The background is a dark blue gradient with various digital and network-related icons. On the left, there's a stylized person icon inside a square frame. Below it, a padlock icon is next to the text 'Confidential Data'. On the right, there's a vertical stack of server racks. The overall theme is digital identity and network security.

Identità digitale, autenticazione e fiducia nelle reti

Aspetti tecnici e civici nella gestione dell'identità online

Volpato Riccardo

Introduzione al contesto normativo e tecnico

- L'identità digitale è l'insieme di dati che identificano un individuo nei sistemi informatici.
- Rilevanza crescente in ambiti pubblici e privati (SPID, CIE, eIDAS).
- Necessità di autenticazione sicura e interoperabile.

Riferimenti normativi principali

- **Regolamento eIDAS (UE 910/2014):** Standard europeo per identificazione elettronica e servizi fiduciari.
- **GDPR (UE 2016/679):** Protezione dei dati personali legati all'identità.
- **Linee guida AgID:** Regolano l'identità digitale in Italia (es. SPID).





Evoluzione dei sistemi di autenticazione

- **Password tradizionali** → deboli e facilmente attaccabili.
- **Autenticazione a più fattori (MFA):** Combinazione di “ciò che sai”, “ciò che hai”, “ciò che sei”.
- **Tendenza attuale:** passwordless + autenticazione biometrica.

Infrastrutture a Chiave Pubblica (PKI)

- Utilizzate per autenticazione forte, firma digitale e cifratura.
- **Componenti principali:**
 - Certificati digitali
 - Chiavi pubbliche/private
 - Autorità di certificazione (CA)
 - Fondamento per fiducia nelle comunicazioni online (es. HTTPS).



Firma digitale


- Garantisce **autenticità, integrità e non ripudio**.
- Usata in documenti legali, contratti e comunicazioni con la PA.
- Basata su crittografia asimmetrica (PKI).



Single Sign-On e Identity Federation

- **SSO**: un solo login per accedere a più servizi (es. Google Workspace).
- **Identity Federation**: condivisione dell'identità tra organizzazioni diverse (es. SPID per più enti).
- Vantaggi: usabilità, sicurezza, riduzione gestione credenziali.





Biometria e nuove tecnologie

- **Impronte, volto, retina, voce:** esempi di fattori biometrici.
- Tecnologie emergenti: autenticazione comportamentale, passkey (FIDO2).
- Sfide: privacy, accuratezza, inclusività (es. utenti con disabilità).

Identità digitale come diritto

- Inclusa nel concetto di cittadinanza digitale.
- Accesso ai servizi pubblici e partecipazione democratica.
- Essenziale per l'inclusione sociale e il rispetto dei diritti fondamentali.





Accessibilità e inclusività

- Sistemi devono essere:
- Accessibili a tutti (disabili, anziani, analfabeti digitali)
- Usabili con tecnologie assistive
- SPID e CIE: progressi, ma permangono barriere per alcune categorie.

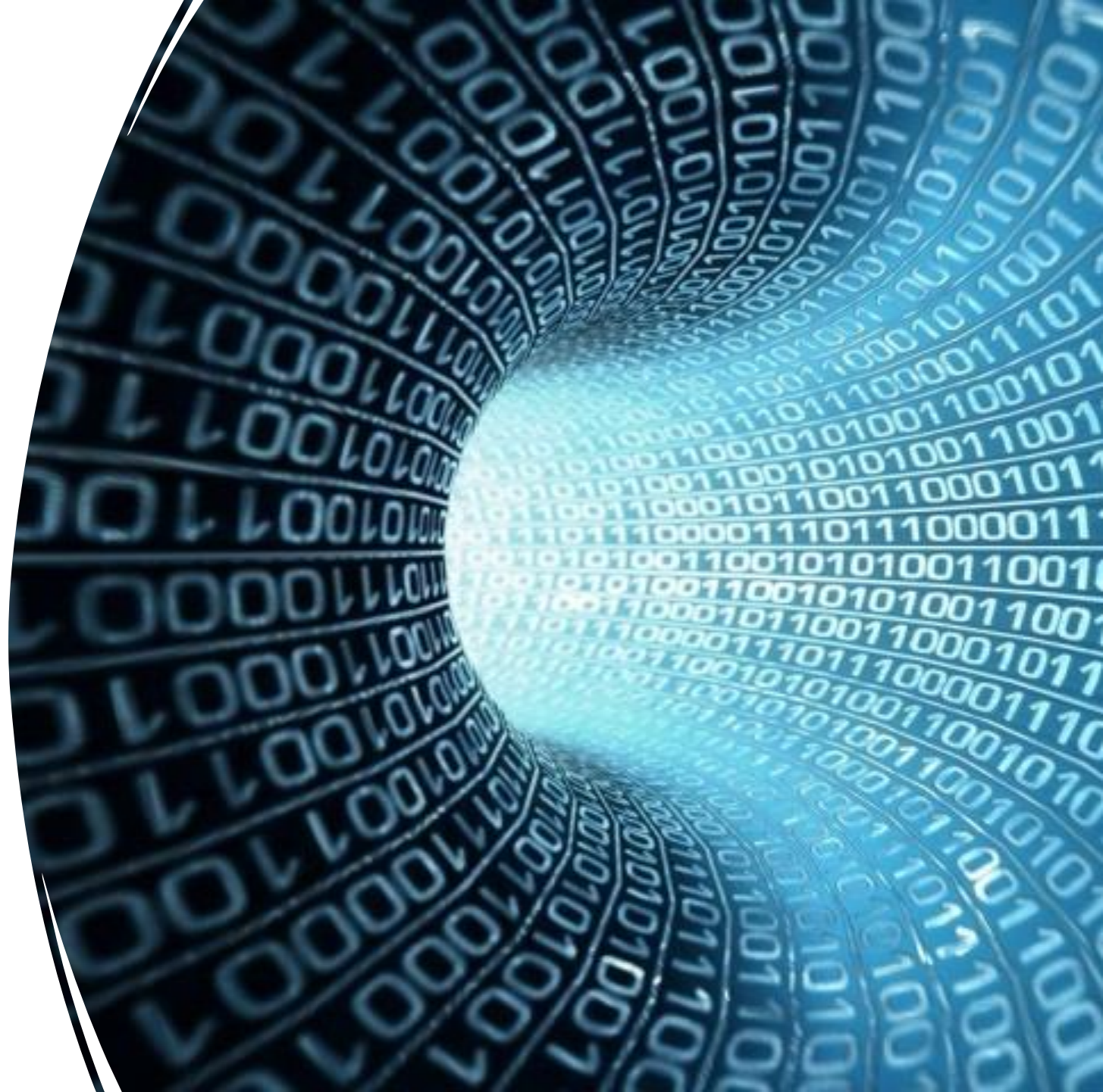


Sovranità digitale

- Controllo dei dati personali da parte dell'utente.
- **Self-Sovereign Identity (SSI)**: modello decentralizzato.
- Evitare dipendenza da big tech estere → sicurezza nazionale e autonomia.

Fiducia digitale e democrazia elettronica

- Fiducia = combinazione di trasparenza, sicurezza e responsabilità.
- Cruciale in votazioni elettroniche, servizi sanitari, istruzione online.
- Ruolo dell'identità digitale nel rafforzare la partecipazione democratica.



Implementazione pratica: SPID



- Sistema Pubblico di Identità Digitale
- Livelli di sicurezza: 1 (solo password), 2 (OTP), 3 (smart card).
- Usato per accedere a INPS, Agenzia Entrate, Fascicolo Sanitario, ecc.

Case Study: Estonia e-ID

- Estonia: leader mondiale in identità digitale.
- Tutti i cittadini hanno una e-ID: accesso a 99% dei servizi pubblici online.
- Sistema altamente sicuro, basato su PKI e blockchain.



Sfide e rischi

- **Sicurezza:** phishing, furto d'identità.
- **Esclusione digitale:** mancanza di alfabetizzazione informatica.
- **Gestione dei dati:** rischio di sorveglianza e uso improprio.



Opportunità e sviluppi futur

- Diffusione del **digital wallet europeo**.
- Integrazione con intelligenza artificiale e blockchain.
- Modelli decentralizzati per maggiore privacy.



A person in a blue suit is working on a laptop. The laptop screen displays a large white padlock icon over a background of binary code. A tablet next to the laptop also shows binary code. The scene is dimly lit, with the primary light source being the screens. There are faint, semi-transparent padlock icons and binary code overlays across the entire image, emphasizing a theme of digital security and data protection.

Raccomandazioni e best practices

- Educazione digitale a scuola.
- Adozione di standard aperti e interoperabili.
- Favorire sistemi inclusivi e trasparenti.



Conclusioni e riferimenti

- L'identità digitale è un pilastro della cittadinanza moderna.
- Serve equilibrio tra innovazione, inclusività e tutela dei diritti.
- **Fonti:** eIDAS, AgID, GDPR, white paper ENISA, casi SPID ed Estonia.