IDENTITÀ DIGITALE, AUTENTICAZIONE E FIDUCIA NELLE RETI

Discussione e presentazione su aspetti tecnici, e aspetti di educazione civica

Scopo: Analizzare l’evoluzione dei meccanismi di autenticazione e autorizzazione nel contesto della sicurezza digitale.

Nel contesto della trasformazione digitale, **identità digitale**, **autenticazione** e **fiducia nelle reti** rappresentano elementi fondamentali per garantire la sicurezza, l'affidabilità e l'interoperabilità dei servizi digitali, sia nel settore pubblico che privato. L’Unione Europea e gli Stati membri hanno sviluppato un quadro normativo e tecnico per regolamentare questi ambiti e favorire l’adozione di soluzioni standardizzate e sicure.

ASPETTI TECNICI

EVOLUZIONE DEI SISTEMI DI AUTENTICAZIONE E AUTORIZZAZIONE E EVOLUZIONE DEI SISTEMI DI AUTENTICAZIONE E AUTORIZZAZIONE

Le tecnologie di **AUTENTICAZIONE** sono:

-Password(inital) vulnerabile a brute force, phishing, e credential stuffing.

-Autenticazione a due fattori (2FA): SMS, email, TOTP (miglioramento ma ancora attaccabile.)

TECNOLOGIE DI AUTORIZZAZIONE

-RBAC (ROLE-BASED): SEMPLICE, STATICO.

-ABAC (ATTRIBUTE-BASED): FLESSIBILE, DINAMICO.

SFIDE COLLEGATE

- GESTIONE SICURA DELLE SESSIONI (COOKIE, TOKEN JWT).
- REVOKE E SCADENZA DEI TOKEN.

INFRASTRUTTURE A CHIAVE PUBBLICA (PKI) E FIRMA DIGITALE

Elementi fondamentali

Chiavi asimmetriche (pubblica/privata): base della crittografia moderna.

Certificati X.509: identificano un soggetto, firmati da una CA.

FIRMA DIGITALE

Algoritmi: RSA, ECDSA, SHA-2.

-Firma elettronica semplice

-Firma elettronica avanzata

-Firma elettronica qualificata (con QSCD)

SFIDE TECNICHE

-Scadenza e rinnovo dei certificati.

SINGLE SIGN-ON (SSO) E IDENTITY FEDERATION

SINGLE SIGN-ON

Permette all'utente di autenticarsi una sola volta per accedere a più servizi.

Riduce la superficie di attacco legata alle credenziali multiple.

IDENTITY FEDERATION

SAML 2.0: usato in SPID, università, PA.

OAuth 2.0 / OpenID Connect: ideale per applicazioni moderne (web/mobile).

eduGAIN, EUDI Wallet: federazioni internazionali per identità interoperabili.

ELEMENTI TECNICI

IdP (Identity Provider) e SP (Service Provider).

Metadata Exchange: scambio delle chiavi e delle policy.

Token ID e token accesso (JWT): trasmettono informazioni sull'identità/autorizzazione.

SFIDE TECNICHE

Federation trust chain: gestione sicura delle relazioni tra entità

BIOMETRIA E NUOVE TECNOLOGIE DI AUTENTICAZIONE

TìECNOLOGIE BIOMETRICHE

Fisiologiche: impronta, volto, iride.

Comportamentali: voce, andatura, dinamiche di digitazione.

TECNOLGIE E STANDARD

FIDO2 / WebAuthn: autenticazione biometrica locale, senza invio dei dati biometrici al server.

Liveness detection: verifica che l'utente sia reale (anti-spoofing).

ISO/IEC 30107: standard per il testing di sistemi biometrici.

SICUREZZA DEI DATI BIOMETRICI

I dati biometrici non sono revocabili → crittografia e separazione dei dati sono obbligatorie.

SFIDE TECNICHE

Falso accettato (FAR) vs falso rifiuto (FRR).

Rischi legati alla privacy (GDPR).

Integrazione con sistemi esistenti, fallback sicuri (es. PIN, OTP).

IMPLEMENTAZIONE PRATICA: IDENTITÀ DIGITALE E AUTENTICAZIONE

[L'OBBIETTIVO È QUELLO DI CREARE UN ACCESSO SICURO E CONFORME A SERVIZI DIGITALI (SPID, CIE, FIDO2) PER CITTADINI E OPERATORI.]

Architettura di riferimento

Federazione identità: SPID/CIE via SAML2 / OpenID Connect

Autenticazione forte: FIDO2/WebAuthn + biometria

Controllo accessi: RBAC per ruoli e servizi

Consent Management: gestione opt-in (GDPR)

Audit & Logging: tracciabilità via SIEM

Tecnologie chiave

Keycloak / Auth0 / WSO2 IS (IdP federato)

WebAuthn.io / YubiKey / Apple Passkey (FIDO2)

Open Policy Agent / XACML (policy RBAC/ABAC)

ELK / Wazuh / Splunk (SIEM)

Benefici

Alta sicurezza (phishing-resistant)

Conformità eIDAS, GDPR, NIS2

Esperienza utente fluida

Riduzione accessi non autorizzati

ACCESSO SICURO AL FASCICOLO SANITARIO ELETTRONICO (ESEMPIO DI CASE STUDY)

Attori coinvolti

Cittadini: accesso al proprio FSE

Medici: accesso a dati pazienti

Operatori PA: gestione anagrafiche sanitarie

Risultati ottenuti

Autenticazione forte implementata (phishing-resistant)

Conformità a eIDAS, GDPR, Linee Guida AgID

Aumento accessi digitali sicuri del 40%

Maggiore fiducia da parte degli utenti e operatori

(a destra c'è la mia soluzione implementata)

Funzione	Tecnologia/Standard
Autenticazione federata	SPID / CIE (SAML2 + OIDC)
Accesso via app mobile	FIDO2/WebAuthn + FaceID
Autorizzazione per ruolo	RBAC + policy dinamiche
Tracciabilità accessi	Logging con Wazuh + SIEM
Consenso utente (GDPR)	UI dedicata + audit trail

ASPETTI DI EDUCAZIONE CIVICA:

Identità Digitale come Diritto Fondamentale

L’accesso sicuro ai servizi digitali è oggi condizione necessaria per esercitare diritti civili (salute, istruzione, partecipazione).

L’identità digitale deve essere pubblica, gratuita e universalmente accessibile principio sancito anche dall’EUDI Wallet.

Fiducia Digitale e Democrazia Elettronica

L’identità è fondamento della fiducia online: senza di essa non sono possibili voto elettronico, sanità digitale, giustizia digitale.

Richiede:

- **Governance trasparente**
- **Audit indipendenti**
- **Partecipazione civica alla definizione degli standard**

IMPLICAZIONI ETICHE, SOCIALI E NORMATIVE DELL'IDENTITÀ DIGITALE

Inclusività e Accessibilità

Rischio di **esclusione digitale** per anziani, persone con disabilità, minoranze linguistiche o non digitalmente alfabetizzate.

Necessità di:

- **Design inclusivo e accessibile** (WCAG, mobile-first)
- **Supporto multicanale** (sportello fisico, app, web)
- **Assistenza digitale personalizzata**

Sovranità Digitale e Controllo dell'Identità

Chi controlla le infrastrutture di identità (governo, Big Tech, consorzi)?

Importanza di:

- **Soluzioni open source e decentralizzate** (DID, SSI)
- **Portabilità e interoperabilità europea** (EUDI Wallet)
- **Protezione da sorveglianza e profilazione commerciale**

ASIMMETRIE INFORMATIVE E POTERE DEI DATI NELL'IDENTITÀ DIGITALE

L'**asimmetria informativa** si verifica quando una parte possiede più informazioni rispetto all'altra, creando squilibri di potere e potenziali abusi, inoltre le grandi piattaforme raccolgono questi dati personali senza la consapevolezza degli utenti, sfruttandoli per fini commerciali (ad esempio la vendita di essi a altre aziende.)

Quindi si incorrono in rischi coma la profilazione e la sorveglianza questo porta quindi alla perdita della fiducia, dunque La concentrazione del potere informativo in poche mani solleva questioni sulla **sovranità digitale** e sulla capacità degli individui di controllare la propria identità online.

La raccomandazione è quella di Promuovere trasparenza e responsabilità nell'uso dei dati, e Adottare un'etica by design nello sviluppo di tecnologie digitali, integrando considerazioni etiche fin dalle fasi iniziali

SFIDE E OPPORTUNITÀ FUTURE

Sfide emergenti

Cyberminacce avanzate (phishing evoluto, attacchi deepfake, AI spoofing)

Dilemmi etici su sorveglianza, profilazione e gestione del consenso

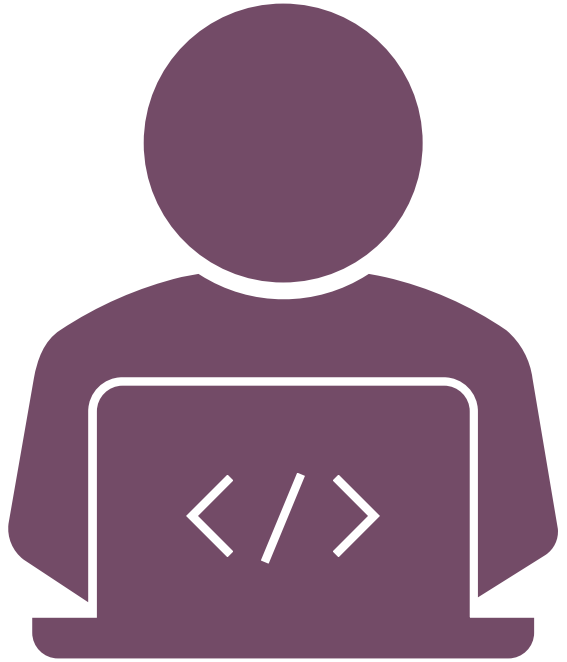
Resistenza sociale all'adozione di tecnologie biometriche o federate

Opportunità strategiche

EUDI Wallet (Identità digitale europea) → interoperabilità e portabilità

Modelli decentralizzati (Self-Sovereign Identity – SSI) → controllo ai cittadini

Autenticazione post-password → FIDO2, passkey, biometria locale



RACCOMANDAZIONI E BEST PRACTICES

Autenticazione forte e moderna

Favorire l'adozione di FIDO2, passkey, autenticazione biometrica locale

Evitare l'uso di password statiche e OTP via SMS

Educazione e cultura digitale

Formare utenti e operatori su rischi e buone pratiche e Promuovere una cultura della fiducia digitale

Federazione e interoperabilità

- Utilizzare standard aperti (SAML2, OpenID Connect)
- Garantire la portabilità dell'identità (es. EUDI Wallet)

MATRICE DI MAPPATURA TRA REQUISITI NORMATIVI/ETICI E CONTROLLI TECNICI

Requisito Normativo / Etico	Controllo Tecnico Implementabile
GDPR – Minimizzazione dei dati	Identity Proofing con selezione attributi minimi; Attribute-Based Access Control (ABAC)
GDPR – Consenso informato e revocabile	Consent Management UI + Logging del consenso; standard User-Managed Access (UMA)
GDPR – Portabilità dei dati	API standardizzate interoperabili (OAuth2 + OIDC) + EUDI Wallet
eIDAS – Autenticazione forte (LoA)	FIDO2 / CIE / SPID con SAML2 + classificazione LoA conforme ETSI
eIDAS 2.0 – Identità auto-sovrana (SSI)	DID (Decentralized Identifiers) + Verifiable Credentials
NIS2 – Tracciabilità degli accessi	Audit trail + Centralized Logging + SIEM (Wazuh, Splunk, ELK)
Accessibilità digitale (WCAG 2.1)	Interfacce web conformi WCAG + test utente inclusivi
Sovranità digitale	Adozione di stack open-source (es. Keycloak, eIDAS wallet open) + cloud nazionale/UE
Equità e non discriminazione	Validazione algoritmi biometrici con dataset eterogenei; esclusione di AI opachi da processi critici
Etica e trasparenza dell'identità digitale	Codice open, auditabili + governance multi-stakeholder + impact assessment etico (ALTAI, etc.)
Democrazia elettronica e fiducia nei servizi pubblici digitali	Meccanismi di accountability pubblica, audit indipendenti, trasparenza degli algoritmi

CONCLUSIONI

L’identità digitale è:

Un diritto fondamentale, non solo uno strumento di accesso che cerca di creare equilibrio tra sicurezza, privacy, usabilità e compliance, e spera nella fiducia delle reti

Il futuro:

Adottare modelli decentralizzati e user-centrici (SSI, EUDI Wallet)

Rafforzare trasparenza, inclusività e controllo individuale e integrare AI contestuale e autenticazione adattiva

GRAZIE MILLE A TUTTI PER AVER PRESO VISIONE DI QUESTO POWER POINT