EDUCAZIONE CIVICA digitale

So chi sei e so cosa offrirti!

La sfida dell'identificazione dei cittadini nella pubblica amministrazione

artemisdian / 123RF

1. In che modo identificare l'utente

Le applicazioni Web che mantengono uno storico delle proprie informazioni (documenti creati, post o commenti personali, cerchie di amici) devono prevedere l'autenticazione degli utenti. Ogni forma di autenticazione prevede di fornire un identificativo (email o nome utente) che viene associato o a un'informazione nota solo all'utente (come una password o un PIN) o a un oggetto in possesso solo dell'utente (un telefono, una smart card come una Carta di Identità Elettronica - CIE - o una tessera sanitaria) o a una parte del corpo dell'utente (riconoscimento del volto, dell'iride, delle impronte digitali). Ultimamente ci si può basare su un quarto fattore di riconoscimento: il luogo in cui ci si trova. Per un maggior livello di sicurezza si raccomanda di usare una combinazione di due o più metodi diversi tra quelli presentati; si parla così di *Multifactor authentication* (MFA).

2. Identificazione per ogni applicazione

L'identificazione dell'utente può avvenire in ogni applicazione; questo ha il vantaggio che ogni applicazione richiede all'utente solo i dati necessari all'applicazione stessa, li gestisce e li memorizza; lo svantaggio è che l'utente è costretto a creare tanti account quante sono le applicazioni e può diventare molto difficile ricordare le diverse credenziali. Il rischio è che un utente tenda a usare sempre le stesse credenziali; in questo modo, se un'applicazione viene compromessa e un malintenzionato intercetta le credenziali di un utente su di essa, potrebbe poi riutilizzarle in altre applicazioni.
C'è uno svantaggio anche per gli sviluppatori, che sono costretti a replicare il codice di gestione dell'identificazione.
Infine, gli amministratori del sistema devono poi mantenere allineate tutte le diverse banche dati; per esempio, se a un utente viene revocata una credenziale, c'è il rischio che questa revoca non venga fatta su tutte le altre applicazioni.

3. Identificazione per ogni organizzazione

Lo scenario appena descritto potrebbe migliorare se all'interno di un'organizzazione si usasse un meccanismo di autenticazione unico e centralizzato. In questo modo l'utente diminuisce il numero di credenziali diverse, gli sviluppatori demandano al modulo condiviso la logica di autenticazione ed eventuali cambiamenti sono fatti in un unico punto. Anche per gli amministratori non ci sarebbe il rischio di avere dei dati non allineati, perché la banca dati degli utenti sarebbe unica.

4. Identificazione unica (o universale)

La naturale evoluzione del modello centralizzato, ma all'interno di un contesto ben specifico, è quella di prevedere un'autenticazione condivisa anche tra organizzazioni diverse. Si parla di **autenticazione distribuita** o **federata**. Un esempio molto comune è quello di numerose applicazioni web che sono federate e interoperanti con organizzazioni già in grado di autenticare gli utenti: è quello che accade quando accediamo ai servizi di un'applicazione con le credenziali di Google, Facebook o altri social. I vantaggi sono gli stessi del modello centralizzato, ma a un fattore di scala ancora maggiore; il rischio è rappresentato dal fatto che, se la credenziale usata viene compromessa, vengono compromesse tutte le applicazioni collegate. Per minimizzare il rischio si utilizza l'MFA.

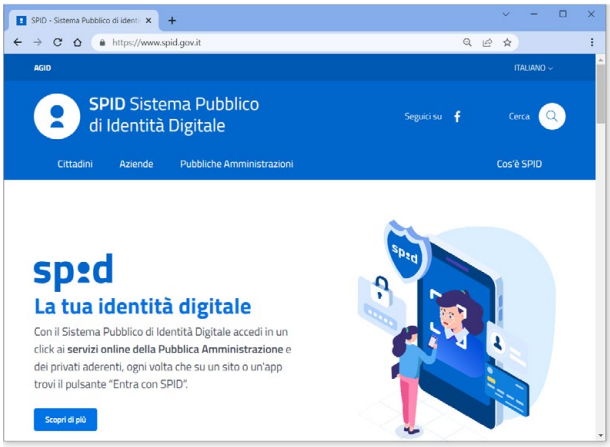
5. Identity provider (IdP) e Service provider (SP)

In un contesto distribuito c'è sempre la distinzione tra l'applicazione che offre il servizio (service provider, o SP) e il gestore dell'identità (Identity provider, o IdP).
Deve esserci una relazione di fiducia tra IdP e diversi SP. A livello informatico i diversi attori devono scambiarsi dei messaggi. Non potendo fare assunzioni sui linguaggi usati o sui sistemi operativi che

gestiscono le applicazioni, i messaggi devono prevedere un formato standard **interoperabile**, cioè gestibile dalle più comuni piattaforme software.

6. SPID

In uno scenario di autenticazione distribuita si colloca SPID: il Sistema Pubblico di Identità Digitale. Nato all'interno della pubblica amministrazione con l'obiettivo di avere un unico metodo di accesso per tutti i servizi, si è evoluto permettendo il suo utilizzo anche da parte di aziende private.



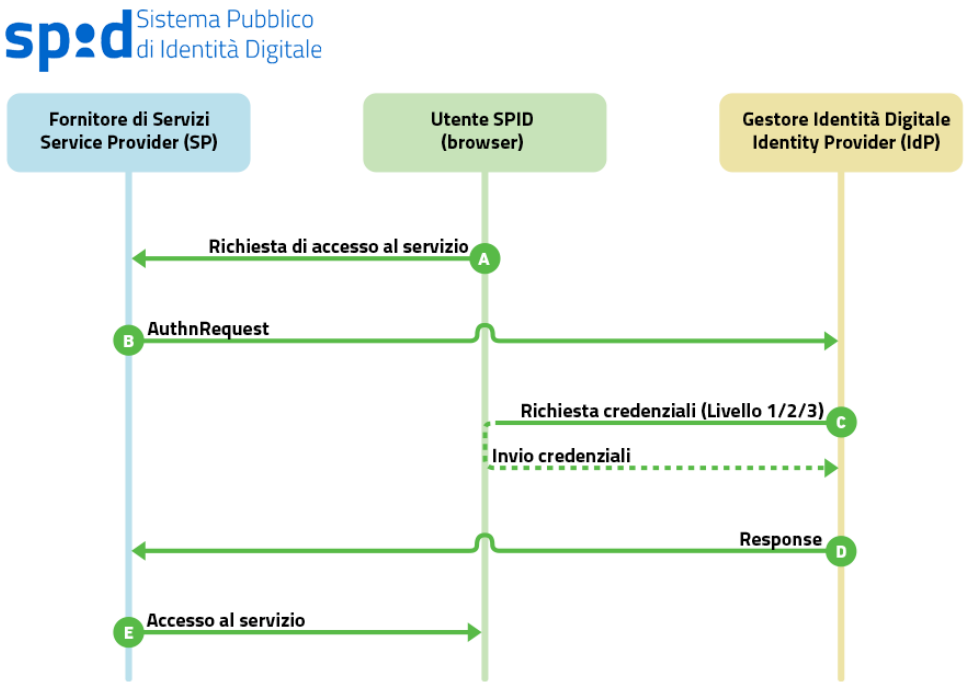
Lo Stato crea delle regole da seguire e si fa garante della corretta gestione dei dati personali e sensibili, demandando a organizzazioni esterne il ruolo di IdP e la possibilità a chiunque (aziende pubbliche e private) di adottare SPID e divenire SP. Per divenire un IdP una organizzazione deve aver superato un'attenta verifica per dimostrare affidabilità organizzativa, tecnica e finanziaria. L'elenco aggiornato degli IdP è disponibile a questa pagina.

SPID prevede, oltre a IdP e SP, dei gestori di attributi qualificati. Un gestore di attributi qualificati è un soggetto che può attestare qualifiche e stati personali: ne sono un esempio gli Ordini e i collegi professionali, gli Albi e le pubbliche amministrazioni. Un docente, per esempio, oltre a vedersi riconosciuto come persona fisica dall'IdP, potrebbe essere validato come docente del MIUR, assumendo che il MIUR diventi un gestore di attributi qualificati.

7. Uno sguardo «dentro SPID»

Dal 2016 fino al 2022 SPID si basava unicamente sul framework SAML 2.0 (Security Assertion Markup Language). Dal 2022 SPID utilizza anche il framework OpenId Connect usando SAML 2.0 in cui l'utente deve dapprima collegarsi al SP (il passo A nel diagramma seguente).
Il SP ridirige una richiesta all'IdP (passo B) chiedendo l'autenticazione e fornendo dei dati come il livello di sicurezza atteso e quali insiemi di dati sono richiesti per offrire i propri servizi.
L'IdP prende le credenziali (passo C) basandosi sul livello di sicurezza richiesto.
Se l'autenticazione è andata a buon fine vengono passati gli opportuni dati al SP (passo D), il quale fornirà il servizio richiesto se, in base ai dati, l'utente ha diritto di utilizzo (passo E).

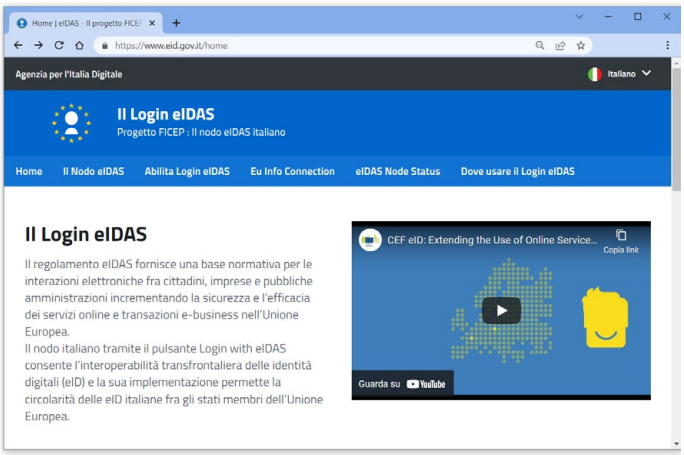
SPID ha tre livelli di sicurezza: il primo livello permette di accedere ai servizi online usando nome utente e password. Il secondo livello, utile per i servizi che richiedono un grado di sicurezza maggiore, permette l'accesso attraverso le credenziali



del primo livello e la generazione di un codice temporaneo di accesso, chiamato OTP (one time password), o l'uso di una app fruibile attraverso un dispositivo associato all'utente (per esempio uno smartphone). Il terzo livello prevede, oltre alle credenziali SPID, l'uso di ulteriori soluzioni di sicurezza e di eventuali dispositivi fisici (come le smart card) erogati dall'Identity Provider.

Quando l'IdP ha riconosciuto l'utente, prima di restituire i dati al SP chiede all'utente l'autorizzazione a farlo e rende espliciti quali dati verranno trasmessi (per esempio il nome e il cognome, il codice fiscale, il telefono e così via).

8. eIDAS



A livello europeo è stato definito il regolamento eIDAS (electronic IDentification Authentication and Signature), che ha l'obiettivo di rendere interoperabili tutti i sistemi di autenticazione degli Stati dell'Unione Europea: si vuole cioè permettere a ogni cittadino, in possesso di credenziali valide nel suo paese di origine, di poter accedere a tutti i servizi degli altri Stati europei. In questo modo chi si trova in un altro Stato potrebbe accedere ai servizi sanitari locali, partecipare a concorsi pubblici che richiedono l'autenticazione, pagare le tasse nel nuovo Stato e così via.

9. Non solo SPID: la CIE

Un'altra modalità di autenticazione digitale è quella con la Carta di Identità Elettronica (CIE). Anche con essa è possibile accedere ai servizi conformi a eIDAS. Nel caso della CIE il Ministero dell'Interno garantisce la corretta identificazione del soggetto e di aver consegnato la CIE e i relativi codici al legittimo titolare; l'identificazione avviene dagli ufficiali di anagrafe presso i Comuni italiani. Nata come sostituta della carta di identità tradizionale, la CIE è sia un documento di identità, sia una carta dei servizi (utilizzabile senza PIN e utile nei casi in cui è richiesto un accesso fisico veloce, come per esempio sui mezzi di trasporto pubblico o nelle aree con accesso controllato), sia un token di autenticazione tipo smart card. Per utilizzare quest'ultimo tipo di autenticazione, richiesto per l'identità digitale online, è necessario disporre di un lettore NFC (disponibile in molti modelli di smartphone) oppure di un lettore di smart card. La CIE, attraverso un lettore di smart card e opportuni software, è utilizzabile anche come dispositivo di firma elettronica avanzata (FEA) per firmare documenti elettronici (PDF o altri file).
Avere due modalità di autenticazione può rappresentare anche un'opportunità per avere una modalità di accesso disponibile nel caso ci sia qualche problema con l'altra.
La tabella seguente sintetizza e confronta i vantaggi e gli svantaggi di SPID e CIE.

	SPID	CIE
Vantaggi	▪ Diversi livelli di sicurezza, che possono essere scelti in maniera appropriata in base alla tipologia di servizio richiesto. I primi due livelli non necessitano di hardware e software specifici. ▪ L'uso di IdP come organizzazioni esterne presenta i vantaggi del libero mercato (aggiornamenti tecnologici, flessibilità organizzativa e operativa, offerta diversificata in termini di costo e modalità di riconoscimento). ▪ Conforme all'articolo 5 della Costituzione (riconosce e promuove le autonomie locali; attua il decentramento amministrativo). ▪ Conforme a eIDAS al 100%.	▪ Rilasciato a tutti coloro che richiedono una nuova carta d'identità. ▪ È documento di identità e, come tale, utilizzabile anche per i servizi "tradizionali". ▪ Vari meccanismi anti contraffazione sia fisici che elettronici (tra cui lo standard ICAO). ▪ Può essere usata come Carta dei servizi. ▪ Token di autenticazione tipo smart card. ▪ Può essere utilizzata come dispositivo di "firma elettronica avanzata" (FEA) per firmare documenti elettronici. ▪ Contiene la fotografia a colori ad alta risoluzione della persona a cui è stata rilasciata, oltre a informazioni biometriche (con certificato di sblocco) come le impronte digitali.
Svantaggi	▪ Non sostituisce un documento di identità: per essere rilasciata si deve presentare un documento di identità valido. ▪ Ogni IdP ha le sue regole di riconoscimento (alcune in presenza, altre completamente online). ▪ Al momento SPID è rilasciato solo a chi ha almeno 18 anni.	▪ Rilasciata unicamente dal Ministero dell'Interno tramite gli uffici Anagrafe dei Comuni, con tempi di rilascio non immediati. ▪ Necessita di un lettore NFC per usare il token di autenticazione oppure di un PC collegato a un lettore di smart card. ▪ Soluzione completamente hardware e, come tale, non aggiornabile in caso di problemi.

10. Tutti i servizi a portata «di clic»

Attraverso un metodo di autenticazione universale ogni cittadino europeo può davvero beneficiare delle opportunità offerte in ogni Stato e ottenere un trattamento paritario e non discriminatorio nella fruizione dei principali servizi digitali.

La digitalizzazione dei servizi ha l'obiettivo di semplificare l'accesso dei cittadini alla pubblica amministrazione e ha trovato in SPID ed eIDAS un modo agevole per la loro fruizione, garantendo, al tempo stesso, la privacy dei dati nel pieno rispetto del GDPR.

FISSA I CONCETTI IMPORTANTI

1 **Con *Multi-factor Authentication* si intende:**

- A utilizzare due o più fattori di conoscenza (es. PIN e password).
- B utilizzare due o più fattori di tipo diverso (qualcosa che conosco insieme a qualcosa che possiedo, per esempio).
- C permettere di autenticare più utenti con le stesse credenziali.
- D essere certi che chi usa le credenziali sia l'utente autorizzato a farlo.

2 **Quale vantaggio c'è nell'utilizzare un'autenticazione locale ad ogni applicazione?**

- A Aiuta gli sviluppatori a creare l'applicazione.
- B Aiuta gli amministratori a gestire gli utenti.
- C Si può decidere in autonomia quali dati trattare e memorizzare.
- D Aiuta gli utenti a ricordare le credenziali usate.

3 **Un sistema di autenticazione distribuito:**

- A dovrebbe essere interoperabile.
- B si basa sempre e solo su uno specifico linguaggio di programmazione.
- C utilizza un'unica applicazione chiamata Service Provider.
- D utilizza un'unica applicazione chiamata Identity Provider.

4 **Cosa fa un Identity Provider?**

- A Fornisce i servizi di cui l'utente ha bisogno.
- B Riconosce l'azienda che fornisce un servizio.
- C Autentica l'utente che cerca di accedere ad un Service Provider.
- D Definisce di quali dati avrà bisogno un Service Provider.

5 **eIDAS permette:**

- A a un qualsiasi cittadino mondiale di usare le stesse credenziali ovunque.
- B a un qualsiasi cittadino statunitense di usare le stesse credenziali in qualunque applicazione.
- C a un qualsiasi cittadino europeo di usare le stesse credenziali nelle applicazioni Web della pubblica amministrazione e in quelle delle aziende private aderenti.
- D di usare credenziali diverse per ogni applicazione usata.

APPLICA I CONCETTI

6 Divisi in gruppi secondo le indicazioni del docente, verificate quali sono gli Identity Provider attualmente supportati da SPID e predisponete una scheda comparativa. Poi verificate se le pubbliche amministrazioni della vostra città offrono servizi online accessibili attraverso SPID. Ogni gruppo presenta agli altri i risultati raccolti e, al termine, i vari gruppi elaborano un documento di sintesi.