazione dell'utente; per la firma qualificata è necessaria la comparizione di persona. Successivamente all'utente viene rilasciato un certificato qualificato;
- usando un certificato qualificato si possono firmare documenti in modo digitale e legalmente valido;
- la verifica di documenti muniti di firma digitale può essere effettuata per mezzo di un'applicazione di validazione.

Aspetti centrali:

- accesso complicato alla firma qualificata poiché è obbligatorio presentarsi di persona.

Situazione auspicata:

- accesso semplice alla possibilità di realizzare firme elettroniche qualificate
- promozione dello scambio digitale di documenti contrattuali.

Utilità concreta per l'utente dell'Ie:

- la conclusione digitale legalmente valida di contratti scritti diventa la soluzione standard grazie alla firma elettronica qualificata con il conseguente risparmio di tempo e spese.

4.4 Basi legali

L'analisi delle basi legali della futura legge e l'elaborazione del progetto di legge non sono oggetto del presente documento. Per elaborare le basi legali dell'Ie statale occorre prima scegliere il livello di ambizione auspicato nonché una delle possibili varianti.

4.5 Comunicazione

Per introdurre un'Ie statale è fondamentale una buona comunicazione con tutti sin dall'inizio: potenziali utenti, Cantoni, economia privata, organizzazioni e Amministrazione federale devono essere coinvolte nella realizzazione dell'Ie affinché la sostengano. Occorre sempre concentrarsi sull'utilità per la collettività e analizzare i possibili casi e le possibili forme di applicazione. La discussione sulle questioni tecnologiche segue soltanto in un secondo momento.

Oltre alle procedure di partecipazione usuali, ulteriori cerchie vengono, laddove possibile, coinvolte mediante piattaforme di discussione interattive e test pubblici d'intrusione.

5 Possibili soluzioni Ie

5.1 Soluzione Ie per mezzo della Self-Sovereign Identity

5.1.1 Approccio

Self-Sovereign Identity (SSI) è la soluzione più recente per un ecosistema di Ie tra quelle proposte nel presente documento. Nel 2016 Christopher Allen ha formulato 10 principi riferiti agli utenti e alla protezione dei dati sui quali deve fondarsi l'idea di «identità gestite autonomamente»[6], ossia identità sulle quali l'utente ha il maggior controllo possibile. Ciò corrisponde alla tendenza attuale di porre al centro dell'attenzione i temi della protezione e della sicurezza dei dati nonché della dipendenza da sistemi d'identità centrali, il che si riflette anche nelle mozioni menzionate nel capitolo 2.2. Nel contempo si cercano risposte alla questione del modo di collegare i sistemi in maniera universale senza dover definire continuamente nuove interfacce.

In pochi anni sono stati sviluppati standard flessibili, framework tecnici e un'architettura univoca per attuare la SSI. Non si tratta di un approccio rivoluzionario, ma basato sulle conoscenze delle infrastrutture a chiave pubblica e delle procedure crittografiche più recenti. Pertanto già oggi sono in esercizio ecosistemi di SSI produttivi, anche se ancora nessuno Stato rilascia Ie basate su tale soluzione. Anche gli sviluppi più recenti nell'UE vanno in questa direzione.

In linea di principio la soluzione della SSI è ideale per il livello di ambizione 3: un ecosistema di prove digitali. È tuttavia adeguato per tutti i livelli di ambizione e vi sono soltanto differenze nella governanza poiché i mezzi tecnici utilizzati sono identici.

[6] Self-Sovereign Identity è spesso tradotto con «identità autogestita» poiché p. es. una prova statale dell'identità è rilasciata dallo Stato ed è trasmessa all'utente per l'uso e la gestione.

5.1.2 Come funziona

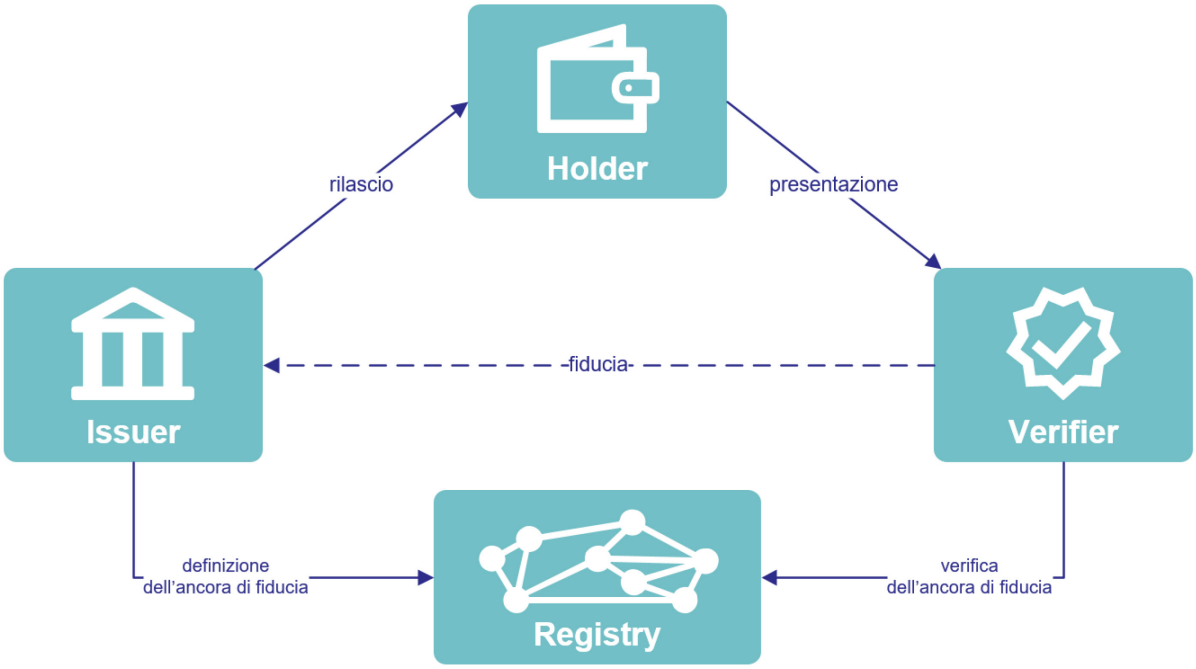


Illustrazione 1: architettura di base della SSI

Il triangolo «servizio di rilascio (Issuer) – utente (Holder) – verificatore (Verifier, Relying Party)» è presente in molte architetture di fiducia. Nel caso della SSI è determinante che i collegamenti illustrati rappresentino direttamente i flussi di comunicazione, senza istanze intermedie. Il flusso di dati tra il servizio di rilascio e l'utente nonché l'utente e il verificatore avviene in forma di comunicazione criptata peer-to-peer. Di norma, il canale di comunicazione è istituito per mezzo di un codice QR.

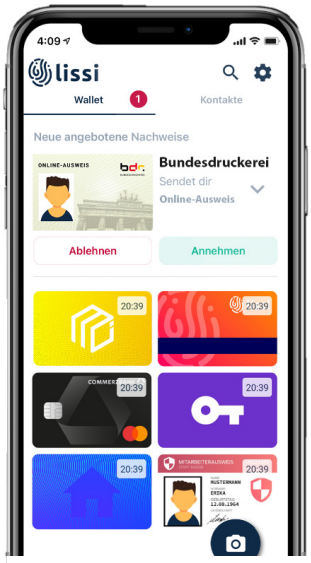


Illustrazione 2: esempio di wallet che l'utente usa per ricevere, gestire e presentare credenziali verificate (fonte: I-Dunion, lissi)

Il servizio di rilascio trasmette all'utente le credenziali verificate. L'utente le salva in un wallet sullo smartphone. Il verificatore può richiedere dati all'utente mediante il canale di comunicazione sicuro. Quando risponde alla richiesta, l'utente può decidere quali dati trasmettere effettivamente al verificatore. Si può trattare di tutte le credenziali verificate, di una parte di esse o di dati registrati dall'utente stesso.

Per controllare l'autenticità dei dati digitali verificati, le prove crittografiche – non i dati – sono a disposizione in una memoria con ancore di fiducia elettroniche (cosiddetta registry). Una registry è di solito un registro decentrale (p. es. DLT, blockchain) in cui ogni utente ha depositato la sua identità e la sua chiave pubblica. Il verificatore può controllare i dati presentati dall'utente senza contattare il servizio di rilascio o un terzo. Il rapporto di fiducia tra il verificatore e il servizio di rilascio si basa su un contatto personale o su una referenza pubblica (p. es. informazione su un sito web).

I dati digitali verificati possono essere impostati come «annullabili/revocabili». Il servizio di rilascio ha quindi la possibilità di dichiararli nulli

in qualsiasi momento e senza contattare l'utente. La relativa informazione è inserita nella registry in un elenco di revoche.

Il caso di applicazione minimo per l'Ie è il seguente:

- mediante una procedura completamente automatizzata lo Stato (servizio di rilascio) mette a disposizione dell'utente l'Ie sotto forma di credenziali verificate;
- l'utente gestisce in un wallet le credenziali verificate;
- qualsiasi terzo (verificatore) può chiedere l'Ie o parti di essa e verificarne l'autenticità dopo la trasmissione controllata e autorizzata dall'utente.

5.1.3 Componenti gestite dallo Stato

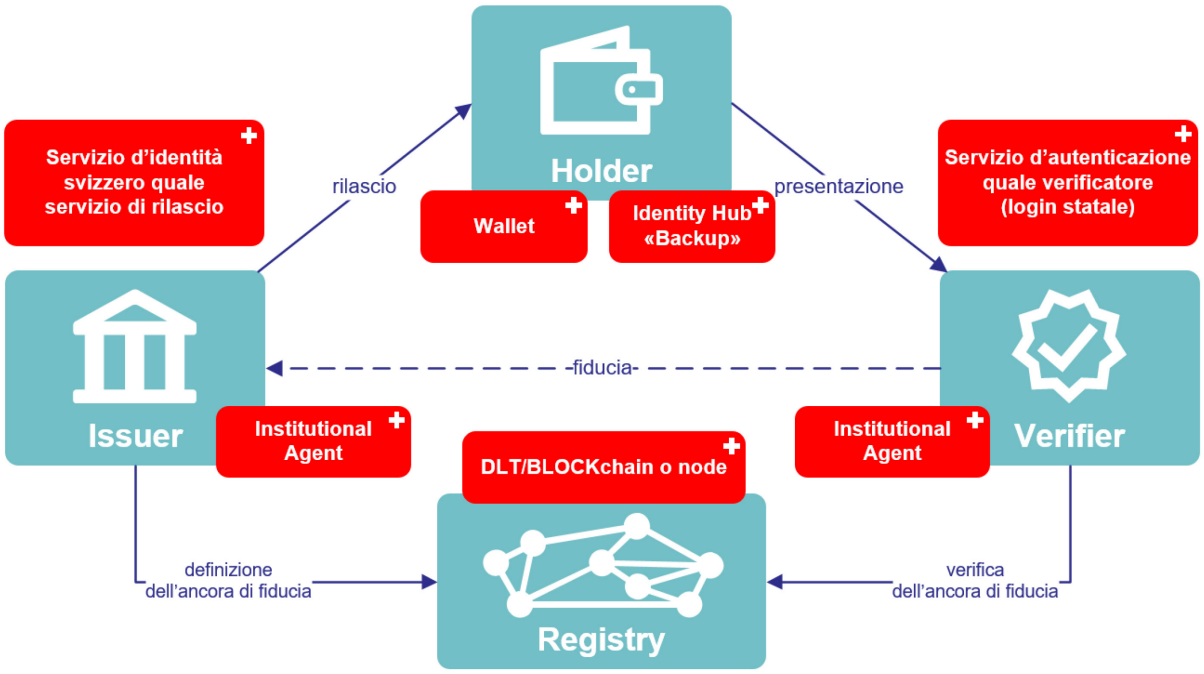


Illustrazione 3: panoramica delle componenti gestite o messe a disposizione dallo Stato (campi rossi) in un'architettura SSI

L'Illustrazione 3 riporta in rosso le seguenti singole componenti tecniche che secondo le richieste delle mozioni devono essere gestite o messe a disposizione dallo Stato sotto forma di software liberamente accessibili.

- **Servizio d'identità svizzero SID:** processo digitale automatizzato per la validazione, determinazione e verifica di una persona. Il risultato del processo (con l'aiuto di un institutional agent) è il rilascio e la trasmissione di una credenziale verificata, che costituisce l'Ie.
- **Institutional agent:** software per il rilascio e la verifica di credenziali verificate, che un'API (interfaccia tecnica) mette a disposizione per tutte le funzioni.
- **Wallet:** applicazione per smartphone per la gestione sicura di credenziali.

- **Registry:** memoria di dati con ancore di fiducia elettroniche usata da tutti i partecipanti all'ecosistema di Ie e di norma realizzata sotto forma di registro distribuito (distributed ledger DLT), ad esempio per mezzo di una blockchain. Nella memoria sono registrate prove crittografiche, identità e chiavi pubbliche dei servizi di rilascio, definizioni e schemi di credenziali, ma mai dati personali o materiali.
- **Identity hub «backup»:** componente per agevolare la portabilità e il backup dei propri credenziali. Pur non essendo necessaria per la funzionalità minima dell'Ie, l'identy hub è raccomandabile per garantire la facilità dell'utilizzazione a lungo termine e la soddisfazione degli utenti in un ecosistema con molte credenziali.
- **Servizio d'autenticazione:** servizio di login per piattaforme statali ed eventualmente anche private. L'Ie è usata come mezzo (multiplo) d'autenticazione.

Secondo quanto chiesto dalle mozioni menzionate al capitolo 2.2, la gestione della soluzione di Ie deve essere di competenza di un'autorità statale. Il caso minimo di applicazione deve quindi essere realizzato esclusivamente con componenti messe a disposizione o gestite dallo Stato. La flessibilità tecnica su cui si fonda l'ecosistema permetterebbe tuttavia anche ai fornitori privati di mettere a disposizione componenti (soprattutto institutional agent, wallet, identity hub). Quanto alla registry, è ipotizzabile che lo Stato ne metta a disposizione una parte (node) o l'intero sistema, ad esempio coinvolgendo i Cantoni.

Le componenti SID, IdP e identity hub sono sistemi esterni, che l'ecosistema SSI sfrutta per il rilascio, la trasmissione e la verifica dell'autenticità dell'Ie.

Attualmente si stanno sviluppando gli standard per un'interazione che permetta di sviluppare indipendentemente le singole componenti su incarico dello Stato. Le interdipendenze tecniche tra i singoli elementi si limitano alla definizione degli standard.

5.1.4 Vantaggi e svantaggi della soluzione SSI

Vantaggi:

- la filosofia della SSI si fonda sulla protezione e la parsimonia dei dati nonché sul principio «privacy by design» e soddisfa le richieste delle mozioni;
- l'approccio generico offre molte possibilità di applicazione e molti scenari di utilizzazione ed è molto simile a un «portafoglio» reale:
- l'utente ha una panoramica completa delle transazioni ricevute e inviate;
- al momento l'evoluzione internazionale va decisamente in questa direzione; sono in corso molti progetti e iniziative basate su questa soluzione;
- interfacce libere e standardizzate rendono possibile la connessione di altri sistemi;
- fornisce un canale di comunicazione criptato peer-to-peer tra le parti. Oltre alle credenziali verificate attraverso il canale protetto possono essere trasmesse anche altre comunicazioni;
- le tecnologie di base sono a disposizione come open source.

Svantaggi:

- soluzione relativamente recente; alcune questioni di fondo non sono ancora definitivamente chiarite e gli standard non sono ancora completi;
- deve prima diffondersi un'ampia consapevolezza delle possibilità di questa soluzione globale (rispetto a un login);
- la responsabilità per la gestione delle credenziali verificate è conferita del tutto all'utente, il che rende praticamente impossibili prestazioni di sostegno del servizio di rilascio;
- l'utilizzabilità in giudizio è difficile, poiché il sistema è decentrale e protetto crittograficamente. In caso di abuso dell'Ie o di altre prove ciò può rendere difficile dimostrare una manipolazione da parte di terzi;
- wallet di elevata sicurezza per applicazioni speciali dovrebbero basarsi su elementi sicuri (secure elements) negli smartphone. Al momento tuttavia non tutti gli smartphone li contengono e gli strumenti per svilupparli non sono ancora completi e facilmente disponibili.

5.1.5 Coinvolgimento di piattaforme cantonali di governo elettronico

Da una parte, sulle piattaforme di governo elettronico cantonali potrebbero essere implementate prove dell'identità mediante l'Ie, quale tappa del processo analogamente a un processo di pagamento; dall'altra sarebbe possibile l'uso del servizio d'autenticazione statale.

Inoltre i Cantoni, ed eventualmente anche i Comuni, potrebbero sfruttare l'ecosistema per fungere essi stessi da servizio di rilascio e rilasciare prove proprie (p. es. attestato di domicilio, licenza di circolazione).

In un ecosistema con il livello di ambizione 3, nel quale fungono da servizi di rilascio anche attori privati, sarebbero ipotizzabili molte altre agevolazioni da parte delle piattaforme di governo elettronico cantonali: i certificati di salario e dei conti bancari rilasciati rispettivamente dai datori di lavoro e dalle banche sotto forma di credenziali verificate potrebbero essere inoltrati direttamente in occasione della dichiarazione delle imposte online, il che semplificherebbe i processi successivi.

5.1.6 Questioni irrisolte della soluzione SSI

Gli specialisti in materia concordano in generale sugli aspetti fondamentali della SSI. Le discussioni si concentrano sugli aspetti della governance e sui processi esterni alla SSI:

- Quali sono livelli di governance e chi ne è responsabile (p. es. livelli di governance secondo trust over IP framework: ecosistema, credenziali, provider, utility)?
- Lo Stato deve possedere un monopolio su determinate componenti? I wallet devono essere certificati? La scelta dei wallet e dell'institutional agent è lasciata all'utente? Vi è una regolamentazione indicante quali parti vanno allestite e gestite in modo cooperativo e quali in modo concorrenziale?
- Chi gestice la registry? È necessaria una registry nazionale o si opta per la connessione a un ecosistema internazionale esistente? I Cantoni, le città o le imprese private

vogliono o devono essere abilitati a gestire nodi di memorizzazione (node)? Quale tecnologia va favorita? Quale ruolo svolge la quantità di dati? Come risolvere le questioni dell'interoperabilità con altre registry? Il servizio di rilascio può addirittura scegliere liberamente la registry?

- Chi può fungere da servizio di rilascio? Il sistema resta completamente disponibile per ulteriori casi di applicazione o i servizi di rilascio vengono appositamente scelti o autorizzati?
- Come rendere possibili i backup e il trasferimento di credenziali verificate? Come evitare backup centrali che possono diventare obiettivo degli attacchi di hacker? Quale ruolo svolge la possibile connessione crittografica tra wallet e credenziali verificate?
- Quali meccanismi di sicurezza sono necessari per l'accesso al wallet?
- Come si potrebbero usare su diversi apparecchi le credenziali verificate? Quando sarebbe necessario? È sufficiente che con un determinato smartphone può essere allestito un collegamento con il verificatore, a prescindere dall'apparecchio su cui si avvia il processo per il quale è richiesta l'Ie?
- Chi definisce lo schema delle credenziali? È necessario un servizio designato per la definizione e il coordinamento (p. es. eCH) oppure le definizioni sono sviluppate a seconda del ramo?
- È necessario un servizio di autenticazione statale? Sarebbe sensato collegare il processo di rilascio e il deposito di fattori di autenticazione per approfittare dell'oneroso processo di identificazione in occasione del rilascio e permettere un'elevata sicurezza nel processo di autenticazione?

5.2 Soluzione Ie mediante infrastruttura a chiave pubblica

5.2.1 Approccio

L'infrastruttura a chiave pubblica (PKI) è attualmente già impiegata dallo Stato per validare i dati dei documenti d'identità muniti di microchip (passaporto, carta di soggiorno). In qualità di autorità di rilascio, la Confederazione firma digitalmente i dati prima che questi siano memorizzati nel microchip e, pubblicando la chiave pubblica, permette a tutti i verificatori di validarli. Questa tecnica è standardizzata da oltre 30 anni ed è applicata in tutto il mondo alle tecnologie più diverse. L'applicazione più recente della soluzione PKI è il certificato COVID.

L'approccio della PKI è simile a quello della SSI. Un'Ie rilasciata sotto forma di certificato (X.509) è un'identità decentrale di esclusivo controllo, e quindi anche di esclusiva responsabilità, dell'utente. Nell'uso dell'Ie, è rispettata la sfera privata dell'utente nei confronti del servizio di rilascio, poiché quest'ultimo non è a conoscenza dell'impiego dell'Ie. È tuttavia molto difficile realizzare l'obiettivo della parsimonia dei dati, dato che l'Ie è firmata nella sua globalità e quindi può essere trasmessa soltanto globalmente al verificatore per l'accertamento dell'identità.

Questa soluzione soddisfa l'obiettivo di una prova digitale applicabile nel mondo analogico e in quello digitale. L'applicazione online di questo tipo di certificati è standardizzata (Mutual TLS Authentication). Per l'applicazione nel mondo analogico si sono affermate diverse procedure basate su codici QR (p. es. Swiss Pass nell'applicazione FFS, certificato COVID), anche se manca un'applicazione offline standardizzata.

L'approccio generico del rilascio di certificati permette di realizzare tutti i livelli di ambizione. È possibile la connessione logica o matematica di prove. Pur essendo tecnicamente possibile

anche il coinvolgimento di servizi di rilascio privati, la soluzione PKI è usata di norma soltanto da servizi di rilascio di un gruppo controllato o controllabile.

5.2.2 Come funziona

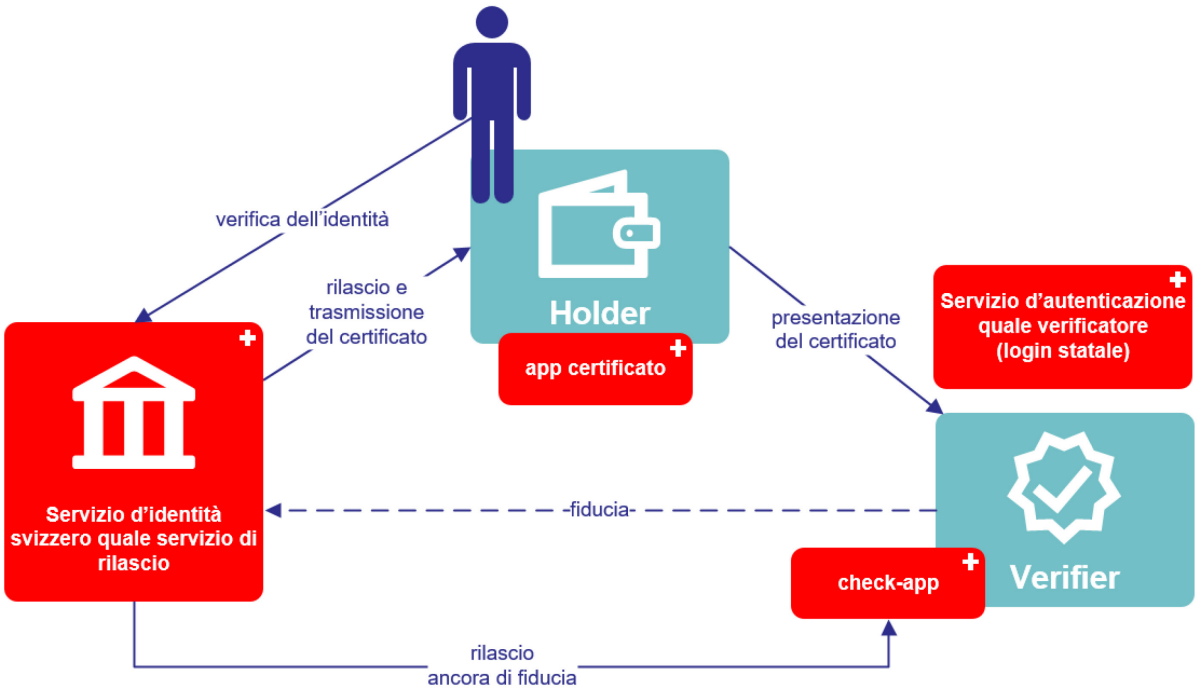


Illustrazione 4: architettura di una soluzione PKI

Il triangolo di fiducia «servizio di rilascio (Issuer) – utente (Holder) – verificatore (Verifier, Relying Party)» sussiste anche in questo caso. La comunicazione avviene nel modo illustrato, ma rispetto alla soluzione SSI sono possibili canali di comunicazione differenti.

Dopo aver verificato l'identità, il servizio responsabile (Issuer) rilascia e trasmette il certificato all'utente (Holder). Questi lo salva in un'apposita applicazione in cui è conservato in modo sicuro e non può essere copiato. In caso di necessità l'utente può presentare il certificato a un verificatore mediante un canale digitale o un codice a barre. In tale occasione vengono rivelati tutti i dati firmati. Una volta ricevuto il certificato, il verificatore può controllarne la validità mediante un'applicazione di verifica. In questa applicazione è fornita direttamente la chiave pubblica del servizio di rilascio e quindi la verifica è possibile anche senza connessione a Internet.

Per dichiarare nulli certificati già rilasciati il servizio di rilascio tiene un elenco di tutti i certificati revocati. Affinché il verificatore non indichi troppo apertamente al servizio di rilascio quando effettua un controllo, per ricevere l'elenco delle revoche esistono diversi protocolli e procedure tesi a rafforzare la protezione dei dati. L'elenco delle revoche può essere ricevuto online in tempo reale, periodicamente o anche in modo decentrale mediante autoconsultazione.

5.2.3 Componenti gestite dallo Stato

L'Illustrazione 4 riporta in rosso le seguenti componenti tecniche che secondo le richieste delle mozioni devono essere gestite o messe a disposizione dallo Stato sotto forma di software liberamente accessibili.

- **Servizio d'identità svizzero SID:** sistema per il processo digitale automatizzato per la validazione, risoluzione e verifica di una persona. Il risultato del processo è il rilascio e la trasmissione del certificato, che costituisce l'Ie. Inoltre il sistema gestisce un elenco delle revoche e lo mette a disposizione per consultazione.
- **App certificato:** applicazione per ricevere, salvare e presentare certificati.
- **Check-app:** applicazione per ricevere, indicare e controllare certificati.
- **Servizio d'autenticazione:** servizio di login per piattaforme statali ed eventualmente anche private. L'Ie è usata come mezzo (multiplo) d'autenticazione.

5.2.4 Vantaggi e svantaggi della soluzione PKI

Vantaggi:

- uso di tecniche e tecnologie consolidate da anni e molto diffuse;
- permette la realizzazione di varianti e requisiti molto diversi;
- identità e loro uso decentrali. L'uso non crea ulteriori metadati. L'applicazione tiene conto del principio «privacy by design»;
- sostiene l'idea che l'Ie è un documento e non solo un login.

Svantaggi:

- il compito della salvaguardia dell'identità è conferito completamente all'utente e una maggiore affidabilità della sicurezza di custodia e d'impiego è quasi sempre connessa a ulteriori hardware (p. es. per la protezione da copie o un'autenticazione multifattoriale forte);
- in linea di principio, i certificati possono essere presentati solo per intero. Per rispettare la parsimonia dei dati sono ipotizzabili certificati parziali, ma in tal caso l'utente dovrebbe richiedere e gestire più certificati Ie; la scelta di singoli attributi in funzione della situazione si presenta complicata;
- diversi possibili canali di trasmissione tra servizio di rilascio, utente e verificatore ostacolano l'uso corretto e sicuro dei certificati.

5.2.5 Coinvolgimento di piattaforme cantonali di governo elettronico

Sulle piattaforme cantonali di governo elettronico potrebbero essere implementate prove dell'identità mediante l'Ie, quale tappa del processo analogamente a un processo di pagamento; dall'altra sarebbe possibile usare il servizio d'autenticazione statale.

Inoltre i Cantoni, ed eventualmente anche i Comuni, potrebbero sfruttare l'ecosistema per fungere essi stessi da servizio di rilascio e rilasciare certificati propri (p. es. attestato di domicilio, licenza di circolazione).

5.2.6 Soluzioni PKI basate su una carta

Invece di un'applicazione contenente i certificati sullo smartphone, anche una carta munita di microchip potrebbe essere un luogo di registrazione sicuro. Per presentare il certificato è necessario un apparecchio di lettura della carta: nel mondo analogico deve possederne uno il verificatore, in quello digitale l'utente. Molti modelli attuali di smartphone permettono la lettura di carte munite di microchip. In assenza di questa possibilità è necessario un apparecchio specifico di lettura.

La SuisseID e il nuovo documento di legittimazione tedesco (neuer Personalausweis, nPA) si fondano entrambi sul suddetto principio e permettono anche un'identificazione digitale. In entrambi i casi queste soluzioni non si sono imposte su vasta scala e l'uso stesso della carta costituisce solo uno degli ostacoli. Su scala internazionale si sta delineando la rinuncia a sistemi di Ie con carte munite di microchip. I sistemi più promettenti puntano sull'uso di dispositivi mobili/smartphone con applicazioni specifiche, poiché la facilità del loro uso implica una maggiore popolarità di tali sistemi. A titolo di esempio si può menzionare l'Estonia, un Paese pioniere nel settore del governo elettronico, che ha cominciato con una carta munita di microchip, successivamente è passata a un'Ie sul cellulare connessa a una carta SIM e oggi offre in primo luogo una soluzione del tutto dematerializzata basata su un'applicazione (smart-ID). Anche in Germania si sta cercando una soluzione che permetta di registrare in modo sicuro i dati del nPA sullo smartphone, in modo da rendere superfluo l'uso della carta fisica. La Svizzera potrebbe approfittare di queste esperienze.

A sfavore dell'attuazione concreta mediante una carta d'identità statale munita di microchip, analogamente al nPA, si possono menzionare, in aggiunta a quelli già esposti, i motivi seguenti:

- nei prossimi anni è prevista l'introduzione di una nuova carta d'identità. Tuttavia, la funzionalità dell'Ie non era parte dell'appalto pubblico e dovrebbe quindi essere acquisita posteriormente. Questo vale anche per tutti i documenti per stranieri e per rappresentanti del corpo diplomatico;
- a causa della durata di validità, il roll-out di un documento d'identità fisico in Svizzera dura almeno 10 anni (più il tempo di preparazione). Non è sensato far dipendere l'introduzione dell'Ie dal ciclo di rinnovo della carta d'identità.
- l'impiego di un supporto fisico per trasmettere dati sulla persona limita la scelta e le possibilità di una futura soluzione di Ie.

5.2.7 Questioni irrisolte della soluzione PKI

- Sono necessari certificati specifici d'applicazione per l'Ie? Potrebbero essere ridotti a un numero esiguo?
- Quali sarebbero i vantaggi di una public key directory, ossia un'istanza di gestione delle chiavi pubbliche e degli elenchi delle revoche? Come andrebbero valutate le differenze con l'approccio della SSI?
- È necessario un servizio di autenticazione statale? Sarebbe sensato collegare la procedura di rilascio e il deposito di fattori di autenticazione in modo da trarre profitto dall'onerosa procedura di identificazione in occasione del rilascio e garantire un'elevata sicurezza in occasione della procedura di autenticazione?

5.3 Soluzione Ie per mezzo di un fornitore d'identità (IdP) statale centrale

5.3.1 Approccio

La legge sull'Ie, respinta in votazione, prevedeva una soluzione Ie che coinvolgeva fornitori d'identità riconosciuti statali e privati. L'idea era mettere quanto prima un'Ie a disposizione di un'ampia cerchia di utenti e creare nel contempo delle possibilità di applicazione. Il coinvolgimento di privati è però stato uno dei motivi che ha condotto al rigetto della legge sull'Ie nella votazione popolare.

L'idea di fondo di mettere a disposizione degli utenti un'identità elettronica verificata dallo Stato sulla base di un login può essere realizzata anche con un fornitore d'identità centrale dello Stato. Rispetto all'architettura prevista dalla legge sull'Ie respinta, questo approccio più semplice rende obsolete determinate questioni relative all'interoperabilità e al flusso dei dati, ma ostacola una diffusione rapida dell'uso. L'esercizio del sistema compete alla Confederazione. Questa soluzione permette in primo luogo un login statale univoco di governo elettronico.

Le basi e i protocolli tecnologici (p. es. openID connect) necessari per questa soluzione sono consolidati e idonei per il livello di ambizione 1. Per contemplare livelli di ambizione più elevati sono necessari ampliamenti attualmente in fase di sviluppo.

5.3.2 Come funziona

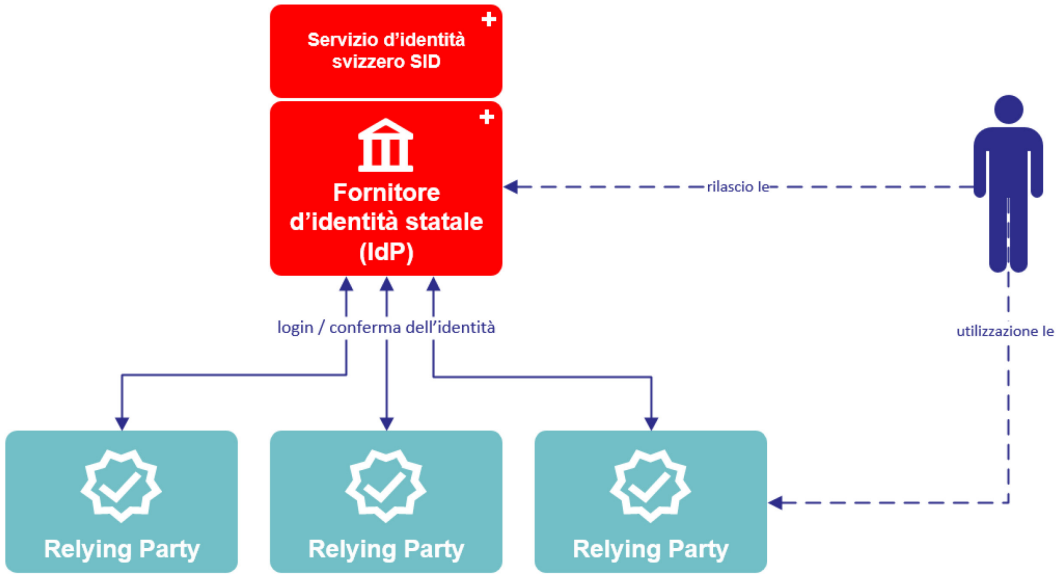


Illustrazione 5: panoramica dell'architettura di una soluzione Ie basata su un fornitore d'identità statale centrale

Il fulcro di questa soluzione è un fornitore d'identità statale che gestisce l'Ie dell'utente, la quale può essere usata mediante un processo di login. Al fornitore d'identità possono collegarsi varie «relying party», per esempio piattaforme cantonali di governo elettronico. Vi sono due possibilità:

- la relying party sfrutta il servizio IdP per la gestione attiva dell'identità istituendo un conto login dell'utente per mezzo dell'IdP statale;

- la relying party usa il servizio IdP soltanto come documento che permette all'utente di renderle noti determinati attributi dell'Ie, senza che l'IdP statale assuma la funzione della gestione dell'identità.

L'utente chiede il rilascio di un'Ie direttamente all'IdP statale. Per la verifica completa dell'identità quest'ultimo si serve del Servizio d'identità svizzero (cfr. 5.4 procedura di rilascio Ie).

Collegandosi a un'Ie le relying party potrebbero offrire prove connesse (livello di ambizione 2). Sarebbe possibile l'uso di una tecnologia indipendente dall'IdP, ad esempio in analogia all'approccio PKI (cfr. cap. 5.2).

5.3.3 Componenti gestite dallo Stato

La portata ristretta di un ecosistema con un IdP centrale si ripercuote sull'attuazione. L'illustrazione 5 mostra in rosso le seguenti componenti che secondo la richiesta delle mozioni dovrebbero essere gestite sotto la responsabilità dello Stato o messe a disposizione come software liberamente accessibili.

- **Servizio d'identità svizzero SID:** sistema per il processo digitale completamente automatizzato per la validazione, risoluzione e verifica di una persona. Il risultato del processo è la trasmissione della conferma della verifica all'IdP per allestire l'Ie.
- **Fornitore d'identità:** fornitore d'identità (IdP) statale che gestisce l'Ie e la rende utilizzabile, mediante un processo di login, per relying party statali o eventualmente anche private.

5.3.4 Vantaggi e svantaggi della soluzione IdP

Vantaggi:

- architettura semplice, soluzione chiara;
- tecnologie e protocolli ampiamente utilizzati;
- la connessione della verifica della persona e del login per l'Ie la rende una possibilità di login sicura.

Svantaggi:

- la soluzione è contraria ai principi richiesti dalle mozioni. Non è decentrale e non è rispettata la «privacy by design», poiché si basa sulla piena fiducia nei confronti dell'IdP. Le preoccupazioni in merito alla parsimonia dei dati e ai metadati sono un po' mitigate dal fatto che la responsabilità globale del sistema compete alla Confederazione e perciò è possibile un controllo preciso;
- il problema dell'uovo e della gallina è irrisolto: le esperienze all'estero indicano che le probabilità di una rapida adozione da parte degli utenti come pure di una rapida connessione volontaria di possibili servizi sono esigue;
- probabilità di utilizzazione limitate e uso piuttosto difficile nel mondo analogo;
- è difficile estendere l'ecosistema a livelli di ambizione più elevati;
- nessuna separazione tra rilascio dell'Ie, da una parte, e il suo uso dall'altra, il che è contrario all'uso odierno dei documenti d'identità e non corrisponde al pendant nel mondo analogico;

- la connessione dell'Ie con altre prove è possibile solo con i servizi collegati, il che rende complicata l'applicazione delle prove;
- non rispetta il principio «Ie = documento digitale»;
- dipendenza del sistema da un IdP.

5.3.5 Coinvolgimento di piattaforme cantonali di governo elettronico

L'IdP centrale è collegato alle piattaforme cantonali di governo elettronico. La gestione degli accessi e dei ruoli resta di competenza della rispettiva piattaforma, l'identità è tuttavia fornita dall'IdP della Confederazione che garantisce una procedura di login sicura. Questo potrebbe rappresentare un'agevolazione per i Cantoni che non possiedono ancora una soluzione propria di login e uno sgravio per i Cantoni che oggi gestiscono un proprio IdP. I Cantoni con un IdP proprio potrebbero collegare alla propria piattaforma di governo elettronico anche l'IdP della Confederazione, il che significa in pratica stabilire una connessione tra un'identità già esistente presso il proprio IdP e l'identità fornita dall'IdP della Confederazione e non una gestione parallela. Va tuttavia osservato che soprattutto per le applicazioni mobili è difficile realizzare un'architettura con più IdP (refresh-token ecc.). Se si usa un IdP federale per una piattaforma cantonale bisognerebbe tenere debitamente conto del servizio di supporto, in modo da garantire che gli utenti possano rivolgersi a un centro di contatto in caso di problemi.

In linea di principio sarebbe possibile una federazione di IdP cantonali già esistenti, il che garantirebbe una certa decentralizzazione (regionalizzazione) grazie alla distribuzione su diversi sistemi. Rispetto a una soluzione IdP centrale, i sistemi federativi richiedono un onere maggiore oltreché una maggiore regolamentazione e più meccanismi di controllo (standard, livello di affidabilità dell'identità, protezione dei dati, ecc.). Nello sviluppo di altre funzioni, ad esempio i certificati di età, dovrebbero essere prima fissati gli standard e poi ogni IdP sarebbe costretto a realizzare le nuove funzioni. Solo così tutti gli utenti potrebbero usare le stesse funzioni, a prescindere dall'IdP cantonale. Nonostante il riutilizzo degli IdP di alcuni Cantoni, si stima che le spese per lo Stato sarebbero notevolmente maggiori rispetto all'attuazione di un IdP statale centrale da collegare alle piattaforme cantonali.

5.3.6 Questioni irrisolte della soluzione IdP

- Chi può usare l'Idp centrale statale come fornitore di login e per la conferma di determinati attributi? La connessione è riservata a piattaforme statali o è a disposizione anche dei sistemi dell'economia privata?
- Quali piattaforme di governo elettronico si connetterebbero a un IdP statale? Quanti Cantoni hanno ancora bisogno di una soluzione IdP al momento dell'attuazione?
- Per i Cantoni e altre relying party è sensata l'esternalizzazione del login?
- Chi è partner contrattuale delle relying party e responsabile della stipula del contratto? Quali condizioni devono soddisfare le relying party? In che modo è garantito il controllo?

5.4 Procedura di rilascio dell'Ie

La procedura di rilascio è indipendente dalla soluzione scelta. Sono necessarie le seguenti tappe:

- il richiedente presenta una prova della sua identità;
- si verifica che la persona corrisponda alla prova dell'identità;
- lo Stato rilascia l'Ie alla persona in questione.

Per la diffusione rapida e semplice dell'Ie è auspicabile una procedura online automatizzata, come applicata ad esempio in Italia. Questo non esclude il supporto presso sportelli reali. Lo Stato gestisce il sistema necessario a tal fine e, mediante un canale sicuro, trasmette la prova digitale al richiedente.

Seguendo il principio secondo cui devono essere possibili la parsimonia dei dati e degli attributi derivati, si può osservare il contenuto di un'Ie sotto un altro punto di vista: non occorre rinunciare, per motivi inerenti alla protezione dei dati, a determinati attributi poiché il controllo sulla trasmissione di ogni singolo attributo compete all'utente. L'Ie comprende i dati presenti su un documento d'identità cartaceo: nome e cognome, data di nascita, immagine del viso, luogo di attinenza, luogo di nascita, nazionalità, data di rilascio. È ipotizzabile integrare anche il numero AVS, poiché è necessario per molte pratiche con le autorità e sarebbe pertanto pratico per l'utente.

Per garantire un'elevata interoperabilità su scala internazionale, è auspicabile un alto livello di sicurezza per il rilascio di un'Ie (identificazione e verifica). Tuttavia, il livello di sicurezza di un'Ie non dipende esclusivamente dalla procedura di rilascio. Per la memorizzazione e la presentazione di una determinata prova o di un documento digitale, a seconda del tipo di attuazione, sono possibili diversi livelli di sicurezza. Non ha quindi senso fissarsi su un livello di sicurezza e per ogni caso di applicazione è necessario osservare l'intera catena di fiducia, nel caso ideale con un elemento di alta affidabilità: l'Ie.

I dettagli dell'attuazione della procedura di rilascio devono ancora essere elaborati e non sono quindi oggetto del presente documento.

6 Attuazione

6.1 Scadenze

Dopo la discussione pubblica delle questioni sollevate dal presente documento e la sua analisi, il Consiglio federale prenderà una decisione di fondo probabilmente entro la fine del 2021. In base alle direttive di tale decisione sarà elaborato un avamprogetto di legge da porre in consultazione entro la metà del 2022. Seguiranno l'elaborazione del messaggio, il dibattito parlamentare, un eventuale referendum e l'emanazione delle disposizioni esecutive. Il momento dell'introduzione di un'Ie statale dipenderà dalla durata di questo processo.

Per guadagnare tempo, parallelamente al processo legislativo si potrà avviare la pianificazione dell'attuazione e l'attuazione stessa. Già nel corso della pianificazione dell'attuazione tecnica potrebbero essere realizzate prime applicazioni pilota e proof of concept al fine di chiarire nella pratica eventuali questioni. Dopo primi dibattiti orientativi in Parlamento potrebbero poi essere avviati bandi concorso e lavori di sviluppo.

6.2 Stima dei costi per le diverse soluzioni Ie

Come per la pianificazione delle scadenze, vi sono molte incognite anche per la stima dei costi. In mancanza di requisiti ben definiti non è possibile una stima affidabile. Si può presumere che tutte le soluzioni presentate nel presente documento genereranno costi simili. Per questo motivo rinunciamo al momento a una stima dei costi. Questi ultimi si possono suddividere su tre ambiti:

1) spese per l'implementazione, la gestione e lo sviluppo dei sistemi funzionali e tecnici;
2) spese per la promozione dell'utilità dell'Ie e del suo impiego da parte degli utenti, l'economia e lo Stato mediante la comunicazione nonché programmi pilota e di promozione;
3) spese per garantire la compatibilità e assicurare una maggiore utilità (internazionale, federale, esigenze dell'economia).

Per loro natura le spese aumenteranno in concomitanza con la crescita del livello di ambizione, che però implica anche una maggiore utilità.

6.3 Possibilità di finanziamento

Se uno degli obiettivi principali è creare una «piattaforma usata da molti», va preso in considerazione il finanziamento mediante sussidi statali: lo Stato se ne assume le spese e lo considera un contributo di base per la digitalizzazione della Svizzera. Gli abitanti della Svizzera si aspettano che l'identità digitale statale sia una prestazione di base dello Stato.

Pur non adempiendo il principio secondo cui le prestazioni dello Stato debbano essere fornite dietro emolumenti che ne coprano le spese, questa soluzione impedisce un onere burocratico scoraggiante. In caso di rifiuto di un sussidio statale, occorrerebbe evitare emolumenti onerosi per non ostacolare inutilmente la diffusione dell'Ie.

Le esperienze fatte a livello internazionale mostrano che gli utenti non sono disposti a pagare per l'Ie. Gli utenti ritengono che l'Ie e l'uso dell'infrastruttura affidabile a essa connessa devono essere gratuiti.

A causa delle misure di protezione dei dati, nel caso di sistemi decentrali i verificatori o le relying party non rientrano di norma tra i servizi che potrebbero assumersi una parte del finanziamento. Restano i servizi di rilascio, che in SSI potrebbero cofinanziare l'infrastruttura mediante un emolumento per il deposito delle proprie identità, schemi, definizioni delle credenziali e delle revoche nella registry (il rilascio effettivo di credenziali verificate sarebbe gratuito poiché non dovrebbe essere iscritto nella registry). Nel caso di una soluzione IdP potrebbero essere fissate delle tariffe nel quadro dei contratti tra IdP e relying party.

7 Discussione pubblica degli obiettivi di un'Ie

Anche se contiene tre tipi di soluzione, il presente documento costituisce soprattutto la base per discutere gli obiettivi di un'Ie. La Svizzera si trova davanti a un'importante decisione di principio, in merito alla quale è necessario chiedere il parere del pubblico specializzato. Che tipo di Ie vuole la Svizzera, quale ecosistema desiderano gli utenti, i Comuni, i Cantoni e l'economia, quali sono i casi di applicazione più urgenti per gli utenti e i fornitori di servizi?

I partecipanti alla discussione dovrebbero esprimersi per scritto almeno in merito ai seguenti punti:

- in quali ambiti ritenete utile un'Ie e quali casi di applicazione ritenete prioritari?
- Quali sono i tre requisiti più importanti che dovrebbe soddisfare un'Ie statale in quanto documento digitale?
- Qual è l'utilità di un'infrastruttura nazionale che permetta allo Stato e a privati di rilasciare e verificare prove digitali (p. es. Ie, licenza di condurre digitale, tessera di collaboratore, certificato di formazione)?

Ovviamente nei pareri scritti e nella discussione i partecipanti possono esprimersi anche su tutti gli altri aspetti inerenti all'Ie. Nella discussione si possono sollevare questioni e mettere in dubbio determinati approcci. La discussione è un'opportunità per ampliare i punti di vista e pensare in grande. La Svizzera deve osare puntare su una soluzione di Ie con potenziale senza conoscerne i dettagli precisi o è sufficiente una variante minima usata esclusivamente dallo Stato? La discussione dovrebbe fornire spunti e risposte a queste domande.

La discussione pubblica si svolge in vari «sounding-board» con rappresentanti di politica, economia, scienza, società civile, Cantoni e amministrazione pubblica. Inoltre sarà organizzata una discussione pubblica in forma di conferenza. I risultati delle varie discussioni e i requisiti già noti saranno riassunti e il Consiglio federale se ne servirà per la sua decisione di principio. Da questo processo dovrà scaturire un progetto di legge sostenuto da una maggioranza politica e in grado di trovare il consenso del Parlamento e del Popolo.