10/05/2025

Identità digitale, autenticazione e fiducia nelle reti

VICTOR TASCA
ANNO: 2024/2025
CLASSE: 4^D

Introduzione al contesto

- Nell'era digitale, **l'identità** è definita da **dati** e **credenziali**.
- Accessi a servizi digitali richiedono **autenticazione sicura**.
- L'identità digitale è un **diritto**, ma anche un punto critico di **vulnerabilità**.
- Serve equilibro tra **sicurezza**, **privacy** e **accessibilità**.

Evoluzione dell'autenticazione

- **Password deboli** -> vulnerabili a furti
- **2FA:** aggiunge sicurezza con token o SMS
- **MFA:** combina più fattori (es. Password + biometria)
- **Autenticazione adattiva:** si adatta al rischio
- **Passwordless:** elimina l'uso della password

Fattori di autenticazione

1. Qualcosa che **conosci** (password, PIN)
2. Qualcosa che **possiedi** (token, smart card)
3. Qualcosa che **sei** (biometria: volto, impronta)
4. **Dove** e **quando** ti autentichi (luogo e orario)

Tecnologie di autenticazione forte

- OTP(HOTP, TOTP)
- Token hardware come Yubikey
- App mobile per autenticazione(Google Authenticator)
- Biometria: impronte, volto, voce

Protocolli e standard

- **OAuth 2.0:** autorizzazione tramite token
- **OpenID Connect:** gestione dell'identità su OAuth
- **SAML:** scambio sicuro di dati tra provider
- **FIDO2 / WebAuthn:** login senza password

Single SIgn-On e federazione dell'identità

- **SSO:** acceso unico a più servizi (es. Google)
- **Identity Federation:** identità condivisa tra provider
- **Esempio:** login con SPID o social login
- **Vantaggi:** meno password, maggiore sicurezza

PKI e firma digitale

- **PKI:** gestisce certificati digitali (X.509)
- **Firma digitale:** garantisce integrità e autenticità
- **Componenti:** CA, RA, chiavi pubbliche/private
- **Usi:** PEC, SPID, documenti ufficiali

Case Study: SPID (Italia)

- **S**istema **P**ubblico di **I**dentità **D**igitale
- 3 livelli di sicurezza (password, OTP, biometria)
- Accesso a servizi PA e privati
- Conforme a eIDAS e GDPR

Implicazioni civiche ed etiche

- L'identità digitale è un **diritto riconosciuto**
- **Inclusività:** accesso anche per anziani o disabili
- **Rischi:** sorveglianza, controllo, privacy
- **Sovranità digitale:** chi controlla i dati?

Sfide e opportunità future

- Interoperabilità europea (eIDAS 2.0)
- Identità decentralizzata (SSI)
- Bilanciare sicurezza e usabilità
- Educazione e consapevolezza digitale

Raccomandazioni e best practices

- Attivare MFA ovunque possibile
- Non riutilizzare password
- Usare un gestore di password
- Controllare la sicurezza dei siti (HTTPS, certificati)

Conclusioni

- L'identità digitale è centrale nella società moderna
- Serve equilibrio tra sicurezza, privacy e accesso
- Cittadini e tecnici devono essere formati e consapevoli

Fonti e riferimenti

- PDF scolastico: Standard e sicurezza avanzata
- SPID.gov.it
- ENISA eIDAS Overview
- OWASP Authentication Cheat Sheet
- European Union Agency for Cybersecurity