Link.it

# IT WALLET

## Introduzione e Contesto

L'IT-Wallet è il portafoglio digitale nazionale previsto dal DL 19/2024, finalizzato a permettere ai cittadini di accedere e utilizzare documenti digitali ufficiali tramite un ecosistema di Wallet provider, garantendo requisiti di sicurezza e interoperabilità. Il sistema introduce un nuovo paradigma di fruizione delle attestazioni digitali, orientato alla riduzione degli oneri documentali e alla standardizzazione dei meccanismi di verifica e presentazione.

### Il quadro europeo (EUDI Wallet)

Il contesto normativo europeo di riferimento è rappresentato dall'EUDI Wallet, che mira a garantire un'identità digitale interoperabile tra Stati membri e a superare la frammentazione tecnologica attraverso un framework comune. In tale quadro, la disponibilità di strumenti standard per emissione e presentazione delle attestazioni costituisce un prerequisito per l'adozione uniforme di servizi digitali transfrontalieri, con un impianto che valorizza controllo dell'utente e verificabilità delle informazioni.

### Perché l'Italia ha sviluppato l'IT-Wallet

L'adozione dell'IT-Wallet risponde alle limitazioni dei modelli tradizionali basati su sola autenticazione e abilita l'uso di attestazioni digitali in scenari che richiedono presentazione e verifica di attributi (es. certificati anagrafici, titoli di studio, abilitazioni professionali). L'obiettivo è estendere l'identità digitale verso un modello basato su credenziali e attributi verificabili, rafforzando l'abilitazione di servizi cross-border e la visione "Once Only", secondo cui il cittadino non deve essere chiamato a fornire più volte informazioni e documenti già detenuti e certificati dalle Pubbliche Amministrazioni, favorendone il riuso controllato nei procedimenti autorizzati, e l'evoluzione verso una gestione più strutturata e controllata degli attestati digitali del cittadino.

### Gli attori principali dell'ecosistema

L'ecosistema è composto da attori con ruoli distinti: Wallet Provider, Credential Issuer, Fonti Autentiche e Relying Party/Verifier. Le Pubbliche Amministrazioni operano come Fonti Autentiche; IPZS opera come Credential Issuer/Fornitore di Attestati Elettronici; PDND svolge il ruolo di trust e interoperabilità per l'esposizione e lo scambio controllato di e-service; AppIO rappresenta uno dei canali istituzionali di interazione con il cittadino.
In questo assetto, GovWay si colloca come componente abilitante per la conformità tecnica e la semplificazione operativa nell'ecosistema IT Wallet.
In particolare, può supportare le Pubbliche Amministrazioni nel ruolo di Fonti Autentiche, gestendo aspetti di compliance (voucher PDND, DPoP, firma, digest, tracciamenti) necessari all'esposizione sicura e conforme degli e-service. Allo stesso tempo, GovWay può essere adottato anche dagli altri attori dell'ecosistema che espongono o fruiscono e-

service tramite PDND, fornendo un layer di interoperabilità, sicurezza e governance coerente con i pattern e le linee guida nazionali.

## Struttura dell'IT-Wallet

Il Wallet Provider è l'applicazione che risiede sul dispositivo dell'utente e costituisce il punto di presidio locale per la gestione delle credenziali. Esso governa chiavi crittografiche e meccanismi di sicurezza locali, memorizza le credenziali in modo protetto e supporta i protocolli europei EUDI per la presentazione delle attestazioni. Ne deriva un modello in cui le credenziali non sono semplici "documenti digitali", ma artefatti verificabili gestiti secondo policy crittografiche e di sicurezza coerenti con il framework.

### Il Credential Issuer

Il Credential Issuer costruisce e firma la credenziale digitale a partire da dati ottenuti dalle Fonti Autentiche. Nel perimetro nazionale l' IPZS come soggetto incaricato dell'emissione e firma degli Attestati Elettronici, con garanzia di validità legale. Il ruolo dell'Issuer è quindi quello di garantire integrità e affidabilità dell'attestazione, assicurando che la credenziale prodotta risulti verificabile e coerente con i requisiti tecnici e normativi del sistema.

### Le Verifiable Credentials (VC)

Le Verifiable Credentials rappresentano il formato logico e funzionale con cui vengono espresse le attestazioni digitali: dati strutturati, firmati e verificabili, destinati a essere presentati dall'utente verso un soggetto verificatore (Verifier/Relying Party). L'adozione delle VC consente di disaccoppiare presentazione e verifica dalla mera autenticazione, abilitando un modello in cui attributi e documenti sono verificati secondo standard tecnici condivisi e con vincoli di integrità.

### La Fonte Autentica

La Fonte Autentica è l'ente titolare di basi dati ufficiali e di attributi certificati. Nel sistema IT-Wallet, la Fonte Autentica è responsabile di rendere disponibili attributi e informazioni in forma interoperabile e conforme alle specifiche. La presentazione in interoperabilità e la pubblicazione dei servizi avvengono secondo logiche di adesione e conformità alla PDND e ai registri previsti dal sistema, con responsabilità operative e di presidio del dato.

## L'infrastruttura di Trust

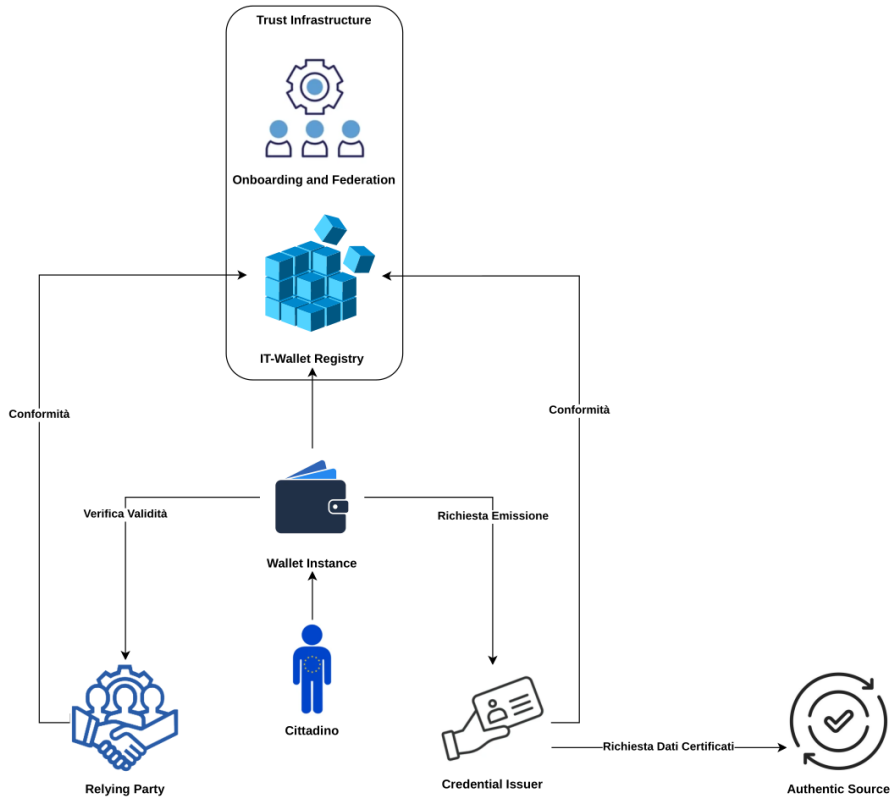
L'infrastruttura di Trust ha la funzione di mantenere l'affidabilità complessiva dell'ecosistema, garantendo che attori e scambi siano riconoscibili, autorizzati e verificabili. In ambito nazionale, la PDND viene qualificata nel documento come piattaforma di interoperabilità che espone e-service e implementa meccanismi di autenticazione, autorizzazioni e scambio dati tra gli attori coinvolti.

Questo strato assicura che l'accesso alle informazioni e l'interazione tra componenti avvengano tramite canali controllati e con evidenze di sicurezza adeguate.

## L'infrastruttura di Registro

L'infrastruttura di Registro fornisce un riferimento strutturato per l'identificazione e la consultazione degli elementi del sistema (attori, servizi, schemi e metadati necessari). Essa abilita discovery e consultazione coerente dei servizi e delle informazioni disponibili, riducendo ambiguità semantiche e tecniche e favorendo la federazione dei soggetti aderenti attraverso un impianto di metadati e regole condivise.

Nel suo complesso, l'IT-Wallet abilita un flusso in cui un cittadino custodisce attestazioni digitali nel Wallet, le presenta a un Verifier/Relying Party e ottiene una verifica basata su credenziali emesse da Issuer qualificati e fondate su dati di Fonti Autentiche. L'insieme di trust e registri consente di mantenere coerenza, verificabilità e governance su tutta la filiera, riducendo integrazioni "one-off" e favorendo standardizzazione.

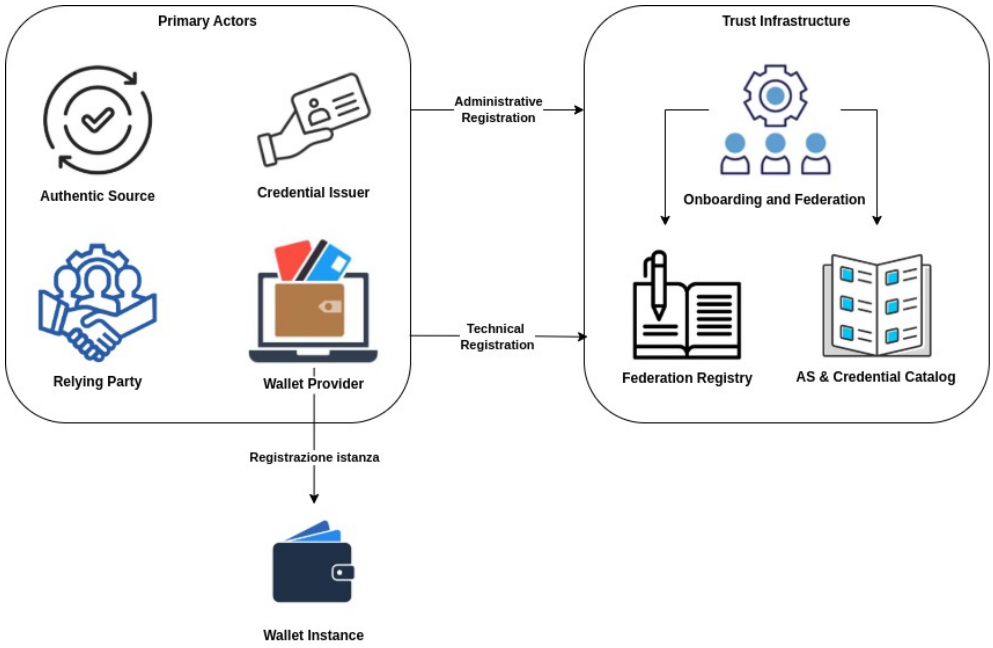


## L'infrastruttura di Trust

L'infrastruttura di Trust abilita la creazione e la gestione di relazioni fiduciarie tra l' entità del sistema, assicurando che le interazioni avvengano tramite canali sicuri e secondo policy comuni. Le funzioni tipiche includono la gestione di meccanismi di autenticazione e autorizzazione tra attori, la verifica dell'identità tecnica delle controparti e la disponibilità di informazioni necessarie a validare comportamenti e scambi nel ciclo di vita delle credenziali.

L'infrastruttura di Trust è essenziale perché il portafoglio digitale non è un semplice "contenitore" di dati: la sua efficacia dipende dalla possibilità di verificare che una credenziale sia stata emessa da un soggetto legittimato e che i flussi di scambio dati abbiano rispettato requisiti di sicurezza e autorizzazione. In assenza di tale strato, il sistema ricadrebbe su pratiche frammentate e su integrazioni non uniformi, con aumento del rischio operativo e riduzione dell'interoperabilità.

La visione d'insieme del Trust layer è quella di un'infrastruttura che, integrandosi con la PDND e con i registri, permette alle componenti di riconoscersi, scambiare dati e produrre evidenze verificabili. Questo garantisce coerenza e affidabilità del sistema, soprattutto in presenza di molteplici Fonti Autentiche e di un numero elevato di soggetti verificatori.




## L'infrastruttura di Registro

L'infrastruttura di Registro è l'insieme dei registri e dei metadati necessari a rendere operativa l'architettura federata, consentendo di identificare chi fa cosa, quali dati sono disponibili e con quali schemi e modalità tecniche siano rappresentati. Essa rende

consultabili gli elementi "di configurazione" del sistema, indispensabili per emissione, presentazione e verifica delle credenziali.

I registri comprendono tipicamente repertori di attori e capability, di schemi e metadati, e di elementi necessari alla discovery dei servizi. L'adozione di registri distinti consente di isolare responsabilità (es. anagrafica attori, catalogo credenziali, schemi dati, tassonomia) e di governare in modo consistente l'evoluzione del sistema, riducendo disallineamenti tra implementazioni e facilitando controlli di conformità.

L'infrastruttura di Registro serve a supportare l'operatività quotidiana: onboarding, configurazione, discovery e validazione. Rappresenta inoltre un presidio di governance, perché consente di determinare con precisione quali Fonti Autentiche espongono quali attributi e con quali specifiche, garantendo che l'ecosistema rimanga interoperabile anche al crescere del numero di attori.

**Taxonomy**

La tassonomia è l'elemento che abilita un linguaggio comune per classificare credenziali, attributi e domini applicativi. La sua presenza è cruciale per la scalabilità dell'ecosistema: permette di evitare definizioni locali non armonizzate, abilita ricerca e categorizzazione e supporta le logiche di riuso, sia a livello nazionale che in prospettiva europea.

## Le Fonti Autentiche

Le Fonti Autentiche sono Pubbliche Amministrazioni titolari di banche dati ufficiali contenenti attributi certificati relativi a persone fisiche o giuridiche. Nel contesto IT-Wallet, esse costituiscono il fondamento informativo su cui poggiano emissione, aggiornamento e revoca delle attestazioni digitali, in quanto responsabili della qualità e dell'autorevolezza del dato.

La Fonte Autentica fornisce attributi e informazioni necessari all'emissione delle credenziali digitali e, in generale, a tutte le verifiche che richiedono dati certificati. La disponibilità deve essere garantita in coerenza con le specifiche tecniche e con le regole di interoperabilità, incluse le modalità di accesso controllato e la corretta descrizione dei dati resi disponibili.

**Come una Fonte Autentica viene registrata**

Gli obblighi delle Fonti Autentiche includono: registrazione e onboarding (iscrizione al Registro delle Fonti Autentiche e riconoscimento istituzionale), adesione alla PDND con pubblicazione degli e-service, rispetto dei requisiti tecnici di interoperabilità; gestione degli attestati elettronici (emissione, aggiornamento, revoca), nonché logging e conservazione per garantire tracciabilità e conformità alle disposizioni sulla protezione dei dati personali.

**Interazione Fonte Autentica – Credential Issuer**

Il flusso tra Fonte Autentica e Credential Issuer si basa sull'accesso controllato agli attributi e sulla produzione di evidenze utili all'emissione della credenziale. L'Issuer interroga i servizi della Fonte Autentica per ottenere informazioni aggiornate e coerenti con le specifiche; la Fonte Autentica, a sua volta, garantisce correttezza del dato, disponibilità e conformità del canale di esposizione.

In sintesi, la Fonte Autentica è l'elemento che "certifica" il contenuto informativo sottostante alle credenziali: ne garantisce autorevolezza, presidia il ciclo di vita dei dati e assicura l'interoperabilità tramite PDND, catalogazione e tassonomia. L'ecosistema IT-Wallet richiede che tale ruolo sia formalizzato e sostenuto da requisiti tecnici e di audit adeguati.

## I Formati delle Credenziali Digitali

I formati delle credenziali digitali rispondono a esigenze differenziate di utilizzo e verifica: scenari con vincoli di performance, requisiti di sicurezza elevati, modalità di presentazione differenti (online/offline) e necessità di interoperabilità con sistemi eterogenei. La coesistenza di formati permette di massimizzare copertura funzionale e compatibilità, mantenendo tuttavia l'esigenza di un governo centralizzato di schemi, regole e policy tecniche.

Il **formato SD-JWT / VC JSON** è orientato a una rappresentazione strutturata e gestibile nei contesti applicativi tipici (servizi digitali e integrazioni API). Tale formato permette una gestione pratica degli attributi e si integra efficacemente con architetture REST e gateway, fermo restando il rispetto dei requisiti di firma, validazione e verifica previsti nel framework.

Il **formato mDoc (ISO 18013-5)** risponde a scenari di presentazione documentale con requisiti particolarmente stringenti, tipicamente in ambito mobile e con modalità di verifica che possono includere contesti "document-like". L'adozione di questo formato richiede coerenza con schemi e specifiche tecniche, nonché disponibilità di componenti in grado di gestire correttamente strutture e verifiche previste dallo standard.

Il confronto tra i formati serve a determinare la scelta più adatta in funzione del caso d'uso, dei canali di presentazione e dei requisiti di interoperabilità. A livello sistemico, tale pluralità rafforza la necessità di Registry e Taxonomy per assicurare che ogni credenziale sia descritta, classificata e verificabile in modo uniforme, indipendentemente dal formato.

## Ruolo GovWay per la Fonte Autentica

**GovWay: supporto alla conformità e alla semplificazione per le Fonti Autentiche**

Nel documento di riferimento, GovWay è descritto come strumento di supporto fondamentale per consentire alle Fonti Autentiche di integrarsi con la Federazione e con la PDND in maniera semplificata e conforme. In particolare, GovWay gestisce interazioni in interoperabilità con la PDND, garantendo uso corretto dei token di interoperabilità e dei meccanismi di sicurezza, e supporta logging e tracciabilità strutturata delle interazioni tra attori.

**1. Trasformazione delle risposte della Fonte Autentica in JWT**

GovWay si posiziona come componente che consente di "industrializzare" la produzione delle risposte conformi (es. JWT) a partire da payload applicativi della Fonte Autentica, riducendo la complessità implementativa sui sistemi sorgente e centralizzando i controlli tecnici (firma, digest, tracciamenti). Questo approccio è funzionale a ridurre errori di implementazione e ad aumentare la ripetibilità dei flussi.

**2. Gestione Signal Hub: negoziazione token e pubblicazione semplificata**

Il documento evidenzia che GovWay semplifica la gestione dei requisiti del Signal Hub, gestendo autonomamente la negoziazione dei token di interoperabilità necessari alla pubblicazione dei segnali e fornendo un'interfaccia di pubblicazione semplificata, sollevando la Fonte Autentica dalla gestione diretta del numero seriale incrementale richiesto per ciascun segnale.

**3. Pattern di sicurezza, integrity e audit**

GovWay supporta i pattern di sicurezza previsti per l'interoperabilità tramite PDND, gestendo meccanismi di proof of possession, firma e digest dei messaggi, nonché i pattern di integrity richiesti per garantire l'autenticità e l'immodificabilità delle comunicazioni machine-to-machine.

La piattaforma assicura inoltre funzionalità di audit, logging e tracciabilità, con registrazione strutturata delle richieste e delle risposte scambiate tra gli attori, a supporto delle garanzie a valore legale.

Questo insieme di capacità consente alle amministrazioni e agli altri soggetti aderenti di operare in coerenza con le linee guida nazionali, fornendo evidenze tecniche a prova di controlli a supporto di ciascun dominio amministrativo istituzionale.