

Identità Digitale, Autenticazione e Fiducia nelle Reti

Relazione di Sistemi e Reti – Classe 4D

Studente: Capuzzo Nicolò

Anno scolastico: 2024/2025

Introduzione



- • L'autenticazione digitale è fondamentale per la sicurezza informatica.
- • Protegge dati personali e transazioni online in ogni ambito.

Metodi di Autenticazione



- PASSWORD



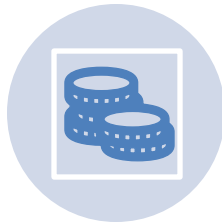
- BIOMETRICA



- CERTIFICATI DIGITALI



- AUTENTICAZIONE A
DUE O PIÙ FATTORI
(2FA/MFA)



- TOKEN



- AUTENTICAZIONE
FEDERATA (SSO)



- PASKEY E
AUTENTICAZIONE
PASSWORDLESS

Autenticazione Biometrica

- • Impronta digitale
- • Riconoscimento facciale
- • Scanner dell'iride o della retina
- • Riconoscimento vocale

Certificati e 2FA



- Certificati digitali come passaporto elettronico.



- 2FA/MFA: combinazione di password con altri fattori (es. codice, impronta).

Token e Autenticazione Federata

- Token fisici o virtuali generano codici temporanei.

- Federata: login unico con Google, Facebook, ecc.

Passkey e Passwordless



- AUTENTICAZIONE SENZA PASSWORD.



- USO DI DISPOSITIVI SICURI E BIOMETRIA.

Gestione dell'Identità (IMS)



- Automatizzazione account e permessi.



- Verifica biometrica/documentale.



- Dashboard, report e integrazioni (es. Active Directory).

Blockchain e Identità Digitale



- SICUREZZA E TRASPARENZA
GRAZIE ALLA DECENTRALIZZAZIONE.



- SOULBOUND TOKEN: IDENTITÀ
DIGITALE IMMUTABILE.


Rischi e Best Practice

- Rischi: furto identità, phishing, password deboli.

- Best practice: MFA, password forti, software aggiornati.



Ciclo di Vita dell'Identità Digitale



1. Creazione
dell'identità

The diagram illustrates the Digital Identity Lifecycle as a sequence of three steps. Each step is represented by a light gray rounded rectangle with a dark blue header and a dark blue border. The rectangles are arranged horizontally and slightly overlap. The first rectangle contains the text '1. Creazione dell'identità', the second contains '2. Verifica e certificazione', and the third contains '3. Utilizzo per accedere ai servizi'. A solid purple horizontal line is positioned at the bottom of the slide.

2. Verifica e
certificazione

3. Utilizzo per
accedere ai
servizi



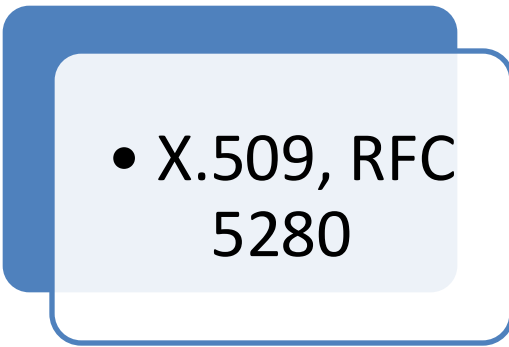
Etica e Inclusione

- Inclusione digitale e accessibilità.

- Privacy e protezione dati sensibili (es. GDPR).
-



Standard e Normative



- X.509, RFC 5280



- eIDAS, ISO/IEC 27001



- NIST SP 800-63



Caso SPID e PKI

- SPID: accesso ai servizi pubblici online.

- Sicurezza e interoperabilità tramite PKI.
-

Analisi Critica

- • Vantaggi: sicurezza, interoperabilità, flessibilità.
- • Limiti: complessità, costi, accessibilità.

Conclusione

- • L'identità digitale è parte essenziale della vita moderna.
- • Necessarie sicurezza, gestione centralizzata e approccio etico.