



# Identità Digitale: Evoluzione Tecnica e Valore Civico

Evoluzione Tecnica e Valore Civico  
La trasformazione dei sistemi di autenticazione e il ruolo sociale  
dell'identità digitale



Questa presentazione affronta sia gli aspetti **tecnici** sia quelli **civici** dell'identità digitale.

Analizzeremo

- l'evoluzione delle tecnologie di autenticazione, le infrastrutture di sicurezza
- le soluzioni biometriche
- nuovi paradigmi di gestione dell'identità.

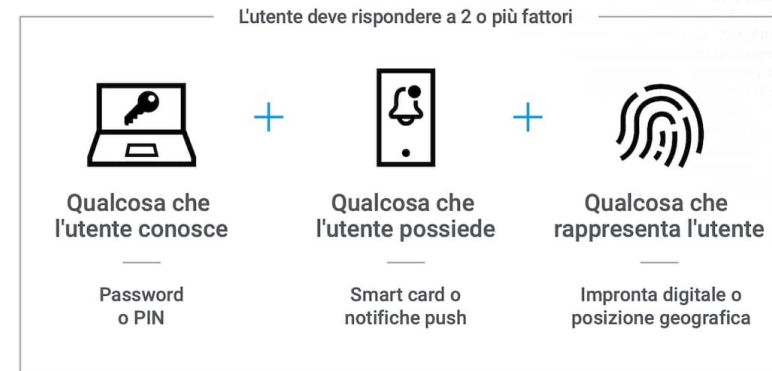
Approfondiremo inoltre

- il valore dell'identità digitale come diritto
- la sua accessibilità
- il concetto di sovranità digitale e il ruolo nella democrazia elettronica.

# Autenticazione e Autorizzazione: Le Basi della Sicurezza Digitale

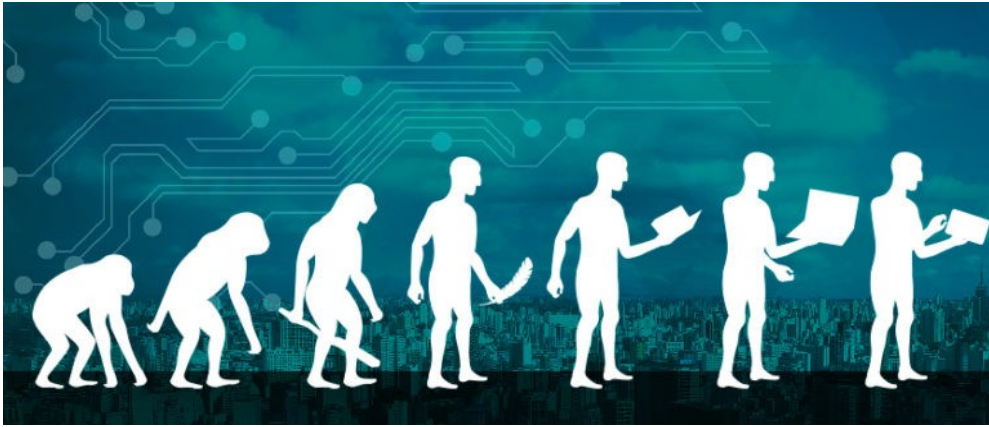
L'**autenticazione** è il processo che permette a un sistema di verificare l'**identità di un utente**, mentre l'**autorizzazione** stabilisce **quali risorse e azioni sono consentite a quell'utente**.

Questi due concetti sono alla base della sicurezza informatica e della protezione dei dati personali e aziendali.



Che cos'è l'autenticazione multifattore (MFA)?

# Evoluzione dei Sistemi di Autenticazione



Dalle semplici password degli anni '90 siamo passati a sistemi sempre più sofisticati: password manager, autenticazione a due fattori (2FA), token hardware e soluzioni passwordless. L'obiettivo è aumentare la sicurezza riducendo la complessità per l'utente.

# Best Practice Moderne per la Sicurezza

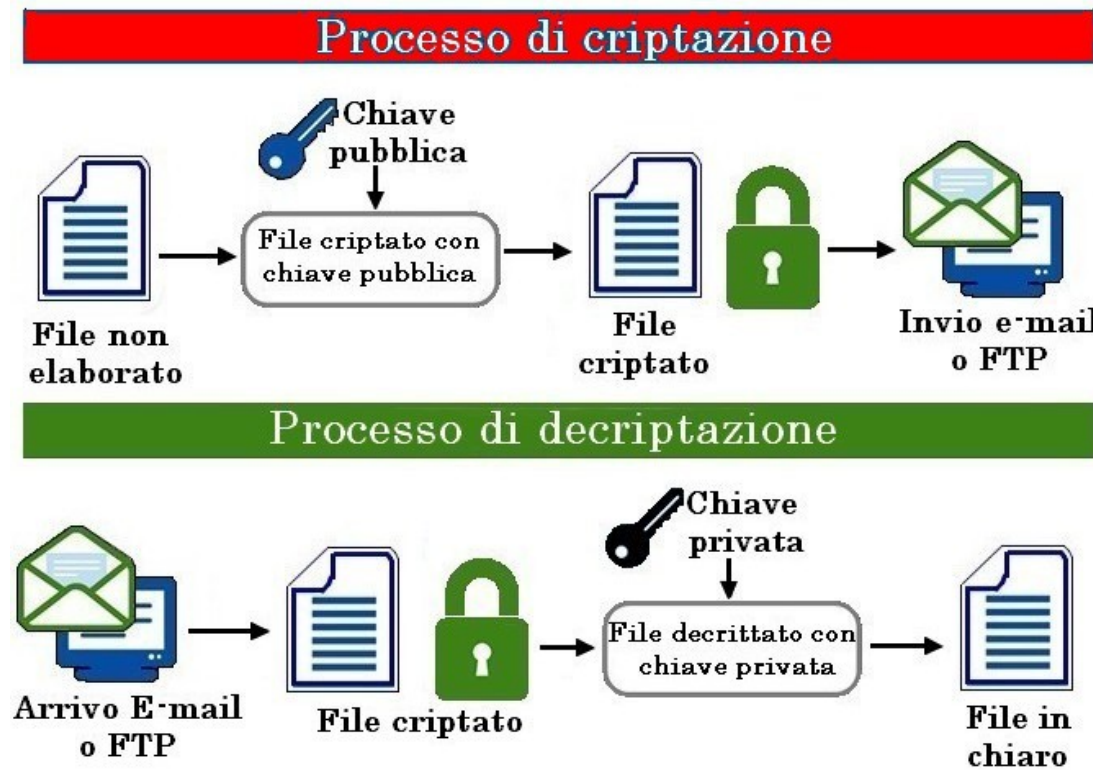
Oggi si raccomanda di utilizzare password robuste, uniche per ogni servizio, e di adottare sistemi di autenticazione multifattore (MFA).

I password manager aiutano a gestire credenziali complesse, mentre le chiavi di sicurezza hardware rappresentano lo standard più elevato di protezione.



# PKI: Infrastrutture a Chiave Pubblica

Le Infrastrutture a Chiave Pubblica (PKI) sono sistemi che permettono la gestione sicura di chiavi crittografiche e certificati digitali. Sono fondamentali per garantire autenticità e riservatezza nelle comunicazioni online, come avviene per la PEC, la Carta d'Identità Elettronica e la firma digitale.





# La Firma Digitale: Sicurezza e Valore Legale

La firma digitale utilizza la crittografia per garantire che un documento elettronico sia autentico, integro e non ripudiabile. In Italia e nell'Unione Europea, la firma digitale ha pieno valore legale e viene utilizzata per contratti, atti pubblici e comunicazioni ufficiali.

Firma il tuo documento

Seleziona il Certificato

Cognometest2016 Nometest2016

Dettagli

Inserisci Pin

\*\*\*\*\*

Salva in:

Aruba Firma

Aruba Firma

ifra

Tipo Busta

Aggiungi la firma al PDF

☐ Richiedi Timestamps

Formato PAdES-T

☐ Firma Grafica

☒ Firma Invisibile

Indietro

Avanti

# Single Sign-On: Un Solo Accesso per Tutti i Servizi

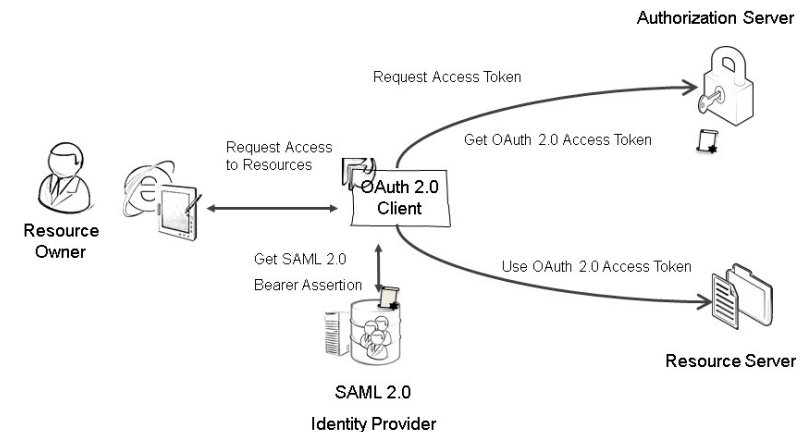
Il Single Sign-On (SSO) consente agli utenti di accedere a molteplici servizi utilizzando un'unica autenticazione. Questo semplifica la gestione delle credenziali, migliora l'esperienza utente e riduce il rischio di errori o furti di password. SPID, Google e Microsoft sono esempi di SSO.





# Identity Federation: Identità che Viaggiano tra Organizzazioni

La federazione delle identità permette a diversi enti o aziende di riconoscere reciprocamente le identità digitali degli utenti, favorendo l'accesso sicuro e trasparente a servizi condivisi. Standard come SAML e OAuth 2.0 sono alla base di queste soluzioni.



# Biometria e Nuove Tecnologie di Autenticazione

---

Le tecnologie biometriche (impronte digitali, riconoscimento facciale, voce, iride) offrono un livello di sicurezza superiore, basandosi su caratteristiche uniche dell'individuo. Tuttavia, pongono sfide in termini di privacy e inclusività, e richiedono algoritmi privi di bias.



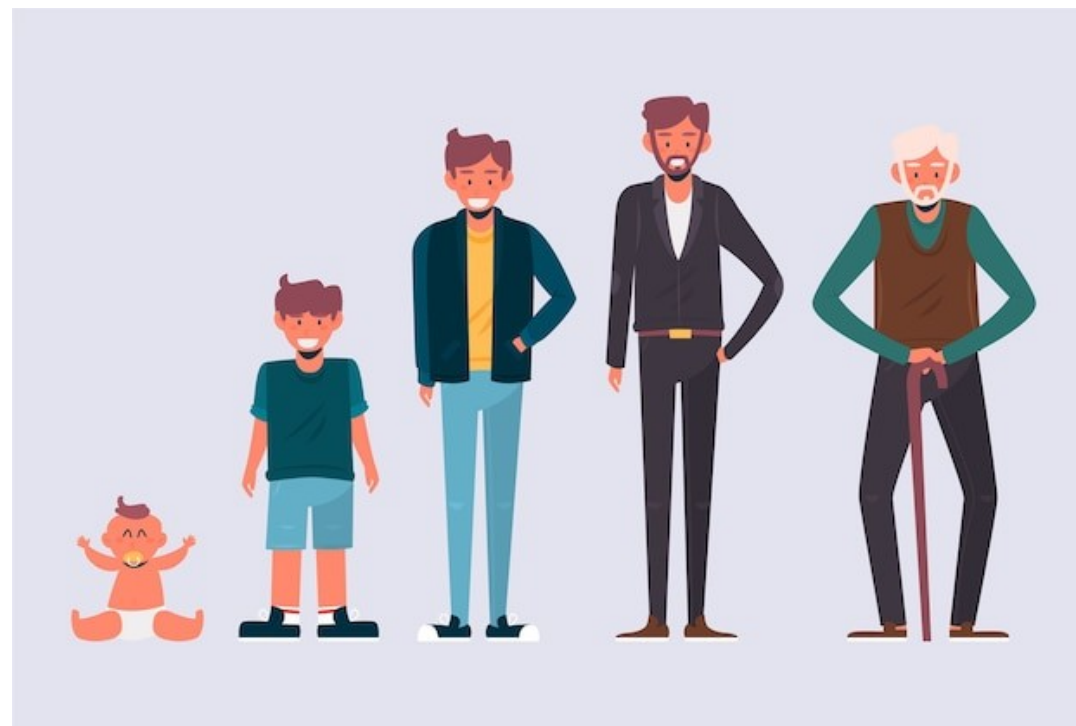
# L'Identità Digitale come Diritto Fondamentale

L'identità digitale è sempre più riconosciuta come un diritto fondamentale, essenziale per la partecipazione attiva alla vita sociale, economica e politica. In Italia si discute la sua tutela costituzionale, mentre strumenti come SPID e CIE ne garantiscono l'accesso.



# Inclusività e Accessibilità dei Sistemi di Identità

Per essere davvero universale, l'identità digitale deve essere accessibile a tutti, inclusi anziani, persone con disabilità e cittadini meno esperti. È fondamentale progettare interfacce inclusive e testare i sistemi su utenti diversi per ridurre il digital divide.





A background graphic featuring a world map composed of a network of blue lines and dots, representing a global digital network or blockchain technology. The word "BLOCKCHAIN" is written in large, white, sans-serif capital letters across the center of the map.

# BLOCKCHAIN

## **Sovranità Digitale: Il Controllo dell'Identità**

La sovranità digitale implica che ogni individuo abbia il pieno controllo sui propri dati e sulla propria identità online. Le soluzioni di Self-Sovereign Identity (SSI), spesso basate su blockchain, permettono di gestire e condividere le proprie credenziali in modo sicuro e decentralizzato.





---

## **Self-Sovereign Identity: Come Funziona**

Con la SSI, l'utente detiene un portafoglio digitale in cui conserva le proprie credenziali, rilasciate da enti verificati. Può decidere quali dati condividere e con chi, aumentando privacy e sicurezza. L'Europa promuove queste soluzioni con il regolamento eIDAS 2.

# Fiducia Digitale: Un Patrimonio da Costruire

La fiducia digitale si basa su trasparenza, sicurezza e rispetto della privacy. Standard, certificazioni e audit indipendenti sono fondamentali per prevenire frodi, furti d'identità e abusi, rafforzando il rapporto tra cittadini, aziende e istituzioni.



# Democrazia Elettronica: Partecipazione e Trasparenza

---

La democrazia elettronica sfrutta l'identità digitale per facilitare la partecipazione politica: votazioni online, consultazioni pubbliche, accesso agli open data. La tecnologia può rendere la democrazia più inclusiva, trasparente e accessibile a tutti.





## **Sfide e Opportunità dell'Identità Digitale**

L'identità digitale offre grandi opportunità, ma pone anche sfide: protezione della privacy, sicurezza, inclusività e alfabetizzazione digitale. È necessario un impegno condiviso per garantire innovazione e rispetto dei diritti fondamentali.



# Conclusioni e Prospettive Future

L'identità digitale è un pilastro della cittadinanza moderna. Per il futuro, sarà sempre più importante sviluppare soluzioni sicure, inclusive e rispettose dei diritti, coinvolgendo cittadini, istituzioni e imprese in un percorso di crescita digitale sostenibile.

