UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

EUDI WALLET: RIVOLUZIONE DELL'IDENTITÀ DIGITALE IN EUROPA

ANNO ACCADEMICO 2023/2024

Data di laurea: 12 Novembre 2024

Laureando/a: Vivaldi Giuseppe

Relatore: Prof. / Dott. Migliardi Mauro

Indice

Introduzione

La rapida evoluzione della tecnologia digitale avvenuta negli ultimi decenni ha trasformato profondamente il modo in cui le persone interagiscono con il mondo, la digitalizzazione ha penetrato quasi ogni aspetto della nostra vita quotidiana, dalla comunicazione ai servizi pubblici.
Ciò nonostante, per alcuni problemi non si è ancora arrivati ad una soluzione digitale a livello mondiale, uno dei problemi più importanti è sicuramente quello dell'identificazione.

Storicamente, l'identità è legata a documenti fisici come passaporti, carte d'identità e patenti di guida, tuttavia, questi strumenti tradizionali talvolta possono essere clonati o falsificati per non parlare del rischio di perdita o di furto.
Queste mancate solidità, la crescente diffusione di servizi online e l'uso massiccio delle tecnologie digitali, hanno sollevato non pochi pensieri in merito alla necessità di un nuovo metodo di identificazione digitale con le dovute precauzioni legate alla sicurezza, alla privacy e alla gestione delle informazioni personali.

Emerge quindi l'identità digitale come soluzione innovativa per garantire che le interazioni online siano sicure e affidabili, fornendo un mezzo per verificare l'identità di una persona in modo rapido ed efficace, secondo uno studio della Commissione Europea del 2021, oltre il 60% degli europei preferisce interagire con i servizi pubblici tramite mezzi digitali, sollecitando quindi la creazione di una soluzione sicura ed efficace.

In questo scenario, l'European Digital Identity (EUDI) Wallet rappresenta un passo fondamentale verso la realizzazione di un sistema di identità digitale a livello europeo. Il progetto EUDI Wallet mira a fornire ai cittadini europei uno strumento sicuro e user-friendly per gestire le proprie credenziali digitali, facilitando l'accesso a servizi pubblici e privati in tutta l'Unione Europea.
L'adozione di un portafoglio digitale non solo migliora l'efficienza e la sicurezza delle transazioni online, ma promuove anche l'inclusione digitale, assicurando che tutti i cittadini abbiano accesso agli stessi strumenti e opportunità nel mondo digitale.

Le motivazioni alla base della creazione del EUDI Wallet, oltre a quelle sopra citate, consistono anche nella necessità di affrontare il problema della frammentazione dei sistemi di identità digitale attualmente esistenti, un portafoglio digitale europeo standardizzato può ridurre la complessità e i costi associati alla gestione di identità multiple, aumentando al

contempo la fiducia dei cittadini nei servizi digitali, inoltre, promuove la cooperazione tra gli Stati membri, rafforzando l'integrazione europea.

Identità Digitale in Europa e regolamentazione eIDAS

Il concetto di identità digitale è già stato esplorato in molte nazioni dell'unione europea, per esempio in Italia esiste SPID (Sistema Pubblico di Identità Digitale), con il quale il cittadino può accedere ai servizi nazionali e dei paesi membri dell'unione europea che hanno scelto SPID come metodo di identificazione ("SPID").
Così come in Italia, anche in altri stati come Germania e Svezia già si sta adottando l'eID, tuttavia l'obiettivo dell'Unione Europea è quello di fornire al cittadino e ad imprese un metodo di identificazione che sia univoco per ogni Stato membro, per questo motivo è stato adottato il regolamento eIDAS (electronic IDentification, Authentication and trust Services), entrato in vigore il 17 settembre 2014 applicato praticamente a partire dal 1º luglio 2016.
("eIDAS Regulation | Shaping Europe's digital future")

Questo regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell' eBusiness e del commercio elettronico nell'Unione europea.
Tuttavia, con il passare del tempo, l'applicazione pratica di questo regolamento ha evidenziato alcune limitazioni, specialmente riguardo alla sua adozione nel settore privato e alla scarsa interoperabilità tra i sistemi di identità digitale degli Stati membri

Nel 2021, la Commissione Europea ha riconosciuto che, sebbene l'eIDAS originale avesse gettato solide basi, non era sufficiente per affrontare le nuove esigenze del mercato digitale e la crescente complessità della sicurezza online, uno dei principali problemi riscontrati, infatti, era la limitata adozione delle soluzioni di identificazione elettronica (eID): solo il 59% dei residenti dell'UE aveva accesso a schemi eID sicuri e interoperabili tra i vari Stati membri senza contare che pochi di questi sistemi erano disponibili in forma mobile, limitando ulteriormente la loro fruibilità e diffusione.
C'è da tener conto anche che nessun paese era obbligato a sviluppare un'identità digitale nazionale e a renderla interoperabile con quelle degli altri Stati membri, il regolamento stesso inoltre non prevedeva l'uso dell'identificazione elettronica per i servizi privati o per i

dispositivi mobili, creando ulteriori discrepanze tra le nazioni. (“Proposal amending Regulation (EU) No 910/2014”)

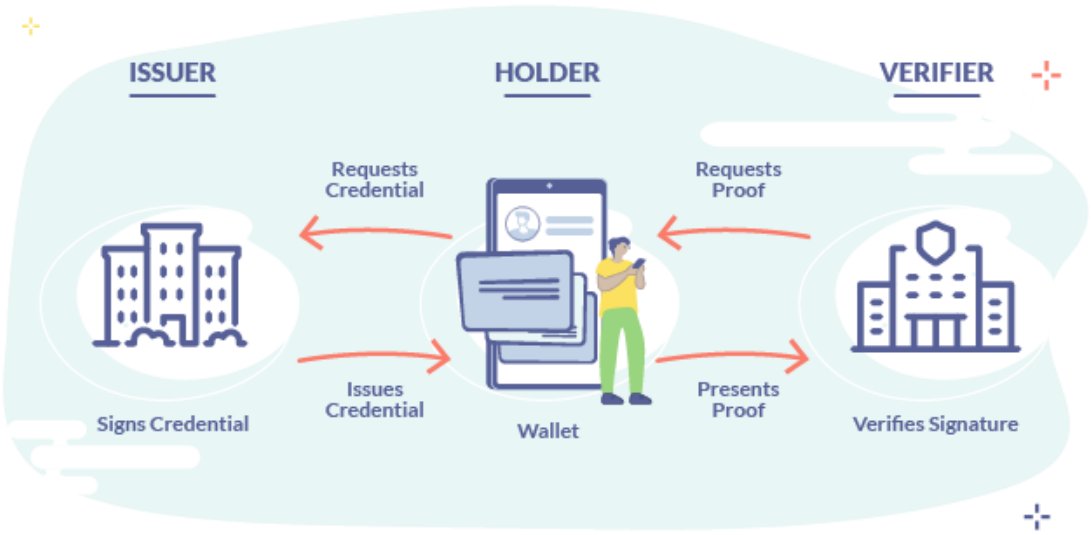
Al contempo, i sistemi di identificazione e autenticazione sviluppati al di fuori del quadro eIDAS possono rispondere solo parzialmente a queste sfide, per esempio i servizi di autenticazione offerti da terze parti (come l'uso di un account Facebook o Google per accedere a vari servizi) sono comuni per i servizi privati non regolamentati, che non richiedono un alto livello di sicurezza, ma non possono garantire lo stesso livello di certezza legale, protezione dei dati e privacy, principalmente perché sono autocertificati e non collegati a eID governativi sicuri e affidabili. (“Revision of the eIDAS Regulation”)

In risposta a queste problematiche, la Commissione ha presentato la proposta per eIDAS 2.0 nel giugno 2021 con l'obiettivo principale di aggiornare il regolamento per rendere possibile la creazione di un portafoglio di identità digitale europeo (EUDI Wallet).
Dopo la fase di consultazione e i briefing che hanno coinvolto varie parti interessate, il nuovo regolamento ha visto la luce ufficialmente con il nome di eIDAS 2.0, questo framework riveduto e migliorato è entrato in vigore nel 2024, con l'obiettivo di garantire che entro il 2030 almeno l'80% dei cittadini dell'UE possa utilizzare soluzioni di identità digitale per accedere a servizi chiave.
Il regolamento, inoltre, si propone di migliorare la sicurezza e la fiducia nei sistemi di identità digitale, facilitando l'integrazione del settore privato e offrendo agli utenti un'esperienza più flessibile e sicura. (“Revision of the eIDAS Regulation”)

Identity Wallet

Con l'introduzione della tecnologia blockchain, è stato introdotto un nuovo modello di gestione dell'identità chiamato SSI (Self-Sovereign Identity), che offre all'utente il pieno controllo sulla propria identità digitale e conserva tutte le informazioni private in un Portafoglio Digitale posseduto e controllato dall'utente.
Il Portafoglio Digitale, o Digital Wallet, è analogo ad un portafoglio fisico che salva tutte le credenziali digitali come entità fisiche, verificabili e firmate digitalmente, di conseguenza sono molto più rapide da emettere e da verificare rispetto alle loro controparti fisiche. (“The Inevitable Rise of Self-Sovereign Identity”)

In pratica, gli utenti raccolgono all'interno del proprio wallet credenziali diverse, come certificati accademici, documenti di identità, qualifiche professionali, o autorizzazioni mediche, il tutto gestibile comodamente dall'utente tramite un identificatore unico e decentralizzato che può essere verificato tramite blockchain o altri sistemi distribuiti. L'infrastruttura di questi Decentralized Identifiers(DIDs) fa in modo che ogni persona possa essere identificata in modo sicuro, senza il bisogno di terze parti come Google o Facebook per gestire i processi di autenticazione, inoltre, una delle caratteristiche di un portafoglio d'identità digitale è la capacità di gestire l'accesso ai dati in modo selettivo, infatti quando un utente deve presentare le proprie credenziali, può scegliere quali informazioni condividere e con chi, limitando l'esposizione dei propri dati personali.



La figura riportata qui sopra mostra un sistema di gestione dell'identità incentrato sull'utente, con un Identity Wallet al centro dello stesso, il sistema coinvolge tre ruoli chiave: Emittente, Detentore e Verificatore (rispettivamente Issuer, Holder e Verifier).
L'Emittente crea e rilascia credenziali al Detentore che le riceve e conserva e, quando serve, le condivide con il Verificatore il quale riceve e verifica le credenziali presentate dal Detentore. Questo sistema elimina la necessità di un Fornitore terzo e supporta una relazione diretta tra il Detentore e un Verificatore, dando agli utenti il pieno controllo sui loro dati tramite l'uso di un portafoglio di identità. ("The Digital Wallet paradigm for identity.")

EUDI Wallet

Come accennato nell'introduzione precedente, con il regolamento eIDAS 2.0, uno dei requisiti fondamentali per ogni Stato membro è quello di fornire almeno un portafoglio digitale, che può essere pubblicato dallo Stato membro o comunque sotto l'autorità dello Stato membro e quindi deve essere riconosciuto dallo stesso, ciò rende possibili anche i portafogli privati e garantisce un'identità digitale sicura per ogni cittadino.

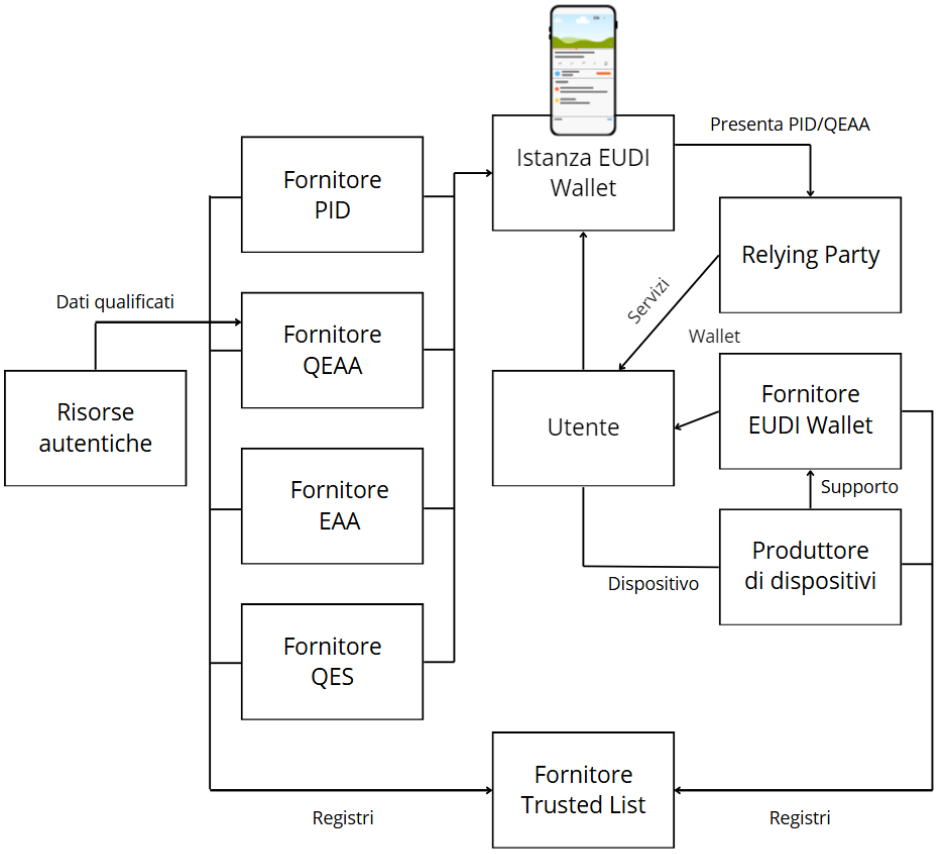
In questo contesto la Commissione Europea ha dato il via al progetto European Digital Identity Wallet (EUDI Wallet) puntando a fornire ai cittadini, residenti e imprese dell'Unione Europea un'identità digitale riconosciuta in tutta l'UE.
Questo portafoglio digitale personale consente a chi lo usa di identificarsi o fornire informazioni personali per accedere a servizi pubblici e privati, sia online che offline con tutti i benefici che ne conseguono come il collezionare e condividere informazioni personali come data e luogo di nascita, dati forniti da aziende private, certificazioni, attestati e molto altro. ("European Digital Identity - European Commission")

A tal proposito, il 3 giugno 2021 la Commissione Europea ha invitato gli Stati membri a lavorare allo sviluppo di un Toolbox, comprendente un insieme di standard e specifiche tecniche comuni e una serie di linee guida e buone pratiche condivise ovvero l'ARF(Architecture and Reference Framework).
L'invito prevede che il Toolbox venga sviluppato dagli esperti degli Stati membri nel Gruppo di Esperti eIDAS, in stretta coordinazione con la Commissione e, ove rilevante per il funzionamento dell'infrastruttura dell'EUDI Wallet, con altre parti interessate del settore pubblico e privato. ("Architecture and Reference Framework")

La prima versione del Toolbox contenente una bozza dell'ARF è stata pubblicata il 10 febbraio 2023, questa include una panoramica generale degli standard e delle pratiche necessarie per sviluppare l'EUDI Wallet e, dall'ora, viene aggiornato continuamente attraverso il lavoro in corso del Gruppo di Esperti eIDAS, utilizzando i feedback dei Large Scale Pilots, fino ad arrivare alla versione più recente datata 22 maggio 2024, con la versione 1.4 dell'ARF.

Ruoli nell’ecosistema di EUDI Wallet

L'ecosistema del European Digital Identity Wallet è progettato per offrire un'infrastruttura digitale sicura e interoperabile, capace di facilitare la gestione delle identità digitali a livello europeo.
La creazione di questo ecosistema è strettamente legata agli standard stabiliti dal regolamento eIDAS 2.0, che ha l'obiettivo di fornire ai cittadini un metodo affidabile per identificarsi e interagire con le istituzioni pubbliche e private nell'Unione Europea. La complessità dell'ecosistema deriva dalla necessità di garantire un elevato livello di sicurezza, protezione dei dati e flessibilità d'uso in vari contesti applicativi.



Il funzionamento dell’EUDI Wallet si basa sull'interazione di diversi ruoli chiave, ciascuno con compiti e responsabilità ben definiti, questi ruoli sono fondamentali per garantire la validità delle transazioni digitali e la corretta gestione delle identità.
Di seguito, si descrivono i principali attori coinvolti nell'ecosistema e il loro contributo al funzionamento del wallet.

Utente (User)

L’utente rappresenta l’individuo, sia cittadino che residente nell’UE, che utilizza l’EUDI Wallet per gestire la propria identità digitale e accedere a servizi online. L’utente è il centro dell’ecosistema, e uno degli obiettivi principali del portafoglio è restituire il controllo completo delle informazioni personali agli individui.
Attraverso il wallet, l’utente può autenticarsi in modo sicuro, presentare attestazioni e gestire i propri identificatori personali.
Gli utenti dei portafogli EUDI utilizzano il Portafoglio EUDI per ricevere, conservare e presentare il PID (Personal Identifiers), il QEAA (Qualified Electronic Attestation of Attributes), il PuB-EAA (Public Electronic Attestation of Attributes), o l'EAA (Electronic Attestation of Attributes) e per dimostrare la propria identità, inoltre, gli utenti possono anche creare Firme Elettroniche Qualificate (QES) e sfruttare interazioni wallet-to-wallet (da portafoglio a portafoglio). (“Architecture and Reference Framework”)

L'EUDI Wallet rappresenta un notevole avanzamento per la privacy dell’utente poiché aderisce a gran parte dei 10 principi della Self-Sovereign Identity (SSI) un modello di identità digitale che propone di restituire agli utenti il controllo totale sui propri dati, consentendo loro di decidere in modo selettivo quali informazioni condividere, migliorando così la sicurezza delle informazioni personali e garantendo una maggiore protezione contro il furto d’identità

Infine, il wallet europeo potrebbe contribuire a diffondere una maggiore consapevolezza sulla gestione dell'identità digitale e sulla protezione dei dati personali, attualmente infatti, molte persone non sono ancora completamente consapevoli dei rischi legati alla divulgazione non controllata delle proprie informazioni, l'uso del wallet e della condivisione selettiva delle informazioni potrebbe sensibilizzare i cittadini su questi temi cruciali, promuovendo una cultura della protezione dei dati. (“European Digital Identity Wallet: rischi e benefici”)

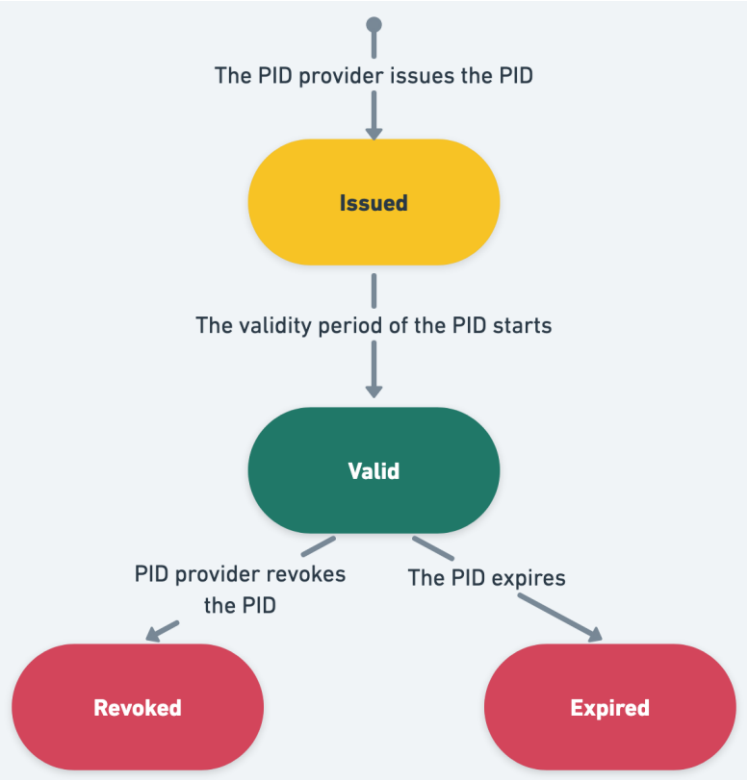
Fornitore del Wallet (Wallet Provider)

Il Fornitore del Wallet è responsabile dello sviluppo e della gestione dell’EUDI Wallet, questo ruolo può essere svolto da entità pubbliche, come governi nazionali, o da soggetti privati che rispondono ai requisiti tecnici e normativi stabiliti dalla Commissione Europea. Il fornitore ha l'onere di assicurare che l'infrastruttura del wallet sia conforme agli standard di sicurezza e interoperabilità previsti dal regolamento eIDAS, e che il servizio offerto sia robusto e affidabile per garantire la fiducia degli utenti.

Il Fornitore del Wallet ha un ruolo centrale nella protezione dei dati dell'utente, implementando le misure crittografiche e di sicurezza per prevenire accessi non autorizzati o abusi, inoltre, il fornitore deve garantire la continuità del servizio, minimizzando i tempi di inattività e migliorando costantemente le prestazioni del wallet, inclusa la protezione contro eventuali attacchi informatici.

PID Provider

Il PID Provider è l'entità responsabile di emettere e gestire i Person Identification Data (PID), ovvero gli identificatori personali degli utenti che sono utilizzati all'interno del wallet, questi identificatori possono includere dati biometrici, come impronte digitali o riconoscimento facciale, e altri attributi univoci che permettono di identificare l'utente in modo sicuro e conforme agli standard europei.
Il PID Provider collabora strettamente con il Fornitore del Wallet per garantire che gli identificatori siano emessi in modo sicuro e che possano essere verificati dalle Parti Affidabili durante le transazioni tramite protocolli sicuri come l'OpenID for Verifiable Credentials Issuance (OID4VCI) ("OpenID for Verifiable Credentials - Overview"), inoltre, l'intero processo di emissione e validazione degli identificatori deve rispettare ulteriori protocolli di privacy e sicurezza quali la ISO/IEC 18013-5 per le comunicazioni sicure in prossimità ("Architecture and Reference Framework") o la ISO/IEC 27001, ovvero lo standard internazionale per i sistemi di gestione della sicurezza delle informazioni (ISMS). ("IEC 27001:2022 - Information security management systems")
Il PID inizia il suo ciclo di vita quando viene emesso per un'Istanza del Portafoglio, in alcuni casi il PID può essere pre-configurato, il che significa che non è ancora valido al momento dell'emissione.
In questo caso, il suo stato è "Emesso" e passerà a "Valido" quando raggiungerà l'inizio del suo periodo di validità. Tuttavia, se il PID viene emesso alla data di inizio della validità o successivamente, il suo stato cambia direttamente a "Valido".



Ci sono due possibili transizioni per un PID valido: scade automaticamente con il passare della data di fine validità oppure viene attivamente revocato dal suo PID Provider.
Sia la scadenza che la revoca sono transizioni indipendenti, inoltre, una volta che un PID è scaduto o revocato, non può tornare ad essere valido.

Relying Party

Le Relying Parties (o parti fiduciarie) sono persone fisiche o giuridiche che si affidano a servizi di identificazione elettronica come quelli offerti dall'ecosistema di EUDI Wallet. In questo contesto, le parti fiduciarie richiedono gli attributi necessari contenuti nei dati di identificazione della persona (PID), nelle attestazioni elettroniche qualificate (QEAA) e negli altri attributi elettronici emessi dagli utenti, previa autorizzazione di questi ultimi e nel rispetto delle normative vigenti.
Le motivazioni per cui una parte fiduciarie può fare affidamento sul portafoglio EUDI includono obblighi legali, accordi contrattuali o scelte autonome, come avviene ad esempio nel settore finanziario, dove l'identificazione digitale è spesso richiesta per soddisfare normative di sicurezza.

Un aspetto fondamentale del processo è che le Relying Parties devono mantenere un'interfaccia con il portafoglio EUDI per richiedere attestazioni in modo sicuro e basato su autenticazione reciproca, in questo modo si garantisce che non solo l'utente sia verificato, ma che anche che la figura che richiede l'informazione sia autentica e affidabile.

Le Relying Parties devono inoltre notificare allo Stato membro in cui sono stabilite la loro intenzione di utilizzare il portafoglio EUDI e devono essere in grado di autenticare gli attributi (come PID e QEAA) ricevuti dagli utenti, tramite meccanismi di verifica certificati (Qualified Trust Service) ovvero servizi che garantiscono maggiore certezza legale e sicurezza nelle transazioni elettroniche rispetto ad un fornitore di servizi di fiducia generico, questi vengono forniti esclusivamente da fornitori certificati noti come Qualified Trust Service Providers (QTSP) i cui nomi appaiono in una lista sancita e costantemente aggiornata dall'Unione Europea nella quale vengono inseriti anche i servizi che il fornitore offre ("Digital Trust Services and QTSPs: what they are and why to choose them").

Esempi di parti fiduciarie includono banche, datori di lavoro, università o amministrazioni pubbliche che necessitano di verificare l'identità di un individuo o le sue credenziali, ad esempio un'istituzione scolastica potrebbe fare affidamento su un portafoglio EUDI per verificare i titoli accademici di uno studente in modo rapido e sicuro, evitando la necessità di lunghi processi burocratici e manuali e riducendo il rischio di falsificazione o frode, in questo modo entrambe le parti ne trarrebbero vantaggio.

Architettura di EUDI Wallet

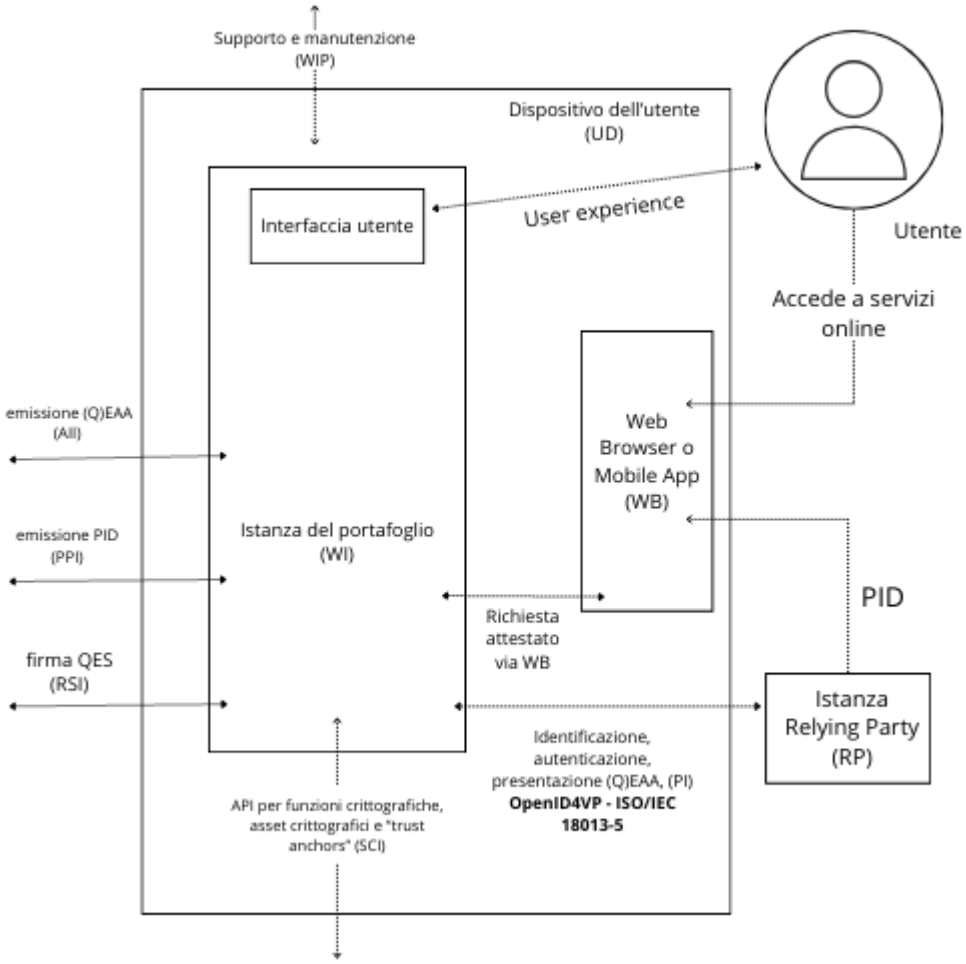
L'architettura del sistema EUDI Wallet si basa su una serie di principi di progettazione fondamentali, volti a tradurre il Regolamento sull'Identità Digitale Europea in un'infrastruttura tecnica sicura, intuitiva e orientata alla privacy.
Questi principi, elaborati nel rispetto delle normative europee e arricchiti dalle migliori pratiche del settore, costituiscono le linee guida essenziali per garantire che il sistema soddisfi le esigenze degli utenti e degli stakeholder coinvolti.

Tra i principi chiave dell'architettura, spiccano la centralità dell'utente, l'interoperabilità, la privacy e la sicurezza, l'approccio "user-centric" pone l'esperienza e il controllo dell'utente al centro del sistema, assicurando facilità d'uso e trasparenza nella gestione dei dati. L'interoperabilità, invece, garantisce un funzionamento uniforme e senza soluzione di continuità del wallet in tutta l'Unione Europea, favorendo l'accesso a servizi sia pubblici che privati in contesti transfrontalieri mentre per quanto riguarda il principio di "privacy by design", questo assicura la protezione dei dati personali degli utenti, minimizzando la raccolta di informazioni e offrendo un controllo puntuale su ciò che viene condiviso. Infine, il principio di "security by design" integra la sicurezza in ogni fase della progettazione, riducendo le vulnerabilità e proteggendo il sistema da potenziali attacchi.

Analizziamo quindi in dettaglio i componenti chiave dell'architettura del sistema EUDI Wallet, esplorando come questi principi siano tradotti in soluzioni tecniche che garantiscono un'adozione sicura e sostenibile a livello europeo.

Dispositivo dell’utente

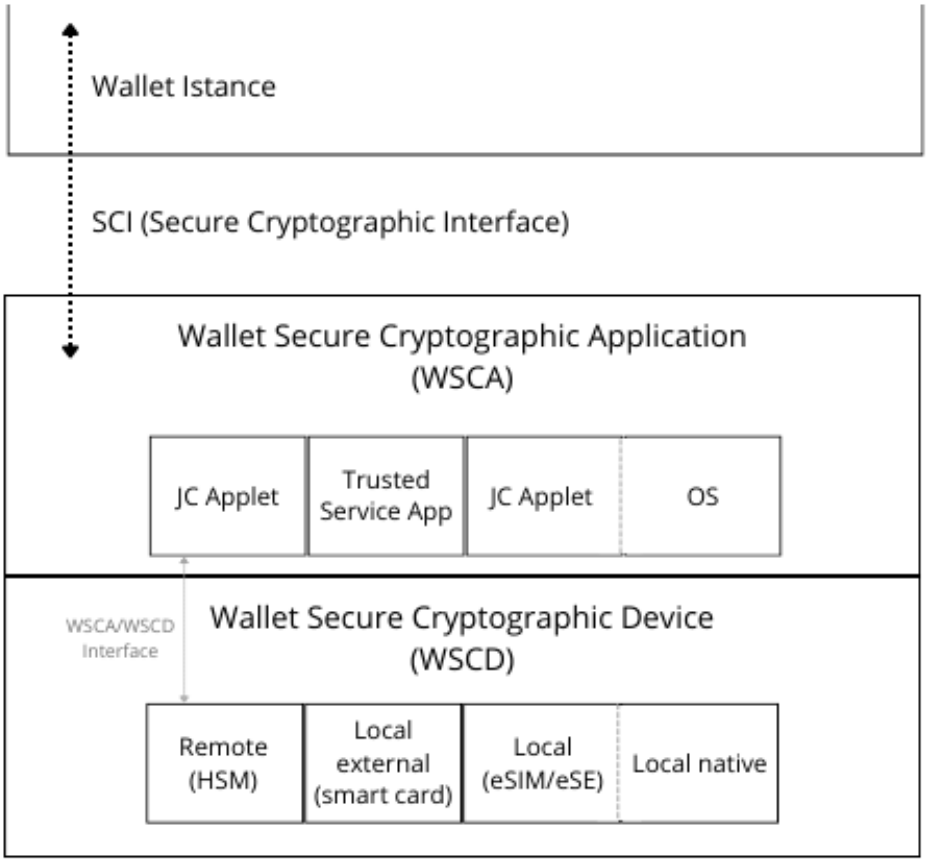
Al centro dell’architettura vi è il dispositivo dell’utente che ospita l’istanza del portafoglio.



Solitamente, per le istanze del portafoglio utilizzate da un utente fisico, il dispositivo utilizzato corrisponde ad un dispositivo mobile (es. smartphone) mentre per le figure giuridiche, il dispositivo utente potrebbe, ad esempio, essere un server cloud.
All’interno del dispositivo è installata l’istanza del portafoglio (WI), ovvero l’applicazione che fa parte del portafoglio EUDI Wallet impiegato, questo componente implementa la logica di business e le interfacce principali per poter comunicare con le altre parti dell’architettura.

WSCA e WSCD

È possibile definire il WSCD (Wallet Secure Cryptographic Device) come un componente fisico (hardware) affidabile che fornisce un ambiente sicuro ed uno spazio di archiviazione per asset crittografici (Token, Criptovalute, ecc.) per eseguire un'istanza del WSCA (Wallet Secure Cryptographic Application), ovvero un'applicazione sicura che gira sui dispositivi WSCD e che gestisce gli asset crittografici stessi per una determinata istanza del portafoglio, di conseguenza ogni WSCA è associata ad una WI di uno specifico utente. ("Is WSCD and WSCA described in European Digital Identity Wallet ARF equivalent to SSCD?")



In ARF identifica almeno quattro diversi WDSC che possono fornire lo stesso livello di sicurezza:

- WSCD Remoto, è situato in una zona fisicamente lontana dal dispositivo dell'utente.

- WSCD Locale Esterno, interagisce direttamente con il dispositivo dell'utente per fornire funzioni crittografiche.
- WSCD Locale Interno, integrato nel dispositivo dell'utente, include le seguenti soluzioni:
    - Per eSIM, il Wallet Provider fornisce una WSCA (es. Java Card Applet)
    - Per eSE, l'accesso al WSCD in questo caso è facilitato dal sistema operativo del dispositivo dell'utente, sono soluzioni mobile native come StrongBox, SecureEnclave.
- Ibridi, combinano uno o più WSCD menzionati precedentemente.

L'istanza del portafoglio interagisce direttamente con il WSCA e con il WSCD per gestire in modo sicuro le risorse crittografiche tramite la SCI (Secure Cryptographic Interface), questa interfaccia è stata sviluppata in parte seguendo le linee guida dell'ENISA (European Union Agency for Cybersecurity) ovvero l'agenzia europea incaricata di rafforzare la sicurezza informatica in Europa fornendo consulenza, supporto tecnico e linee guida sia alle istituzioni che nel settore privato. ("National Cybersecurity Strategies Guidelines & tools — ENISA")

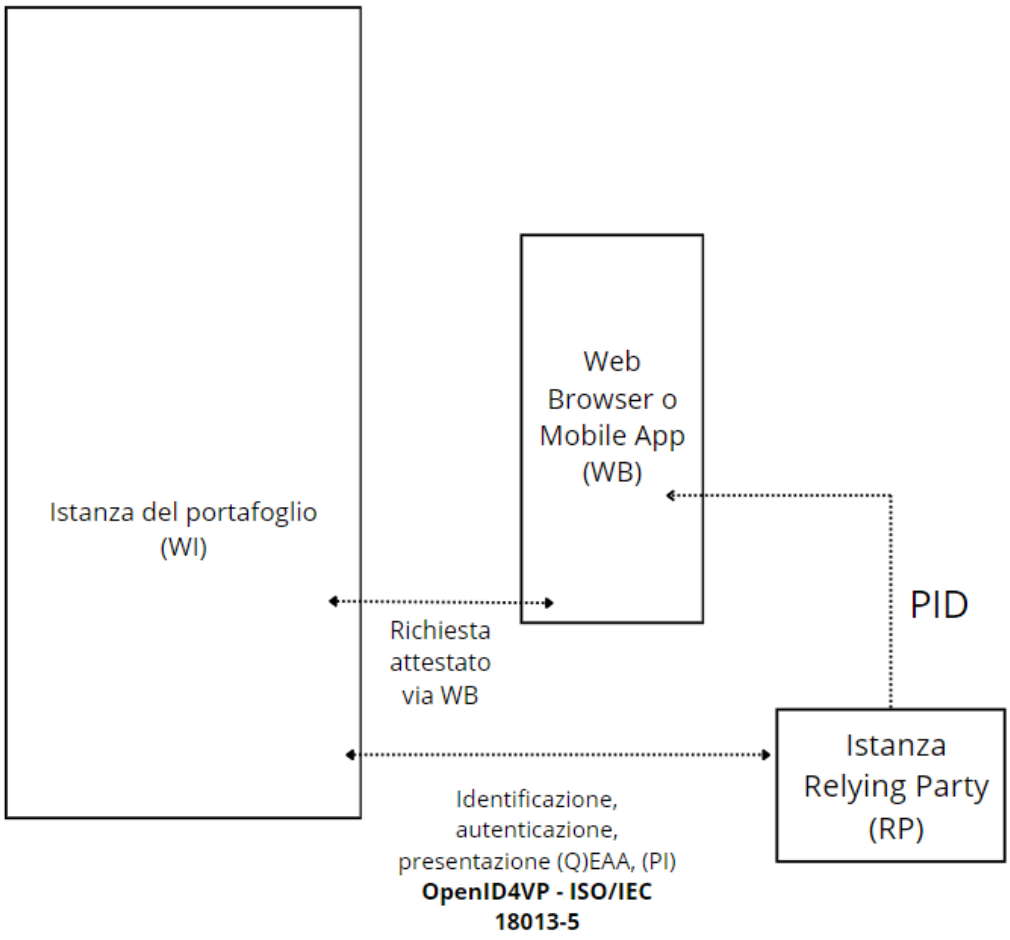
Per fare un esempio prendiamo un cittadino europeo che utilizza l'EUDI Wallet sul suo smartphone Apple per accedere ai servizi pubblici.
L'app del suo EUDI Wallet, che rappresenta la WSCA, è l'interfaccia attraverso cui gestisce la sua identità digitale e si autentica in modo sicuro.

Quando l'utente si autentica sul portale per accedere al servizio, l'app comunica con Secure Enclave, componente hardware che funge da WSCD integrato nel suo iPhone ("Secure Enclave - Supporto Apple (IT)"), questo genera una firma digitale sicura utilizzando le chiavi crittografiche dell'utente, che sono quindi protette all'interno del Secure Enclave evitando così che nessuna delle chiavi venga esposta durante il processo, garantendo la sicurezza dell'operazione.

Dopo aver usufruito del servizio, l'utente utilizza nuovamente l'app per firmare digitalmente il documento, anche in questo caso, il Secure Enclave si occupa di generare la firma in modo sicuro.

Istanza del Relying Party

Come detto precedentemente, le Relying Party o parti fiduciarie, sono delle figure che si affidano ad EUDI Wallet per per verificare l'identità di un utente o accedere a informazioni specifiche su di esso, di conseguenza non fanno propriamente parte dell'architettura, tuttavia è importante osservare il collegamento che intercorre tra l'istanza del portafoglio e l'istanza del Relying Party.



Esistono 4 diversi tipi di flussi possibili tra una Relying Party e un'istanza dell'EUDI Wallet :

- *Flusso di prossimità supervisionato*: l'utente del portafoglio EUDI è fisicamente vicino alla Relying Party quindi gli attestati vengono scambiati utilizzando la tecnologia di prossimità (ad esempio, NFC, Bluetooth) tra l'istanza del portafoglio e l'istanza della Relying Party.
  Durante il processo, un rappresentante umano della Relying Party supervisiona il processo.

- *Flusso di prossimità non supervisionato*: come il flusso supervisionato ma, in questo caso, l'istanza del portafoglio presenta attributi verificabili ad un dispositivo senza la supervisione umana.
- *Flusso remoto cross-device*: l'utente visualizza le informazioni del servizio su un dispositivo separato da quello che ospita l'istanza di EUDI Wallet, che viene utilizzato solo per proteggere la sessione (ad esempio, la scansione di un codice QR su una pagina di login e l'istanza del portafoglio viene usata solo per accedere ai servizi online).
- *Flusso remoto dallo stesso dispositivo*: il dispositivo utilizzato dall'utente per ospitare l'istanza di EUDI Wallet viene utilizzato durante tutta la durata del flusso per monitorare e proteggere l'intera sessione, scambiare informazioni ed infine usufruire del servizio.

In generale, una Relying Party richiede l'autenticazione da parte dell'utente e alcuni dei dati necessari per fornire un servizio, questo processo inizia all'interno di un browser web o di un'applicazione mobile.
In particolare, per quanto riguarda il flusso remoto con lo stesso dispositivo, il browser o l'app dell'utente reindirizza la richiesta al suo EUDI Wallet ogni volta che un fornitore di servizi necessita di autenticazione o di dati.
Al contrario, un flusso remoto cross-device ed entrambi i flussi di prossimità (supervisionati o non supervisionati), potrebbero iniziare attivando l'istanza del portafoglio attraverso NFC o scansionando un codice QR, in generale tramite gesti che non richiedono l'interazione con il browser web, è dunque fondamentale un'interazione sicura e semplificata con altre applicazioni, sia sul dispositivo dell'utente che all'esterno.

È necessario, inoltre, che le Relying Party siano in grado di richiedere ed inviare i vari PID e attestati quali QEAAs, PuB-EAAs e EAAs da EUDI Wallet, per questo è stata definita un'interfaccia di presentazione (PI), sia per le soluzioni remote che di prossimità.
Per i flussi di presentazione remota, come illustrato nella sezione seguente, l'istanza del portafoglio implementa il protocollo OpenID for Verifiable Presentation (OpenId4VP) mentre per il flusso di presentazione di prossimità, invece, aderisce allo standard ISO/IEC 18013-5.

Fornitori di PID, Attestati e Firme Elettroniche

L'articolo 45g del Regolamento (UE) 2024/1183 denota due punti:

1. I fornitori di attestati elettronici di attributi offrono agli utenti dei portafogli europei di identità digitale la possibilità di richiedere, ottenere, conservare e gestire l'attestato elettronico di attributi indipendentemente dallo Stato membro in cui è fornito il portafoglio europeo di identità digitale.

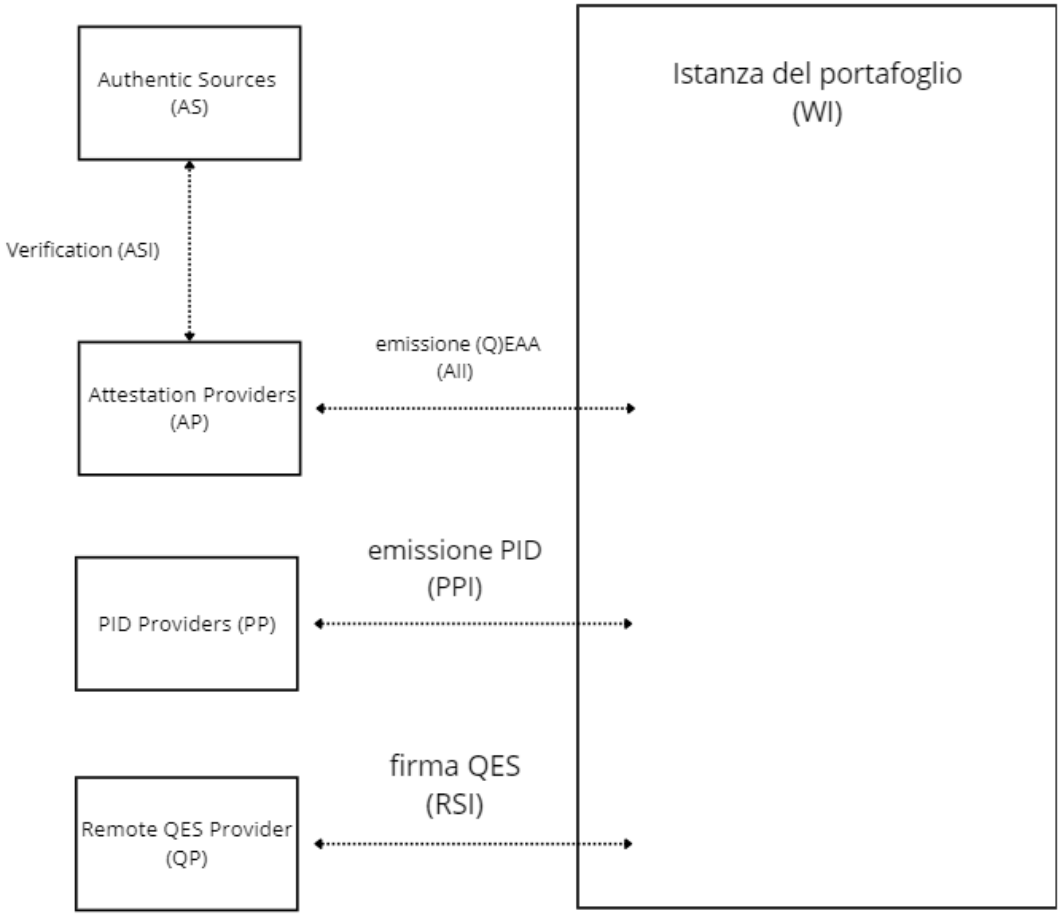
2. I fornitori di attestati elettronici qualificati di attributi forniscono un'interfaccia con i portafogli europei di identità digitale forniti conformemente all'articolo 5 bis (articolo nel quale vengono definiti i punti fondamentali per la definizione di un portafoglio europeo di identità digitale).

Inoltre, citando il punto 74 definito dello stesso documento:
"*Il presente regolamento stabilisce l'obbligo per i prestatori di servizi fiduciari qualificati di verificare l'identità di una persona fisica o giuridica cui è rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato sulla base di vari metodi armonizzati in tutta l'Unione.*
Per garantire che i certificati qualificati e gli attestati elettronici qualificati di attributi siano rilasciati alla persona cui appartengono e che attestino l'insieme corretto e unico di dati che rappresenta l'identità di tale persona, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati o attestati elettronici qualificati di attributi dovrebbero, al momento del rilascio di tali certificati e attestati, garantire con assoluta certezza l'identificazione di tale persona. Inoltre, oltre alla verifica obbligatoria dell'identità della persona, se applicabile per il rilascio di certificati qualificati e al momento del rilascio di un attestato elettronico di attributi qualificato, i prestatori di servizi fiduciari qualificati dovrebbero garantire con assoluta certezza la correttezza e l'accuratezza degli attributi della persona cui è rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato. Tali obblighi di risultato e di assoluta certezza nella verifica dei dati attestati dovrebbero essere sostenuti con mezzi adeguati, anche utilizzando un metodo o, se necessario, una combinazione di metodi specifici previsti dal presente regolamento."

Dovrebbe essere possibile combinare tali metodi per fornire una base adeguata ai fini della verifica dell'identità della persona cui è rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

Tale combinazione dovrebbe poter includere il ricorso a mezzi di identificazione elettronica che soddisfano i requisiti del livello di garanzia significativo in combinazione con altri mezzi di verifica dell'identità che consentirebbero di soddisfare i requisiti armonizzati di cui al presente regolamento per quanto riguarda il livello di garanzia elevato nell'ambito di ulteriori procedure armonizzate a distanza, garantendo l'identificazione con un elevato livello di affidabilità.

"Tali metodi dovrebbero includere la possibilità per il prestatore di servizi fiduciari qualificato che rilascia un attestato elettronico di attributi qualificato di verificare gli elementi da attestare mediante mezzi elettronici, su richiesta dell'utente, conformemente al diritto dell'Unione o nazionale, anche rispetto alle fonti autentiche." ("Regulation - EU - 2024/1183")



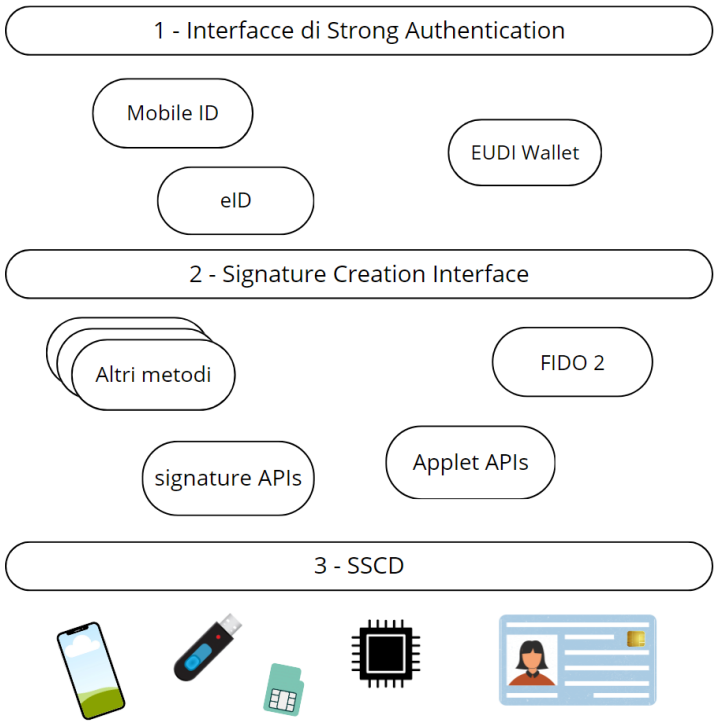
Quindi, una volta verificata l'autenticità degli attributi, bisogna gestire la trasmissione di questi all'istanza del portafoglio, per quanto riguarda i PID e gli attestati che un utente può voler includere nel suo portafoglio abbiamo due interfacce, rispettivamente PII(PID Issuance Interface) e AII(Attestation Issuance Interface), entrambe basate sul protocollo OpenID4VCI, mentre per le firme elettroniche qualificate verrà utilizzata un'interfaccia specifica (RSI) in quanto, come definito nella outline eIDAS del 2021("European Digital Identity Architecture and Reference Framework – Outline"), l'EUDI Wallet deve consentire all'utente di firmare

mediante firma elettronica qualificata o sigillo, questo obiettivo può essere raggiunto in due modi:

- il Portafoglio EUDI include un dispositivo di creazione di firma/sigillo qualificato (QSCD),
- si utilizza uno strumento di autenticazione sicura come parte di un QSCD locale o remoto gestito da un QTSP (Quality Trust Service Provider).

L'EUDI Wallet può anche consentire all'utente di firmare mediante firme o sigilli non qualificati.

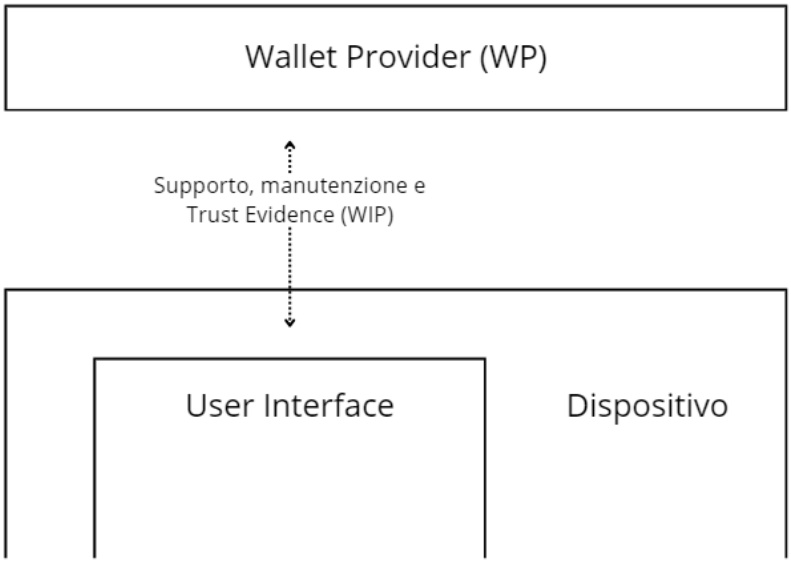
Per implementare queste funzionalità esistono esistono diverse interfacce in grado di integrare i vari dispositivi di creazione di firme ad EUDI Wallet, molti dei quali usano un framework comune a livello strutturale.



La figura qui sopra mostra i 3 livelli di struttura di Strong Authentication dei dispositivi di creazione delle firme, framework peraltro utilizzato anche per la creazione di sigilli elettronici (eSeals). Il primo livello è quello dell'interazione con l'utente e dell'integrazione dei servizi, che definisce le azioni che l'utente vede, il secondo livello è costituito dai meccanismi che il primo livello utilizza per accedere ai dispositivi sicuri mentre il terzo livello è costituito dai dispositivi per la creazione di firme sicure. ("Qualified Signature Creation Device for EUDI Wallet: Future of Strong Authentication")

Fornitori del portafoglio

Come per le altre componenti logiche dell'architettura, anche per i fornitori dei portafogli esiste un'interfaccia che permette all'istanza del portafoglio stesso di comunicare con i fornitori per ricevere manutenzione e assistenza per l'utente, ma soprattutto per la Wallet Trust Evidence (WTE) e la Wallet Instance Attestation (WIA).
La WTE corrisponde a tutte quelle prove che garantiscono che l'architettura del wallet soddisfi i requisiti tecnici e legali, mentre per quanto riguarda la WIA consiste nel garantire che quella particolare versione o implementazione del portafoglio digitale sia conforme agli standard di sicurezza, privacy e operatività stabiliti dalle normative eIDAS e dagli schemi di certificazione pertinenti.



Il regolamento eIDAS 2.0 impone che i wallet siano conformi a requisiti funzionali, di sicurezza e privacy tali da garantire alti livelli di affidabilità e interoperabilità tra i vari paesi membri, di conseguenza, il regolamento prevede l'uso degli schemi di certificazione del *Cybersecurity Act* (CSA), in modo da evitare approcci divergenti e uniformare l'implementazione dei requisiti di sicurezza informatica in tutta Europa. ("Regulation - 2019/881")
Gli Stati membri hanno il compito di designare degli organismi pubblici o privati di valutazione della conformità (CAB) che saranno quindi responsabili della valutazione e della certificazione delle soluzioni di identità digitale e verranno in seguito notificati alla Commissione Europea.

I provider dei portafogli devono selezionare e incaricare uno o più di questi organismi per ottenere il via libera per la propria soluzione, questa certificazione non si limita alla conformità ai requisiti del regolamento, ma include anche una valutazione della robustezza della sicurezza.
I requisiti vengono stabiliti da una serie di articoli del regolamento eIDAS:

- Art. 5a (23) - Atti di esecuzione sulle specifiche tecniche e operative e sulle norme di riferimento, per i requisiti citati all'articolo 5a;
- Art. 5 bis (14) - Separazione logica tra i dati relativi alla fornitura dell'EUDI Wallet e qualsiasi altro dato in possesso del fornitore dell'EUDI Wallet;
- Art. 5a (24) -- Ove applicabile, atto/i di esecuzione su specifiche, procedure e standard di riferimento, al fine di facilitare l'onboarding degli utenti all'EUDI Wallet mediante mezzi di identificazione elettronica conformi al livello di garanzia (LoA) “elevato” o mediante mezzi di identificazione elettronica conformi al LoA “sostanziale” in combinazione con ulteriori procedure di onboarding a distanza che insieme soddisfano i requisiti del LoA “elevato”.

Il processo di certificazione prevede anche un costante aggiornamento, con valutazioni delle vulnerabilità ogni due anni e la possibilità di revocare la certificazione se tali vulnerabilità non vengono risolte.

EUDI Wallet ed EBSI, una soluzione decentralizzata

L'EUDI Wallet, come abbiamo visto, rappresenta una svolta significativa nel modo in cui gestiamo la nostra identità digitale nell'era digitale. Ma come si articola questo nuovo strumento all'interno del più ampio ecosistema tecnologico? Per rispondere a questa domanda, è necessario addentrarsi nel cuore della tecnologia blockchain e di EBSI (European Blockchain Service Infrastructure).

La blockchain, con la sua caratteristica struttura distribuita e immutabile, offre un solido fondamento per la creazione di registri digitali affidabili e sicuri, si può immaginare la blockchain come un grande registro digitale, dove ogni transazione viene registrata in modo permanente e trasparente su migliaia di computer in tutto il mondo, questa caratteristica la rende ideale per gestire informazioni sensibili come le nostre identità digitali.

Entrando più nel dettaglio, EBSI si presenta come un'infrastruttura europea costruita appositamente per sfruttare il potenziale della blockchain, una rete di nodi interconnessi che fornisce un ambiente sicuro e standardizzato per lo sviluppo di una vasta gamma di servizi pubblici basati su blockchain.
Questa infrastruttura crea quindi un ponte tra le diverse amministrazioni pubbliche europee, facilitando lo scambio di informazioni e la creazione di servizi transfrontalieri.

Ma come si inserisce l'EUDI Wallet in questo quadro? L'idea è quella di utilizzare la tecnologia blockchain e l'infrastruttura EBSI per creare un portafoglio digitale sicuro e interoperabile, in grado di contenere tutte le nostre credenziali digitali, dai documenti d'identità ai certificati medici, passando per le qualifiche professionali. Grazie alla tecnologia blockchain, le informazioni contenute nell'EUDI Wallet saranno immutabili e verificabili da chiunque ne abbia diritto, garantendo un livello di sicurezza e affidabilità senza precedenti.

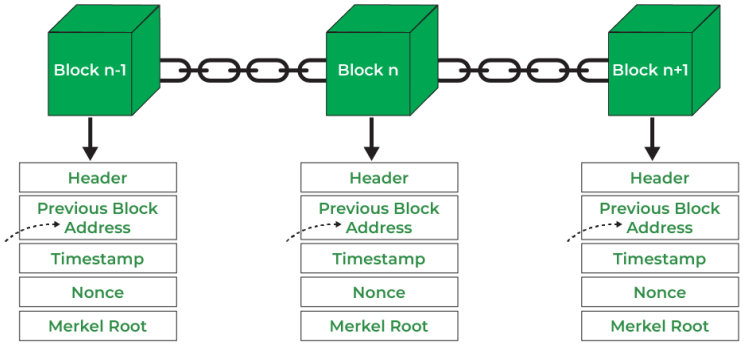
Inoltre, l'integrazione con l'EBSI permetterebbe all'EUDI Wallet di comunicare con altri sistemi e servizi pubblici, facilitando l'accesso a una vasta gamma di servizi online. Immagina di poter utilizzare il tuo EUDI Wallet per accedere ai servizi consolari, noleggiare un'auto, oppure partecipare a una votazione online, tutto senza dover presentare una miriade di documenti cartacei.

La tecnologia blockchain

Immagina un enorme libro contabile digitale, condiviso da milioni di persone in tutto il mondo, dove ogni transazione viene registrata in modo permanente e inviolabile. Questo libro contabile è la blockchain, una tecnologia rivoluzionaria che sta trasformando il modo in cui gestiamo i dati e le transazioni.

Per risalire alla nascita di questa tecnologia bisogna andare nel 2009, in particolare al 9 Gennaio di quell'anno, quando venne rilasciato ufficialmente il Bitcoin da parte di una persona sconosciuta il cui pseudonimo è Satoshi Nakamoto.
Il Bitcoin è una moneta digitale o criptovaluta le cui transazioni sono registrate in maniera decentralizzata e protette da algoritmi cifrati che rendono difficile la falsificazione o qualsiasi attività di hacking, la blockchain non è altro che il registro pubblico di tutte le transazioni di Bitcoin che sono state fatte negli anni. (Blockchain for Business).

A differenza dei tradizionali database centralizzati, controllati da un'unica autorità, la blockchain è distribuita su una rete di computer, nessuno dei quali ha il controllo esclusivo sul sistema. Ogni computer, o nodo, possiede una copia completa del libro contabile, e ogni nuova transazione viene verificata e aggiunta al registro da tutti i nodi della rete.
Pensa a questa rete come una catena indistruttibile, formata da blocchi collegati tra loro, ogni blocco contiene un insieme di transazioni e un riferimento crittografico al blocco precedente, questo porta a creare una sorta di timbro temporale digitale, che rende impossibile alterare i dati registrati in precedenza senza invalidare l'intera catena, come cercare di cambiare una pagina di un libro senza lasciare traccia, sarebbe praticamente impossibile.



Un blocco all'interno di una blockchain è composto da un'intestazione (block header) e da un corpo (block body), l'intestazione del blocco contiene vari elementi fondamentali:

- Versione del blocco: indica quale insieme di regole di validazione deve essere seguito.
- Radice di Merkle (Merkle tree root hash): rappresenta il valore hash di tutte le transazioni contenute nel blocco, permettendo una verifica efficiente della loro integrità.
- Timestamp: indica l'orario corrente in secondi a partire dal 1 gennaio 1970, secondo il tempo universale.
- nBits: rappresenta la soglia target per validare l'hash di un blocco.
- Nonce: è un campo di 4 byte, che solitamente parte da 0 e aumenta ad ogni calcolo dell'hash; questo parametro è centrale nel processo di "mining".
- Hash del blocco precedente: è un valore hash di 256 bit che punta al blocco precedente nella catena, garantendo il collegamento sequenziale dei blocchi.

Il corpo del blocco contiene un contatore di transazioni e le transazioni stesse. La quantità massima di transazioni in un blocco dipende dalla dimensione complessiva del blocco e dalla grandezza di ciascuna transazione.

In sostanza, ecco cosa succede ogni volta che si verifica una nuova transazione sulla blockchain:

1. Un record di quella transazione viene aggiunto al libro mastro di ogni computer connesso alla rete, con una firma crittografica immutabile (hash).
2. I nodi della blockchain eseguono il software necessario per convalidare, ricevere e trasmettere transazioni.
3. Visto che ogni blocco contiene informazioni sul blocco precedente, questi formano effettivamente una catena di blocchi (blockchain) con ogni blocco aggiuntivo che si collega a quelli precedenti.
4. Tutti i nodi aggiornano la propria versione del registro della blockchain in modo che rimanga identico.

Di conseguenza, le transazioni blockchain sono immutabili in quanto, una volta registrati, i dati in un determinato blocco non possono essere modificati retroattivamente senza alterare i blocchi successivi. (“An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”)

Infrastruttura EBSI

È un'iniziativa dell'European Blockchain Partnership (EBP), una collaborazione tra la Commissione Europea, tutti gli Stati membri dell'UE e alcuni paesi dello European Economic Area, nata nel 2018 con l'obiettivo di fornire servizi pubblici transfrontalieri a livello europeo con la tecnologia blockchain.
L'EBSI è la prima infrastruttura blockchain a livello UE guidata dal settore pubblico, tutti i nodi possono creare e trasmettere transazioni che aggiornano il registro, e ogni nodo conserva una copia identica di questo registro.

All'interno dell'EBSI, la Self-Sovereign Identity(SSI) si riferisce a un modello di identità decentralizzato, in cui gli utenti possono scegliere il proprio identificatore, il provider e wallet, le informazioni che desiderano rivelare agli verificatori e il metodo di verifica, potendo quindi gestire la propria identità digitale e interagire con la rete EBSI tramite wallet digitali. ("Where Is Current Research on Blockchain Technology?—A Systematic Review")

Abbiamo già visto cosa sono i wallet digitali ma per EBSI questo non basta, esistono infatti dei test di conformità per valutare se i portafogli soddisfano determinati standard di prestazioni e funzionalità, in particolare questo Conformance Test valuta la capacità del portafoglio di gestire le credenziali assegnate da un finto emittente e di restituirle a un finto verificatore, questi wallet vengono chiamati Conformant Wallet.

Esistono diversi tipi di portafogli "conformi" in base alle necessità dell'utente, è possibile dividerli in base a tre macro funzionalità e in base al tipo di ruolo è coperto dall'utilizzatore, infatti, come accennato all'inizio del documento, esistono tre tipi di figure quando si parla di identità digitale ovvero l'emittente, il detentore ed il verificatore (Issuer, Holder e Verifier):

- Portafogli per i detentori, possono richiedere l'emissione di Verifiable Credentials (VC) e riceverle istantaneamente o in differita.
- Portafogli per emittenti, questi portafogli consentono ad organizzazioni come università o ministeri di gestire le proprie certificazioni nella blockchain e di emettere le VC ai detentori.
- Portafoglio per i verificatori, questi portafogli consentono a organizzazioni come aziende o università di verificare l'autenticità di una VC presentata da un holder.

Prendiamo il caso dell'app di PosteItaliane, grazie a questa app è possibile verificare la propria identità per accedere a servizi statali ma anche richiedere determinate credenziali, tuttavia attualmente non fa più parte dei wallet conformi in quanto non ha rinnovato i test di conformità oppure non li ha superati.
Altri portafogli digitali, come iGrant.io Data Wallet o Walt.id Wallet, sono invece portafogli digitali conformi che vengono utilizzati dalle persone fisiche per avere dati e documenti a portata di mano in forma digitale e per condividerli in maniera facile e veloce, mantenendo comunque il pieno controllo degli stessi.

Per quanto riguarda i wallet per le organizzazioni, come un emittente o un verificatore, viene utilizzato per fornire credenziali digitali o altri servizi agli utenti, per esempio Enterprise Wallet di Validated ID.

Collegamenti tra EUDI Wallet ed EBSI

Con la prima versione del regolamento eIDAS, l'identità digitale veniva tipicamente rilasciata da un'autorità centralizzata, lasciando al concetto di Self-Sovereign Identity (SSI) una mancanza di fiducia dal punto di vista legale.
Le cose iniziarono a cambiare con lo sviluppo dell'eIDAS Bridge, una possibile soluzione tecnica e legale pensata dall'UE per collegare l'approccio centralizzato di , riferito all'eID governativa e ai servizi fiduciari, con l'approccio decentralizzato della DLT(Distributed Ledger Tecnology) ed eventualmente della SSI ("SSI eIDAS Bridge").

Il successo della DLT e degli sviluppi tecnologici come quello di EBSI in Europa, ma anche il limitato utilizzo dell'eID centralizzato, ha portato la Commissione UE a rivisitare il regolamento eIDAS, proponendo nel 2021 quello che oggi è in vigore come regolamentazione eIDAS 2.0, riconoscendo la decentralizzazione da un lato e il requisito della fiducia legale della SSI dall'altro. ("eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI")

Una delle prime applicazioni pratiche di EUDI Wallet sta attualmente venendo sviluppata da DC4EU, un progetto coordinato dalla Spagna con la partecipazione di 23 Stati membri e dell'Ucraina che coinvolge oltre 35 amministrazioni pubbliche e oltre 40 enti privati. ("DC4EU: Digital Credentials for Europe")
Il progetto testerà l'uso del portafoglio EUDI nel settore dell'istruzione e della sicurezza sociale, sarà in linea con la tessera europea di sicurezza sociale e con il modello di apprendimento europeo e utilizzerà l'infrastruttura europea dei servizi blockchain EBSI nel contesto del portafoglio EUDI.

Per realizzare questo pilotaggio su larga scala di EUDI Wallet sono stati fatti partire due progetti principali, il progetto sulle credenziali digitali nell'ambito dell'educazione guidato dal Ministero spagnolo degli Affari Economici e della Trasformazione Digitale ("Digital credentials in education") ed il progetto sulla previdenza sociale guidato da Dachverband der Sozialversicherungsträger ("The social security domain"), includendo le procedure di onboarding, l'identificazione dei requisiti di business, l'implementazione delle interfacce per gli emittenti di credenziali, il test completo dei processi di business dei sistemi di destinazione e la valutazione dei processi.

Applicazioni pratiche e progetti pilota

Per testare le reali potenzialità di EUDI Wallet è necessario provarlo su larga scala, con questo pretesto sono stati stipulati quattro progetti pilota su larga scala, (uno dei quali è DC4EU) con il compito di testare le specifiche del portafoglio in una vasta gamma di casi d'uso, prima dell'effettivo rilascio negli Stati Membri.

Nel 2022 il Programma Europa Digitale, un programma di finanziamento dell'UE incentrato sull'introduzione della tecnologia digitale nelle imprese, nei cittadini e nelle pubbliche amministrazioni, ha pubblicato un invito a lanciare i quattro progetti pilota su larga scala per il Portafoglio dell'identità digitale dell'UE, avviati poi nel 2023.

Potential Consortium for European Digital Identity

Con il supporto di 17 nazioni dell'Unione Europea e di più di 170 istituzioni pubbliche e private, Potential è un consorzio nato per definire una singola versione di identità digitale per i cittadini europei, avvalendosi di esperti e specialisti fondamentali per il raggiungimento dell'obiettivo di definire un'unica visione dell'identificazione online per i cittadini dei Paesi europei. ("Potential - For European Digital Identity")

Addentrandoci nello specifico, i casi d'uso presi in considerazione sono sei:

- Servizi eGov, un'identità digitale sicura che permetterà ai cittadini di autenticarsi in maniera rapida e sicura per accedere ai servizi governativi.
- Apertura di un conto bancario, grazie all'identità digitale sarà possibile aprire un conto bancario in maniera più rapida in ogni banca europea.
- Registrazione SIM, sarà possibile associare un cittadino verificato tramite la sua eID ad un numero di telefono.
- Patente digitale, permette di essere sempre a disposizione e garantisce l'autenticità del documento.

- Firma digitale qualificata, per firmare documenti e dichiarazioni in Europa garantendo l'autenticità della firma.
- Prescrizione digitale, alternativa digitale che permette di ordinare o ri-ordinare farmaci sotto ricetta medica in tutta Europa.

Per ogni Stato ed istituzione partecipante non vengono approfonditi tutti e sei i casi d'uso, per esempio in Italia, nello specifico la Provincia autonoma di Trento supportata dalla società in house Trentino Digitale S.p.A. insieme a Trentinosalute 4.0, contribuiranno allo sviluppo dell'infrastruttura del Wallet per garantire l'accesso ai servizi presenti sul catalogo provinciale e allo svolgimento dei test sull'utilizzo nazionale e transfrontaliero del portafoglio italiano nei tre ambiti a cui partecipa il consorzio italiano, ovvero servizi eGov, patente digitale e prescrizione digitale. ("Provincia autonoma di Trento - POTENTIAL")

Tra il 29 ed il 30 Aprile 2024 ad Atene è stato tenuto il secondo incontro generale di Potential, dove sono stati discussi i progressi ottenuti dalla nascita del progetto, avvenuta il 10 Luglio 2023 a Parigi.
In questo evento sono stati esposti i passi successivi da compiere, in particolare l'implementazione a livello nazionale del portafoglio digitale per gli Stati Membri che dovranno quindi identificare e fornire i propri stakeholders con gli strumenti e la conoscenza necessaria per poter svolgere il proprio ruolo in linea con i regolamenti europei.

Parallelamente, Potential fornirà agli Stati Membri delle liste di controllo complete, che valuteranno la preparazione di ciascun membro a soddisfare i requisiti di implementazione nazionali e a valutare la loro preparazione ad avviare i test di interoperabilità. ("Potential - Resources - Press release - Second BB")

EWC (EU Digital Identity Wallet Consortium)

EWC viene rappresentato da tutti e 27 Stati Membri dell'Unione Europea e da partner di altre nazioni con lo scopo di sviluppare delle Digital Travel Credentials, ovvero delle credenziali digitali utili per viaggiare all'interno dell'Unione Europea, permettendo ai cittadini di accedere a biglietti, credenziali di pagamento e documenti di volo e di identità, agevolando sia l'identificazione del cittadino che la sua esperienza all'estero.

Il prodotto derivante da questo progetto, che dovrebbe vedere la luce a Marzo 2025, sarà frutto di uno sviluppo coordinato tra cinque macro aree di lavoro (WP):

- Il WP1 riguarda la gestione e la comunicazione del progetto ed è capitanato da Bolagsverket e msg.
- Il WP2, preso in consegna da SICPA e GenDigital, riguarda l'applicazione delle credenziali di viaggio digitali lungo l'intero percorso dell'utente, l'integrazione del pagamento e l'onboarding delle parti fidate, nonché l'acquisizione del feedback degli utenti e degli ostacoli alla scalabilità.
- Il WP3 è sviluppato dal centro di ricerca dell'Università di Piraeus (Grecia) e riguarda l'integrazione del portafoglio di riferimento e lo sviluppo delle credenziali PID e ODI, vengono inoltre sviluppati anche gli scenari di test B2B necessari per testare ulteriormente la combinazione PID/ODI.
- Il WP4 copre l'infrastruttura strategica necessaria agli altri WP tecnici ed è gestito da Signicat ed Intesi, in questo pacchetto di lavoro vengono approfonditi l'interoperabilità, i test tecnici generali, la firma e l'autenticazione digitale e molti altri aspetti.
- Il WP5, a capo del quale troviamo msg in collaborazione con il Ministero della Finanza Finlandese, è dedicato alla diffusione dei risultati del progetto e alla comunicazione con progetti ed enti esterni. ("EWC Outputs")

L'ultimo aggiornamento risale al 11 e 12 Aprile 2024, giorni in cui è stata tenuta l'assemblea generale ad Amsterdam, qui sono stati discussi i progressi ottenuti ed i piani futuri per il progetto, le prime implementazioni dell'EUDI Wallet hanno fornito esempi concreti di come un portafoglio di identità digitale possa essere utilizzato per i casi d'uso relativi a viaggi,

organizzazioni e pagamenti, questi casi d'uso hanno messo in evidenza non solo le capacità tecniche, ma anche il design incentrato sull'utente del portafoglio, assicurando che esso soddisfi le diverse esigenze dei cittadini e delle organizzazioni europee. (“Lubkowitz”)

NOBID Consortium

Il Consorzio NOBIS, con 6 Stati partecipanti e circa venticinque partner, è il progetto con il minor numero di collaboratori dei quattro progetti pilota.
In principio nato con il nome di Nordic-Baltic eID Project (NOBID), questo progetto nasce in Nord Europa per facilitare l'uso di soluzioni eID nazionali oltre i confini della regione e per consentire ai cittadini di accedere ai servizi digitali.
È stato avviato dal Consiglio dei ministri nordici e successivamente esteso ad altri Paesi europei e partner rilevanti, come banche e fornitori di attributi, per creare un consorzio per l'EU Digital Identity che si focalizzasse sul tema dei pagamenti. (“NOBID Consortium”)

Il caso d'uso principale di questo consorzio si basa sull'infrastruttura esistente utilizzata per i pagamenti bancari, compresi i pagamenti istantanei SCT e i tradizionali trasferimenti da conto a conto, l’obiettivo è trovare una soluzione che si baserà sulle caratteristiche del portafoglio per garantire una sicura autenticazione del cliente e delle transazioni che soddisfino i requisiti della PSD2, ovvero la Direttiva UE 2015/2366 del Parlamento europeo relativa ai servizi di pagamento nel mercato interno (“2015/2366 - EN - EUR”).

Questo consorzio è composto da alcuni degli esperti di identità più avanzati e affidabili d'Europa, il cui sforzo si concentra in particolare sul caso d'uso dei pagamenti transfrontalieri. Il progetto gode di un sostegno senza pari da parte dei leader del settore bancario e dei pagamenti, tra cui DSGV in Germania, DNB e BankID in Norvegia, Nets in Danimarca, Intesa Sanpaolo, PagoPA e ABILab in Italia e Greiðsluveitan in Islanda ma sono presenti anche Poste Italiane, Intesi Group, InfoCert, FBK e il Centro Radiotelevisivo di Stato lettone. Una delle aziende fondamentali è sicuramente iProov, grazie alla sua tecnologia brevettata di

verifica e autenticazione biometrica del volto, iProov viene utilizzata dalle organizzazioni di tutto il mondo per confermare che un utente online è la persona giusta, una persona reale, e che si sta autenticando in questo momento.

Conclusioni

Possiamo riassumere il tutto sottolineando come l'EUDI Wallet rappresenti un passo avanti significativo verso una gestione moderna e integrata dell'identità digitale a livello europeo, con un impatto che può davvero trasformare il rapporto tra cittadini, istituzioni e aziende, rispondendo non solo all'esigenza di un sistema sicuro e trasparente, ma puntando a migliorare concretamente il modo in cui i cittadini possono accedere e condividere i propri dati personali e professionali all'interno dell'Unione.

I progetti pilota avviati stanno evidenziando come l'EUDI Wallet potrebbe facilitare numerosi aspetti della nostra vita quotidiana, dalla verifica dell'identità all'accesso a servizi sanitari, dalla gestione di documenti ufficiali alle interazioni con enti pubblici e privati, garantendo sicurezza, semplicità e rispetto delle normative europee.

Un aspetto particolarmente importante è l'integrazione della tecnologia Blockchain tramite l'infrastruttura EBSI (European Blockchain Services Infrastructure), che offre vantaggi concreti in termini di tracciabilità, sicurezza e immutabilità dei dati.
Questa tecnologia potrebbe rafforzare la fiducia dei cittadini e la struttura del progetto, migliorando la trasparenza e riducendo i rischi di manomissione dei dati.

Mi piace immaginare un futuro in cui, grazie a soluzioni come questa, ogni cittadino possa esercitare un controllo consapevole sui propri dati, diventando protagonista di un sistema digitale basato su fiducia e collaborazione tra i Paesi membri nel quale EUDI Wallet è il primo pilastro fondamentale, portandoci verso un'Unione ancora più interconnessa, sicura e all'altezza delle sfide di una società sempre più digitalizzata.

Bibliografia

- "Architecture and Reference Framework." *EUDI Wallet*, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework.
- Arun, Jai Singh, et al. *Blockchain for Business: Discover how Blockchain Networks are Transforming Companies, Driving Growth, and Creating New Business Models*. Addison-Wesley, 2019.
- Commissione Europea, 2021. "Programma di lavoro della Commissione per il 2021." *European Commission*, 2021, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A52020DC0690&from=DA.
- "Conformant wallets - EBSI." *European Commission*, https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Conformant+wallets.
- "DC4EU: Digital Credentials for Europe." *DC4EU: Digital Credentials for Europe*, https://www.dc4eu.eu/.
- "Digital credentials in education." *Digital credentials in education*, https://www.dc4eu.eu/wp5/.
- "Digital Trust Services and QTSPs: what they are and why to choose them." *Intesa*, 15 July 2024, https://www.intesa.it/en/digital-trust-services-and-qtsps-what-they-are-and-why-to-choose-them/#%E2%80%8BWhat_are_the_Qualified_Trust_Services?
- "eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI." *GI Digital Library*, https://dl.gi.de/items/c1f6f318-990d-4ef5-9d0f-fb6cebe09308.
- "eIDAS Regulation | Shaping Europe's digital future." *Shaping Europe's digital future*, 4 April 2024, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.
- "European Digital Identity Architecture and Reference Framework – Outline." *Shaping Europe's digital future*, 22 February 2022, https://digital-

strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline.

- "European Digital Identity - European Commission." *European Commission*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en#benefits-of-the-european-digital-identity.
- "European Digital Identity Wallet: rischi e benefici." *Intesa*, 11 January 2023, https://www.intesa.it/european-digital-identity-wallet-rischi-e-benefici/.
- "EWC Outputs." *EUDI Wallet Consortium*, https://eudiwalletconsortium.org/project/outputs/.
- "IEC 27001:2022 - Information security management systems." *ISO*, https://www.iso.org/standard/27001.
- "Is WSCD and WSCA described in European Digital Identity Wallet (EUDIW) ARF equivalent to SSCD?" *Methics*, 11 July 2024, https://www.methics.fi/is-wscd-and-wsca-equivalent-to-sscd/.
- Lubkowitz, Mark. "EU Digital Identity Wallet Consortium Holds Successful General Assembly in Amsterdam." *EUDI Wallet Consortium*, 16 April 2024, https://eudiwalletconsortium.org/2024/04/16/eu-digital-identity-wallet-consortium-holds-successful-general-assembly-in-amsterdam/.
- "National Cybersecurity Strategies Guidelines & tools — ENISA." *ENISA*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools.
- "NOBID Consortium." *Welcome to the NOBID Consortium*, https://www.nobidconsortium.com/.
- "OpenID for Verifiable Credentials - Overview." *OpenID*, https://openid.net/sg/openid4vc/.

- “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” *2017 IEEE International Congress on Big Data*, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379&isnumber=8029291.
- “Potential - For European Digital Identity.” *Potential - For European Digital Identity (digital-identity-wallet.eu)*, https://www.digital-identity-wallet.eu/.
- “Potential - Resources - Press release - Second BB.” *Potential - Resources - Press release - Second BB*, https://www.digital-identity-wallet.eu/resources.
- “Proposal amending Regulation (EU) No 910/2014.” *Proposal-2021*, 3 6 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN.
- “Provincia autonoma di Trento - POTENTIAL.” *Provincia autonoma di Trento - POTENTIAL*, https://www.provincia.tn.it/Documenti-e-dati/Progetti/POTENTIAL.
- “Qualified Signature Creation Device for EUDI Wallet: Future of Strong Authentication.” *Methics*, 27 June 2022, https://www.methics.fi/qscd-for-eudi-wallet-app/.
- “Regulation - 2019/881.” *EUR-Lex*, 7 June 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881.
- “Regulation - EU - 2024/1183.” *REGULATION (EU) 2024/1183*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183.
- “Secure Enclave - Supporto Apple (IT).” *Apple Support*, https://support.apple.com/it-it/guide/security/sec59b0b31ff/web.
- Simone, Tommaso. “The Digital Wallet paradigm for identity.” 2023, https://www.politesi.polimi.it/retrieve/caee647d-e039-4d89-a82a-f4c877bca009/2023_05_Simone.pdf.
- “The social security domain.” *DC4EU*, https://www.dc4eu.eu/project/wp6/.

- “SPID.” *Cos’è SPID*, https://www.spid.gov.it/cos-e-spid/.
- “SSI eIDAS Bridge.” *SSI eIDAS Bridge*, https://interoperable-europe.ec.europa.eu/collection/ssi-eidas-bridge.
- Tenhunen, Susanna. “Revision of the eIDAS Regulation.” *European Parliament*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf.
- “2015/2366 - EN - EUR.” *EUR-Lex*, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32015L2366.
- “Where Is Current Research on Blockchain Technology?—A Systematic Review.” *PLOS*, 3 October 2016, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477#pone.0163477.ref001.
- Windley, Phillip J. “The Inevitable Rise of Self-Sovereign Identity.” *Sovrin*, 29 September 2016, https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.