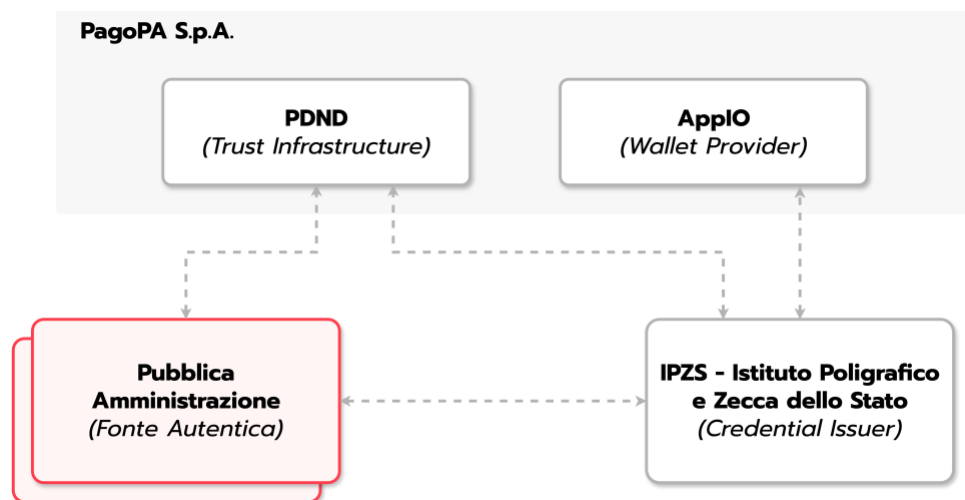


IT Wallet

Contesto di riferimento

Introduzione

L'IT-Wallet è il portafoglio digitale nazionale, previsto dal DL 19/2024, che permette ai cittadini di accedere e usare documenti digitali ufficiali tramite l'AppIO, garantendo sicurezza e interoperabilità. È un progetto del Dipartimento per la Trasformazione Digitale, realizzato con PagoPA e l'Istituto Poligrafico e Zecca dello Stato (IPZS).



Attori coinvolti nel sistema IT-Wallet

- **Pubbliche Amministrazioni (Fonti Autentiche):** enti titolari di banche dati contenenti attributi relativi a persone fisiche o giuridiche, utilizzati nel contesto dell'IT Wallet per l'emissione delle credenziali digitali;
- **IPZS – Istituto Poligrafico e Zecca dello Stato (Credential Issuer):** soggetto incaricato come Fornitore di Attestati Elettronici, emette e firma gli Attestati Elettronici garantendone la validità legale;
- **PDND (Trust Infrastructure):** piattaforma di interoperabilità espone gli e-service ed implementa i meccanismi di autenticazione, autorizzazioni e scambio di dati tra i vari attori coinvolti;
- **AppIO (Wallet Provider):** canale ufficiale per l'interazione con il cittadino/ utenti finali con l'ecosistema IT-Wallet.

Il ruolo delle Fonti Autentiche

Le Fonti Autentiche (FA) sono Pubbliche Amministrazioni che detengono banche dati ufficiali e attributi certificati di cittadini o imprese. Nel contesto IT-Wallet, presentano alcuni obblighi, tra cui:

- **Registrazione e onboarding:** iscrizione al Registro delle Fonti Autentiche, con superamento della verifica di riconoscimento istituzionale come ente titolare di dati

autentici, l'adesione alla PDND e la rispettiva pubblicazione di e-service, e il rispetto dei requisiti tecnici necessari a garantire l'interoperabilità;

- **Gestione degli attestati elettronici:** ogni Fonte Autentica è responsabile dell'emissione, aggiornamento e revoca degli attestati elettronici relativi agli attributi di sua competenza, garantendone l'integrità e la disponibilità nel rispetto delle specifiche tecniche;
- **Interoperabilità e sicurezza:** gli scambi informativi devono avvenire tramite interfacce standard e protocolli sicuri, in linea con gli standard di sicurezza condivisi;
- **Partecipazione al Catalogo PDND:** le Fonti Autentiche devono esporre i propri e-service nel Catalogo PDND e garantire l'accesso controllato agli enti autorizzati, descrivendo i dati e gli attributi disponibili secondo la tassonomia nazionale;
- **Logging e conservazione:** devono assicurare la tracciabilità delle operazioni di emissione, verifica e revoca degli attestati, rispettando le politiche di conservazione dei log previste e le disposizioni sulla protezione dei dati personali.

Il ruolo di GovWay

Nello scenario IT-Wallet, le Fonti Autentiche assumono un ruolo centrale nella federazione dei servizi, dovendo pubblicare e rendere accessibili gli attributi in modo conforme ai requisiti tecnici, di sicurezza e di audit definiti dalla piattaforma. GovWay rappresenta uno strumento di supporto fondamentale in questo contesto, consentendo alle Fonti Autentiche di integrarsi con la Federazione e con la PDND in maniera semplificata e conforme:

- **Gestisce le interazioni in interoperabilità con la PDND**, garantendo l'uso corretto dei token di interoperabilità e dei meccanismi di sicurezza richiesti [ID_AUTH_CHANNEL_01];
- **Semplifica la gestione dei requisiti del Signal Hub**, in particolare:
 - Gestisce autonomamente la **negoiazione con i token di interoperabilità** necessari per la pubblicazione dei segnali
 - Fornisce un'interfaccia di pubblicazione semplificata, sollevando la Fonte Autentica dalla gestione diretta del **numero seriale incrementale** richiesto per ciascun segnale
- **Gestisce i nuovi pattern di sicurezza DPoP** (Demonstration of Proof of Possession), richiesti per i flussi basati su OpenID4VCI e OpenID4VP, garantendo l'autenticazione delle richieste in modo conforme alle specifiche del framework IT-Wallet [REST_JWS_2021_POP];
- **Supporta i pattern di Integrity e Audit**, assicurando la tracciabilità e la verificabilità delle transazioni, come previsto dalle linee guida e dai requisiti di sicurezza e audit del sistema [INTEGRITY_REST_02; AUDIT_REST_02];
- **Supporta il logging e la tracciabilità delle interazioni**, consentendo la registrazione strutturata delle richieste e delle risposte tra gli attori del sistema.