



**Sistemi e Reti &
Educazione Civica**

Identità digitale

autenticazione e fiducia nelle reti



Angelo Serban

Studente e culturista



Cos'è l'identità digitale?

- * E' l'insieme di informazioni che permettono a una persona di essere riconosciuta online. Viene usata per autenticarsi e accedere a servizi digitali in modo sicuro. Ecco degli esempi:
- * **SPID**
Sistema Pubblico di Identità Digitale
- * **CIE**
Carta di identità elettronica
- * **Login**
Che sia con Google, Facebook, Apple...



Perchè è importante?



Viviamo in una società che sta diventando sempre più digitale:

- Le iscrizioni scolastiche, i bonus, e il fascicolo sanitario sono online
- E' fondamentale proteggere l'identità e sapere chi c'è dall'altra parte



L'identità digitale crea fiducia nei servizi digitali, ma va protetta da:

- Furti di identità
- Accessi non autorizzati
- Uso improprio dei dati

I fattori di autenticazione

Per accedere in modo sicuro si usano diversi fattori di autenticazione

* Qualcosa che sai

Password, PIN

* Qualcosa che hai

Token, smartphone

* Qualcosa che sei

Impronta, volto, voce



Autenticazione forte



 **L'autenticazione forte usa almeno 2 fattori:**

- Per esempio: SPID Livello 2 → password + codice via app
- OTP (One-Time Password): codice temporaneo
- Passwordless: login con impronta o notifica

Aiuta a prevenire furti di credenziali, phishing, accessi abusivi

Single Sign-On

SSO = Single Sign-On → Accedi una sola volta, poi puoi entrare in più servizi.

Per esempio: login Google → Accedi anche a Youtube, Gmail, Meet ecc...

Vantaggi:

- * Più comodo per l'utente
- * Meno password da ricordare
- * Maggiore controllo centrale



Protocolli di identità



Dietro l'identità digitale ci sono protocolli e standard:

- OAuth 2.0: autorizzazione con token
- OpenID Connect: estende OAuth per l'identità
- FIDO2/WebAuthn: login senza password
- SAML: usato in aziende per scambio di identità



Questi garantiscono sicurezza, interoperabilità, e conformità alle normative.

Firma digitale e PKI

La firma digitale garantisce:

- * Maggiore autenticità, visto che è firmato da te
- * Maggiore integrità, non può essere modificato
- * Assenza di ripudio, ovvero non si può negare la firma

Basata su PKI (Public Key Infrastructure):

- * Chiave pubblica + chiave privata
- * Certificato digitale emesso da una CA (Certification Authority)



SPID e CIE in Italia



SPID

- 3 livelli di sicurezza (da semplice a forte)
- Usato per INPS, scuola, sanità e bonus
- Rilasciato da provider accreditati

CIE

- Carta di identità elettronica con chip
- Usabile online con lettore o app
- Garantisce accesso forte e sicuro

Normativa europea: eIDAS

eIDAS = Regolamento UE per l'identità digitale e le firme elettroniche

Obiettivi

- * Riconoscere identità digitali in tutta Europa
- * Creare fiducia tra cittadini, aziende e PA (pubblica amministrazione)
- * Standard comuni tra i vari Stati membri

Grazie a eIDAS, SPID e CIE sono validi anche all'estero (per esempio nelle università o nei concorsi)



Aspetti civici ed etici



*** L'identità digitale è anche un tema di cittadinanza:**

- E' un diritto di accesso ai servizi digitali
- Deve essere inclusiva, ovvero accessibile a disabili, anziani o persone senza competenze digitali
- L'utente deve controllare i suoi dati

*** E' importante trovare un equilibrio tra:**

- Sicurezza
- Privacy
- Facilità d'uso

Caso studio: SPID

SPID è il sistema italiano più usato

* E' attivo per milioni di cittadini

* E' usato per accedere a:

- Fascicolo sanitario
- Bonus statali (come 18app o Carta Cultura)
- Portale INPS

Problemi comuni:

- Difficoltà iniziale nell'attivazione
- Alcuni anziani o cittadini non digitali fanno fatica



Sfide e problemi



- * **Furto di identità** (es. phishing con finti login SPID)
- * **Vendor lock-in** (dipendenza da pochi provider)
- * **Esclusione digitale** (chi non ha internet o competenze rimane fuori)
- * **Gestione della privacy** (non è sempre chiaro come vengono usati i dati)

Soluzioni e buone pratiche

Un elenco di buone pratiche e possibili soluzioni:

- * Attivare sempre l'autenticazione a più fattori (MFA)
- * Fare educazione digitale a scuola e nei servizi pubblici
- * Usare standard aperti e interoperabili
- * Progettare con la logica della Privacy By Design



Fine

