

# Identità Digitale

1. Introduzione
2. SPID
3. Firma Digitale
4. Certificato Digitale e Certification Authorities
5. Conclusioni
6. Finalmente un po'di pratica!

# 0. CIA triad

- **Confidenzialità (Confidentiality)**

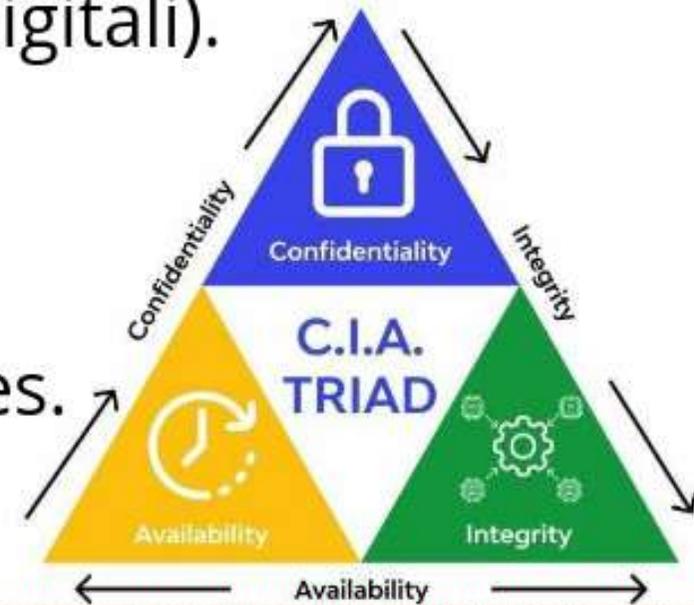
Garantisce che solo le persone autorizzate possano accedere ai dati, prevenendo accessi non autorizzati (es. crittografia, autenticazione).

- **Integrità (Integrity)**

Assicura che i dati non vengano modificati o alterati senza autorizzazione, mantenendoli affidabili e accurati (es. checksum, firme digitali).

- **Disponibilità (Availability)**

I dati e i servizi devono essere sempre accessibili quando necessari, evitando interruzioni causate da guasti o attacchi (es. backup, protezione DDoS).



# 1. Introduzione all'ID

- **Cos'è l'Identità Digitale?**

L'identità digitale è un *insieme di informazioni* elettroniche che permettono di *identificare* un utente online. Può includere credenziali di accesso (username e password), certificati digitali e sistemi di autenticazione avanzati come lo SPID.

- **Differenza tra identità fisica e digitale**

L'identità fisica è legata ai documenti ufficiali di una persona (carta d'identità, passaporto, codice fiscale). L'identità digitale, invece, è l'equivalente elettronico che permette di riconoscere un individuo nei servizi online.

- **Perché è importante nell'era digitale?**

Con la digitalizzazione dei servizi pubblici e privati, avere un'identità digitale sicura permette di accedere in modo rapido e protetto a piattaforme governative, bancarie e aziendali senza dover usare documenti cartacei.

# 2. SPID

1/2

## (Sistema Pubblico di Identità Digitale)

- **Cos'è SPID e a cosa serve?**

SPID è il *sistema di autenticazione online* del governo italiano, che permette ai cittadini e alle imprese di accedere ai servizi pubblici e privati con un'unica identità digitale. Serve per autenticarsi su siti della *Pubblica Amministrazione* (es. INPS, Agenzia delle Entrate) e su alcuni servizi privati.

- **Livelli di sicurezza di SPID (Livello 1, 2 e 3)**

- **Livello 1:** Accesso con username e password.
- **Livello 2:** Richiede un secondo fattore di autenticazione, come un codice OTP generato da un'app o inviato via SMS.
- **Livello 3:** Utilizza dispositivi fisici di sicurezza (smart card o chiavi crittografiche) per garantire la massima protezione.

- **Come ottenere lo SPID (fornitori e requisiti)**

Per ottenere lo SPID è necessario:

- Essere maggiorenni.
- Avere un documento d'identità valido e la tessera sanitaria.
- Scegliere un Identity Provider (es. Aruba, Poste Italiane, TIM, InfoCert) e completare la registrazione tramite riconoscimento (di persona, con webcam, o firma digitale).

# 2. SPID

## (Sistema Pubblico di Identità Digitale)

2/2

- **Utilizzo dello SPID: accesso a servizi della PA, uso privato e aziende**
  - **Cittadini:** Accesso a servizi come INPS, Fascicolo Sanitario Elettronico, Agenzia delle Entrate.
  - **Aziende:** Uso per bandi pubblici, fatturazione elettronica, autenticazione su portali aziendali.
  - **Privati:** Alcune banche e assicurazioni supportano l'accesso via SPID.
- **Sicurezza e rischi dello SPID**
  - SPID migliora la sicurezza degli accessi, ma può essere vulnerabile a phishing e furto di credenziali. È importante proteggere i dati di accesso e non condividere le credenziali con nessuno.

# 3. Firma Digitale

1/2

- **Cos'è la firma digitale e differenza con la firma elettronica**  
La firma digitale è un sistema di autenticazione elettronica che garantisce l'integrità e l'autenticità di un documento. È diversa dalla semplice firma elettronica, che può essere anche un'immagine della firma manuale.
- **Come funziona la firma digitale (crittografia asimmetrica, certificati digitali)**  
Si basa sulla **crittografia asimmetrica** con due chiavi:
  - **Chiave privata:** utilizzata per firmare il documento.
  - **Chiave pubblica:** usata per verificare l'autenticità della firma.  
Un certificato digitale, rilasciato da un'Autorità di Certificazione, collega le chiavi all'identità dell'utente.
- **Tipologie di firma elettronica:**
  - **Firma elettronica semplice:** Non garantisce l'identità del firmatario.
  - **Firma elettronica avanzata (FEA):** Associa univocamente la firma all'utente, garantendo integrità e autenticità.
  - **Firma elettronica qualificata (FEQ):** Ha valore legale equivalente alla firma autografa.

# 3. Firma Digitale

2/2

- **Strumenti per la firma digitale (token USB, smart card, software)**
  - **Token USB:** Dispositivo che contiene le chiavi di firma.
  - **Smart card:** Carta con chip utilizzabile tramite lettore.
  - **Software (es. Dike, ArubaSign):** Programmi per firmare documenti digitalmente.
- **Validità legale della firma digitale**

La firma digitale ha pieno valore legale ed è riconosciuta a livello europeo grazie al regolamento eIDAS.

# 4. Certificati Digitali e Autorità di Certificazione (CA)

- **Cos'è un certificato digitale e a cosa serve?**

Un certificato digitale è un *documento elettronico* che associa un'identità (persona o azienda) a una chiave pubblica. Serve per firmare documenti, autenticarsi su siti web e cifrare dati.

- **Ruolo delle Autorità di Certificazione (CA)**

Le CA sono enti riconosciuti che emettono certificati digitali garantendo l'identità del richiedente (es. Aruba, InfoCert, Actalis).

- **Differenze tra certificato digitale e firma digitale**

- Un **certificato digitale** è l'equivalente elettronico di un documento d'identità.
- Una **firma digitale** utilizza il certificato per garantire l'integrità e autenticità di un documento.

# 5. Conclusioni

## *Vantaggi:*

- Maggiore sicurezza
- semplificazione degli accessi online
- riduzione della burocrazia.

## *Svantaggi:*

- Necessità di dispositivi compatibili
- rischio di attacchi informatici.

## **Evoluzione futura: CIE, CNS, Wallet digitali europei**

- **CIE (Carta d'Identità Elettronica):** Può essere usata per autenticarsi online con un lettore NFC.
- **CNS (Carta Nazionale dei Servizi):** Rilasciata dalle regioni per accedere ai servizi sanitari e amministrativi.
- **Wallet digitali europei:** Progetto dell'UE per creare un portafoglio digitale che permetta di gestire documenti e autenticazioni in tutta Europa.

# 6. Finalmente un po' di pratica

- **Accesso al FSE (Fascicolo Sanitario Elettronico)**
- **Accesso al Portale dell'Automobilista**
- **Firma digitale di un documento**