

Indelli Api gateway

Specifiche Tecniche del Gateway d'Interoperabilità: "Modello di Interoperabilità (ModI) / PDND Nativo in PHP" **Architettura Lightweight Zero-Dependency vs Enterprise API Gateways (WSO2 / GovWay)**

1. Introduzione e Contesto Architettuale

Il presente documento analizza l'architettura tecnica del sistema di interoperabilità basato sulle specifiche del Modello di Interoperabilità (ModI) AgID e dell'infrastruttura PDND (Piattaforma Digitale Nazionale Dati). La soluzione implementa un gateway client-server nativo in PHP, privo di framework pesanti o dipendenze esterne complesse, progettato per garantire la massima efficienza, sicurezza crittografica e conformità normativa.

2. Analisi dei Componenti del Sistema

2.1 Client Federato (Multi-Ente)

Il client gestisce l'interrogazione incrociata e federata verso molteplici endpoint (es. INPS, Agenzia delle Entrate, ANPR). Le sue caratteristiche principali includono:

- - Generazione dinamica dei Voucher JWT (simulazione PDND) firmati con algoritmo RS256 e buffer temporale (clock skew mitigation).
- - Firma JWS compact dei payload di business (dati dell'interrogazione) utilizzando la chiave privata asimmetrica del client.
- - Trasmissione sicura via cURL con intestazioni HTTP personalizzate (es. X- Authorization e application/jose) per aggirare eventuali restrizioni dei web server intermedi.
- - Generazione automatica di report testuali e tracciamento strutturato (Audit Trail live).

2.2 Server Erogatore (ModI ID_AUTH_REST_01)

L'endpoint server agisce da guardiano rigoroso dell'interoperabilità, applicando un hardening di livello Enterprise:

- - Sicurezza dei Transport e Headers HTTP: Iniezione rigida di direttive restrittive (nosniff, DENY, no-store, no-cache).
- - Validazione Crittografica RS256: Verifica rigorosa sia del Voucher PDND (tramite chiave pubblica dell'Ente centrale) sia della firma JWS del client.
- - Controllo Claims e Timing Attacks: Validazione di exp, nbf, iat, aud e iss utilizzando funzioni a tempo costante (hash_equals) per prevenire attacchi di tipo timing.
- - Query Sicure e Opacità degli Errori: Utilizzo di PDO con timeout rigidi e gestione di risposte opache verso l'esterno per evitare il leak di informazioni architetturali.

3. Vantaggi Competitivi rispetto ai Gateway Enterprise (WSO2 / GovWay)

I sistemi tradizionali di Enterprise Service Bus (ESB) e API Gateway come WSO2 API Manager o GovWay sono progettati per ecosistemi mastodontici, ma presentano criticità notevoli per Enti di medie/piccole dimensioni o per micro-servizi agili. La soluzione nativa PHP presenta vantaggi netti in termini di:

Dimensione di Confronto	Gateway Tradizionali (WSO2 / GovWay)	Soluzione Nativa PHP (Modi Lightweight)
Footprint di Risorse & RAM	Richiedono stack complessi (JVM/Tomcat o database dedicati), consumando gigabyte di RAM anche a riposo.	Pochissimi megabytes. Gira perfettamente su qualsiasi VPS standard con overhead quasi nullo.
Complessità di Setup e Manutenzione	Curva di apprendimento ripidissima. Richiedono competenze specialistiche su XML, ESB, console di gestione elefantache.	Zero dipendenze esterne. Il codice è interamente auditabile in pochi file PHP nativi.
Performance e Latenza (Throughput)	Overhead di elaborazione elevato dovuto a pipeline di mediazione complesse e XML parsing estensivo.	Latenza vicina allo zero puro. Esecuzione diretta via PHP-FPM con validazione OpenSSL nativa.
Aggiornamenti e Patching (CVE)	Aggiornamenti frequenti e complessi di interi framework enterprise, con rischi elevati di rottura delle dipendenze.	Manutenzione banale e immediata. Controllo totale e diretto del codice sorgente (Licenza Apache 2.0).
Lock-in Tecnologico	Forte dipendenza da ecosistemi proprietari o configurazioni XML/JSON proprietarie molto rigide.	Piena aderenza agli standard aperti (JWT, JWS, RS256) senza vincoli di piattaforma.

4. Sicurezza e Conformità alle Linee Guida AgID

Nonostante la leggerezza implementativa, il sistema soddisfa pienamente i requisiti di sicurezza prescritti dalle specifiche tecniche ModI e PDND:

- - Autenticazione Forte basata su chiavi asimmetriche (RSA 2048/4096 bit).
- - Tracciabilità e Non-Ripudiabilità grazie ai codici di tracciamento univoci e ai log strutturati in formato JSON.
- - Protezione attiva contro attacchi di Replay, Man-in-the-Middle e Path Traversal.