LEZ4 SICUREZZA DEI SERVIZI DI AUTENTICAZIONE AUTORIZZAZIONE DELL'IDENTITÀ DIGITALE

GLOSSARIO

Termine	Definizione
Identity Provider (IdP)	Entità che autentica utenti e rilascia token.
Federation	Insieme di domini che condividono fiducia reciproca.
DID(Decentralized Identifier)	Identificatore crittografico verificabile su rete distribuita.
Verifiable Credential (VC)	Attestazione digitale firmata e verificabile.
Wallet digitale	Applicazione che conserva chiavi e credenziali SSI.
TPM (Trusted Platform Module)	Chip che custodisce chiavi di sicurezza hardware.
AAL (Authentication Assurance Level)	Livello di garanzia dell'autenticazione (NIST SP 800-63).
PKI (Public Key Infrastructure)	Sistema di certificazione basato su chiavi pubbliche.
Zero Trust	Modello che impone verifica continua e minima fiducia implicita.
SSO (Single Sign-On)	Accesso unificato a più servizi tramite un'unica autenticazione.

SCHEMA DEI FLUSSI EIDAS 2 / WALLET / SSI

Titolo: "Flusso di fiducia nel modello eIDAS 2"

Attori principali:

1. **Issuer (emittente):** università, PA, banca o ente certificatore che rilascia una ***verifiable credential***.
2. **Holder (titolare):** cittadino europeo che custodisce le proprie credenziali nel ***Digital Identity Wallet***.
3. **Verifier (verificatore):** soggetto pubblico o privato che controlla la validità della credenziale.
4. **Trust Anchor:** infrastruttura di fiducia (registro europeo, EBSI, ente di certificazione).

Flusso logico:

1***Emissione*** → l'Issuer crea e firma digitalmente la credenziale (es. laurea, patente).
2 ***Archiviazione*** → l'Holder la conserva nel Wallet sotto il proprio controllo.
3***Presentazione*** → l'Holder decide quali dati condividere (principio di minimizzazione).
4 ***Verifica*** → il Verifier controlla la firma digitale e la validità della credenziale tramite la Trust Anchor.

Concetto chiave:

Il Wallet funge da "ponte di fiducia" fra emittenti e verificatori, mantenendo la sovranità dell'utente sui propri dati.

Benefici :

- Riduzione dei dati condivisi ("need-to-know").
- Eliminazione dell'intermediazione centralizzata.
- Tracciabilità e audit automatici.

Il regolamento eIDAS 2, il Digital Identity Wallet e la Self-Sovereign Identity

Introduzione: dal modello centralizzato al modello sovrano

Il regolamento europeo **eIDAS 2 (Regolamento UE 2024/1183)** rinnova profondamente il quadro di fiducia digitale introdotto dal precedente eIDAS (2014), stabilendo un modello di **identità digitale europea sovrana, interoperabile e verificabile**.

L'obiettivo è creare un ecosistema nel quale ogni cittadino europeo possa:

- possedere un'identità digitale riconosciuta in tutta l'Unione,
- gestire in autonomia i propri attributi e credenziali,
- autenticarsi e firmare digitalmente documenti senza dipendere da piattaforme private.

La vera innovazione è il **Digital Identity Wallet (portafoglio europeo di identità digitale)**, fondato sul paradigma della **Self-Sovereign Identity (SSI)**.
Con il wallet, l'identità digitale non è più "fornita" da un ente centrale ma **appartiene all'utente**, che la custodisce e la presenta in modo sicuro e selettivo.

Struttura e finalità del regolamento eIDAS 2

Obiettivi principali

1. Fornire a ogni cittadino un mezzo di identificazione digitale valido in tutta l'UE.
2. Assicurare **portabilità** e **interoperabilità** di identità e attributi digitali.
3. Estendere l'uso dell'identità digitale ai servizi privati di interesse generale.
4. Favorire un modello di **fiducia decentralizzato**, riducendo la dipendenza dalle Big Tech.

5. Migliorare la protezione dei dati personali e la trasparenza delle transazioni digitali.

STRUTTURA TECNICA

Il regolamento introduce:

- il **European Digital Identity Framework (EDIF)**, che definisce standard comuni per tutti gli Stati membri;
- i **portafogli europei di identità digitale (European Digital Identity Wallets)**, interoperabili a livello UE;
- formati standardizzati per le **verifiable credentials** e le **electronic attestations of attributes (EAA)**;
- obblighi di interoperabilità per enti pubblici e privati "di rilevanza significativa".

Esempio – Uso transfrontaliero del wallet
Un cittadino italiano può accedere a un portale sanitario in Germania utilizzando il proprio wallet.
Il sistema riceve solo l'attributo richiesto ("codice sanitario europeo") senza esporre altri dati personali, in conformità al principio di minimizzazione del GDPR.

IL CONCETTO DI EUROPEAN DIGITAL IDENTITY WALLET

COS'È

Il **Digital Identity Wallet** è un portafoglio digitale personale che permette di:

- conservare credenziali di identità (eID);
- gestire attestazioni e titoli digitali (es. patente, laurea, partita IVA);
- firmare documenti e autenticarsi ai servizi pubblici e privati.

Il wallet è un **software certificato**, implementabile come app o componente hardware sicuro, che custodisce le chiavi crittografiche e le credenziali rilasciate da entità fidate.

Caratteristiche principali

Caratteristica	Descrizione	Impatto sulla fiducia
Sovranità dell'utente	L'utente decide quali dati condividere e con chi	Controllo personale dei dati
Verificabilità	Ogni credenziale è firmata digitalmente e verificabile	Integrità e non ripudio
Interoperabilità UE	Standard tecnici comuni per tutti gli Stati	Accesso unificato ai servizi
Minimizzazione dati	Condivisione selettiva (principio "least disclosure")	Conformità GDPR
Portabilità	Utilizzabile ovunque in UE	Continuità dei servizi e fiducia transfrontaliera

Esempio – Firma di un contratto immobiliare in UE

Un cittadino francese firma digitalmente un contratto in Spagna usando il proprio wallet.
Il documento è legalmente valido in tutta l'UE senza necessità di certificazioni aggiuntive.

Il legame con la Self-Sovereign Identity (SSI) Concetto di SSI

La **Self-Sovereign Identity (SSI)** è un modello decentralizzato di identità in cui l'utente:

1. genera e controlla i propri identificatori digitali (***Decentralized Identifiers – DID***);
2. riceve ***Verifiable Credentials (VC)*** firmate da enti di fiducia;
3. presenta tali credenziali in modo verificabile e selettivo ai servizi che ne fanno richiesta.

Il wallet eIDAS 2 **implementa il paradigma SSI** integrando standard W3C (DID, VC Data Model) con protocolli europei di certificazione.

PROCESSO TIPICO SSI

1. **Emissione** – un'università emette una credenziale firmata ("Laurea in Ingegneria").
2. **Conservazione** – lo studente la archivia nel proprio wallet.
3. **Presentazione** – durante un colloquio di lavoro, condivide solo il titolo richiesto.
4. **Verifica** – il datore di lavoro controlla la firma sul registro pubblico, senza contattare l'università.

Esempio – Diploma digitale europeo

Grazie al wallet, un laureato italiano può dimostrare il titolo in Svezia senza inviare documenti cartacei. La verifica è immediata, automatica e legalmente riconosciuta. Il concetto chiave alla base dell'infrastruttura che consente di utilizzare il wallet è quello di registro pubblico. Ora lo tratteremo in modo specifico e in relazione al concetto di anchor considerate le criticità poste dalla progettazione di un sistema che utilizzi il wallet.

Il Registro pubblico come elemento critico nella progettazione

Nonostante quanto detto sinora nella progettazione di una infrastruttura che utilizzi EIDAS2 come riferimento il termine "registro pubblico" (ledger o blockchain) può generare ambiguità e persino contraddizioni rispetto ai principi di ***self-sovereignity***. Vediamo meglio i problemi che si creano e come vengono trattati nei modelli SSI più coerenti.

AMBIGUITÀ CONCETTUALE DEL "REGISTRO PUBBLICO"

Nel linguaggio comune, "registro pubblico" evoca un'entità terza che **controlla o supervisiona** i dati.
Ma nel modello SSI **non deve esistere un supervisore centrale**: i

l registro serve solo a **pubblicare le chiavi pubbliche e gli schemi di credenziali** (es. chiavi dell'università o della CA), **non i dati personali**.

In altre parole:

- **Sul ledger** non sono registrati i miei attributi **(es. "nome", "laurea"** ecc.);
- Sono registrati solo gli ancoraggi crittografici (vedi nota) necessari alla verifica della firma.

n.b. "Ancoraggio crittografico" → per indicare il legame hash-ledger. "Anchor" → per indicare l'oggetto o il riferimento pubblicato sul registro.

Questo distingue un *ledger pubblico* da un *registro di attributi* (che sarebbe incompatibile con la privacy SSI).

Ruolo del ledger: notarizzazione, non supervisione

Il ledger agisce come un **notaio digitale (notary) pubblico decentralizzato**:

- Garantisce l'**immutabilità e la disponibilità** delle chiavi pubbliche e delle revocation list;
- Permette a chi verifica di essere sicuro che la firma del credential issuer sia autentica e non revocata;
- Ma **non partecipa attivamente alla validazione dei dati**.

Il controllo resta distribuito:

- l'**Issuer** firma e pubblica la propria chiave pubblica;
- il **Holder** conserva e presenta selettivamente la credenziale;
- il **Verifier** controlla la validità crittografica senza interpellare l'Issuer.

Il Concetto di Anchor nel modello Self-Sovereign Identity (SSI)

Dato il modello Self-Sovereign Identity (SSI), in una implementazione SSI corretta , il registro (o ledger) non custodisce dati personali, ma svolge una funzione puramente crittografica di notarizzazione tramite l'uso delle cosiddette 'anchor' che quindi richiede un'approfondimento accurato.

Definizione di Anchor

Un'anchor (in italiano: 'àncora') è un riferimento crittografico che collega un'informazione custodita fuori dalla blockchain a un punto specifico del registro pubblico, senza rivelarne il contenuto. Si tratta di una 'impronta digitale' (hash) calcolata sui dati, che consente di verificarne l'autenticità e l'integrità senza esporre il contenuto stesso.

Esempio pratico

Immaginiamo che un'università emetta una credenziale digitale contenente i seguenti dati:
• Nome: Mario Rossi
• Titolo: Laurea in Ingegneria
• Data: 15/10/2025

Da questi dati viene calcolata una firma crittografica, o più precisamente il suo hash. Sul ledger viene pubblicato solo tale hash, che costituisce l'anchor. Chiunque, in futuro, potrà verificare la validità della credenziale ricalcolando l'hash e confrontandolo con quello pubblicato sul ledger. Se coincidono, la credenziale è autentica e non è stata alterata.

FUNZIONI DELL'ANCHOR

Funzione	Descrizione
Integrità	Garantisce che il documento originale non sia stato modificato.
Verificabilità	Permette di verificare la firma senza contattare l'emittente.
Privacy	Nessun dato personale è visibile: solo l'impronta (hash).
Persistenza	L'anchor (legame hash documento) resta nel tempo sul ledger, anche se il documento originale è archiviato altrove.

ANALOGIA INTUITIVA

L'anchor può essere paragonata al numero di protocollo di un atto notarile: il notaio registra solo il numero e la firma, mentre il documento vero resta

nell'archivio del titolare. Chi vuole verificare l'autenticità consulta il registro e confronta il numero, senza leggere il contenuto del documento.

Conclusione

Nel modello SSI, le chiavi pubbliche degli emittenti (issuers) e le anchor delle credenziali sono le uniche informazioni registrate sul ledger. Le credenziali e i dati personali restano invece nel wallet dell'utente. Questo approccio preserva l'autonomia, la privacy e la verificabilità crittografica, evitando ogni forma di supervisione centralizzata o esposizione dei dati sensibili.

Problemi di sicurezza che possono emergere

Se male implementato, il "registro pubblico" introduce rischi:

- **Rischio di correlazione:** se i DID o i riferimenti sono tracciabili, un attore può ricostruire la rete delle relazioni tra identità.
- **Rischio di centralizzazione nascosta:** se pochi nodi controllano il ledger, si perde la proprietà di decentralizzazione.
- **Rischio di revocation leakage:** le revocation list possono esporre metadati identificabili.
- **Rischio di trust leakage:** se un attore diventa "di fatto" il gestore del registro, si ritorna a una logica di ***trust anchor*** centralizzata.

SOLUZIONI PROPOSTE NEI MODELLI SSI PIÙ MATURI

Per mitigare questi problemi, si stanno affermando diversi approcci:

1. **DID off-ledger** o ***peer DID***: le chiavi vengono scambiate direttamente tra attori, senza pubblicarle su blockchain.
2. **Verifiable Data Registry minimizzato:** la blockchain contiene solo ancore crittografiche, mai dati o identificatori permanenti.
3. **Zero-Knowledge Proofs (ZKP):** il titolare prova la validità di un attributo (es. "ho una laurea") senza rivelare l'attributo completo.
4. **Privacy-preserving revocation:** uso di ***cryptographic accumulators*** per gestire le revoche senza esporre identità.
5. **Layer di governance trasparenti:** consorzi multi-attore (es. eIDAS 2.0 wallet trust frameworks) invece di un unico "registro pubblico".

Riepilogo

DIFFERENZE TRA EIDAS 1 E EIDAS 2

Aspetto	eIDAS 1 (2014)	eIDAS 2 (2024)
Modello di identità	Basato su provider nazionali certificati	Basato su wallet europei interoperabili
Controllo dei dati	Centralizzato (provider → utente)	Self-sovereign (utente → provider)
Attributi verificabili	Limitati (solo identità)	Estesi (patenti, titoli, qualifiche)
Interoperabilità UE	Parziale	Totale e obbligatoria

Aspetto	eIDAS 1 (2014)	eIDAS 2 (2024)
Servizi privati	Non obbligatori	Devono accettare il wallet se “rilevanti”
Tecnologie	SAML, PKI	DID, VC, blockchain, standard W3C

Criticità e prospettive

Tema	Criticità	Soluzione proposta
Standardizzazione	Specifiche SSI e DID ancora in evoluzione	Coordinamento ETSI–W3C–EBSI
Responsabilità legale	Attribuzione di colpa in caso di errore d’identità	Definizione di “Trust Anchors” nazionali
Usabilità	Gestione chiavi e wallet non intuitiva per utenti comuni	Interfacce semplificate e supporto AI
Compatibilità SPID/CIE	Necessità di convergenza con sistemi esistenti	Evoluzione di SPID verso “wallet nazionale” conforme eIDAS 2

🟦 **Nota operativa – SPID e Wallet Europeo**
SPID potrà diventare una componente nazionale del sistema eIDAS 2, garantendo continuità agli utenti italiani e ampliando la compatibilità con credenziali europee e universitarie.

7. Conclusione

Il regolamento **eIDAS 2** rappresenta il pilastro dell'identità digitale europea. Con il **Digital Identity Wallet**, l'Europa introduce un modello unico al mondo:

- basato su **fiducia istituzionale**,
- garantito da **sovranità individuale**,
- sostenuto da **standard aperti**.

Il futuro dell'identità digitale europea si muove verso un equilibrio tra:

- sicurezza e usabilità,
- interoperabilità e privacy,
- fiducia pubblica e innovazione decentralizzata.

Glossario

Termine	Definizione
eIDAS	Regolamento UE sull'identificazione elettronica e i servizi fiduciari.
Digital Identity Wallet	Portafoglio digitale per conservare e condividere credenziali eID.
SSI (Self-Sovereign Identity)	Modello di identità decentralizzata controllata dall'utente.
DID (Decentralized Identifier)	Identificatore crittografico verificabile in rete decentralizzata.
VC (Verifiable Credential)	Attestazione firmata digitalmente e verificabile.
EBSI	European Blockchain Services Infrastructure.
AAL (Authentication Assurance Level)	Livello di garanzia dell'autenticazione definito dal NIST SP 800-63.

Termine	Definizione
SPID	Sistema Pubblico di Identità Digitale (Italia), basato su modello federato.
Trust Anchor	Entità di fiducia che certifica identità e attributi nel sistema eIDAS 2.
GDPR	Regolamento generale UE sulla protezione dei dati personali.