Il Progetto CART

Interoperabilità e Cooperazione Applicativa in Regione Toscana

Obiettivi del Progetto

- Il CART è l'infrastruttura di RT dedicata a regolare le comunicazioni applicative sia con soggetti esterni che tra soggetti interni
- Obiettivi principali:
  - mettere in sicurezza l'accesso ai servizi
  - censire i servizi e le loro modalità di utilizzo
  - assicurare il rispetto dei requisiti applicativi e normativi
  - certificare i flussi in maniera indipendente dai vari interlocutori
  - mettere a disposizione funzionalità infrastrutturali di utilità comune per le applicazioni
  - uniformare le modalità di integrazione con gli applicativi, in maniera trasparente rispetto alle modalità di interscambio utilizzate con l'esterno

Alcuni numeri del CART

- Una media di circa 30 milioni di transazioni settimanali
- Oltre un miliardo di transazioni annue
- Alcuni dati di una settimana classica del CART:
  - Pda v2 (ePrescription): 7 milioni di transazioni
  - Pda-v3 (gestione busta98): 1 milione di transazioni
  - Pdd Center: 15 milioni di transazioni
  - PdA Arpa: 35.000 sessioni utente, con 1.500 utenti diversi, 500.000 transazioni complessive
- A questo si aggiungono i nuovi servizi dell'emergenza covid19:
  - Circa 5 milioni di messaggi settimanali per smistamento tamponi, vaccinazioni, referti-covid, comunicazioni ministeriali

Interoperabilità in RT: il contesto normativo di riferimento

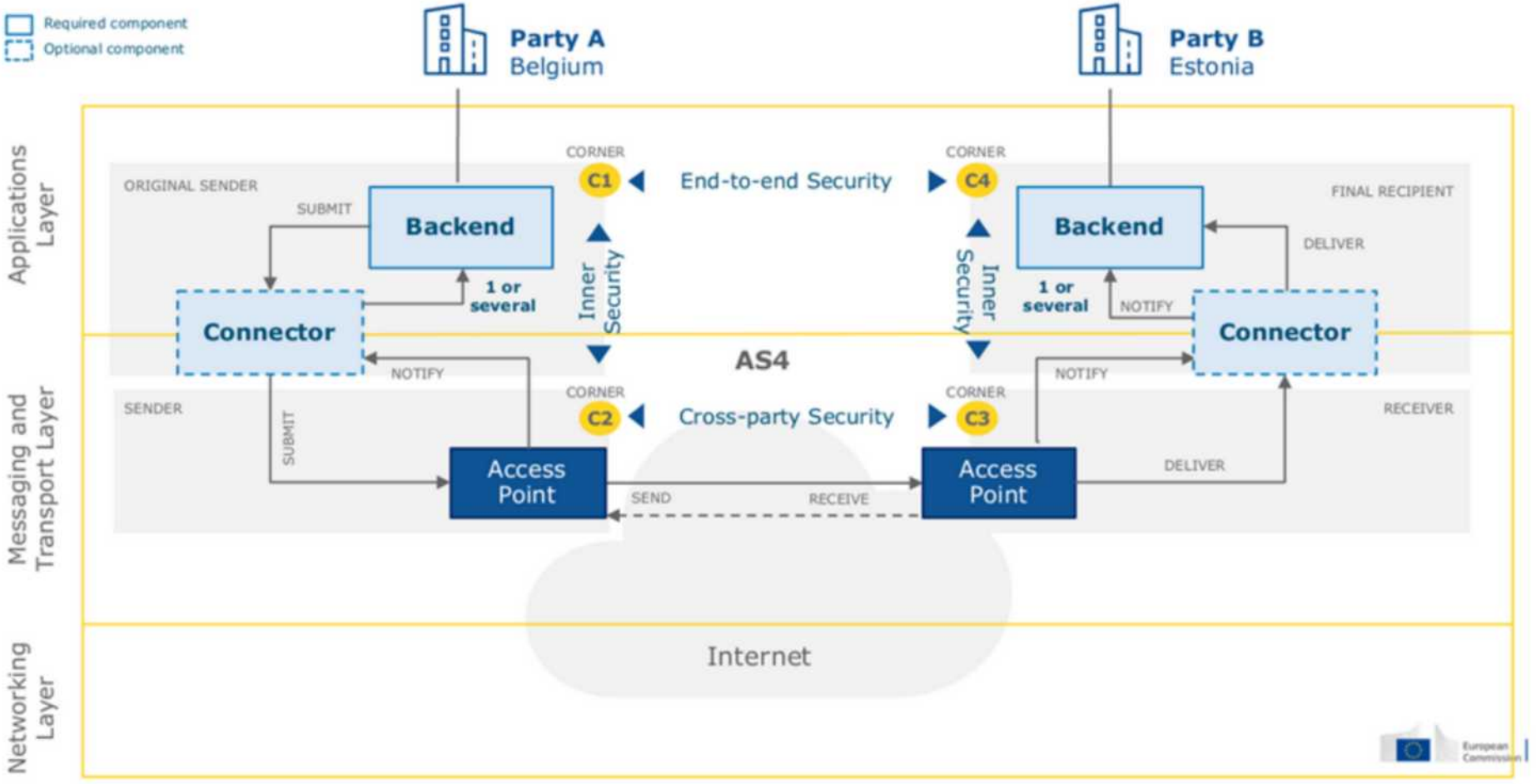
- Livello Europeo:
  - EIDAS → ERDS → eDelivery (AS4)
- Livello Italiano:
  - SPCoop
  - ModI
- Gli Standard Internazionali:
  - OpenAPI 3
  - OAuth2
  - OIDC
- Gli standard regionali:
  - ARPA, ecompliance, busta 98


AGID
Agenzia per l'Italia digitale
Cerca nel Portale Trasparenz
Agenzia
Piattaforme
Infrastrutture
Sicurezza
Dati
Design servizi
Linee guida
Home › Amministrazione trasparente › Provvedimenti › lettura Provvedimenti Amministrativi
Provvedimenti
Riferimenti normativi
Provvedimenti
Provvedimenti organi indirizzo politico
Provvedimenti dirigenti amministrativi
Determinazione n. 406/2020 del 9 settembre 2020 - Adozione della Circolare recante le linea di indirizzo sulla interoperabilità tecnica.
Tipologia: provvedimento organo indirizzo-politico
Provvedimento numero: 406/2020
Struttura responsabile: Direzione Pubblica amministrazione e vigilanza
Responsabile del provvedimento: Paorici Francesco
Data del provvedimento: 09-09-2020
Allegati
Allegato: DT DG n. 406 -9 sett 2020- Circolare 1-2020 Linea di indirizzo interoperabilità tecnica.pdf (15/09/2020 - 3825 kb - pdf)
Allegato: Circolare 1-2020 Linea di indirizzo interoperabilità tecnica.pdf

Le nuove Linee Guida – i contenuti

- Raccomandazioni tecniche sulla realizzazione delle interfacce SOAP e REST
  - Formato Dati
  - Progettazione e Naming delle Interfacce di Servizio
  - Robustezza (Rate Limiting)
  - Gestione Allegati
- Profilo di sicurezza di canale (identificazione delle organizzazioni)
  - Uso di https per l'autenticazione delle parti interagenti
- Profilo di sicurezza di messaggio (identificazione delle Unità Organizzative o Organizzazioni)
  - Integrità e non ripudio tramite firma del payload e degli header rilevanti
  - Per SOAP viene proposto l'uso di WS-Security e WS-Addressing
  - Per REST viene proposto l'uso di token JWS scambiati in appositi header HTTP

Security zones of a 4-Corner



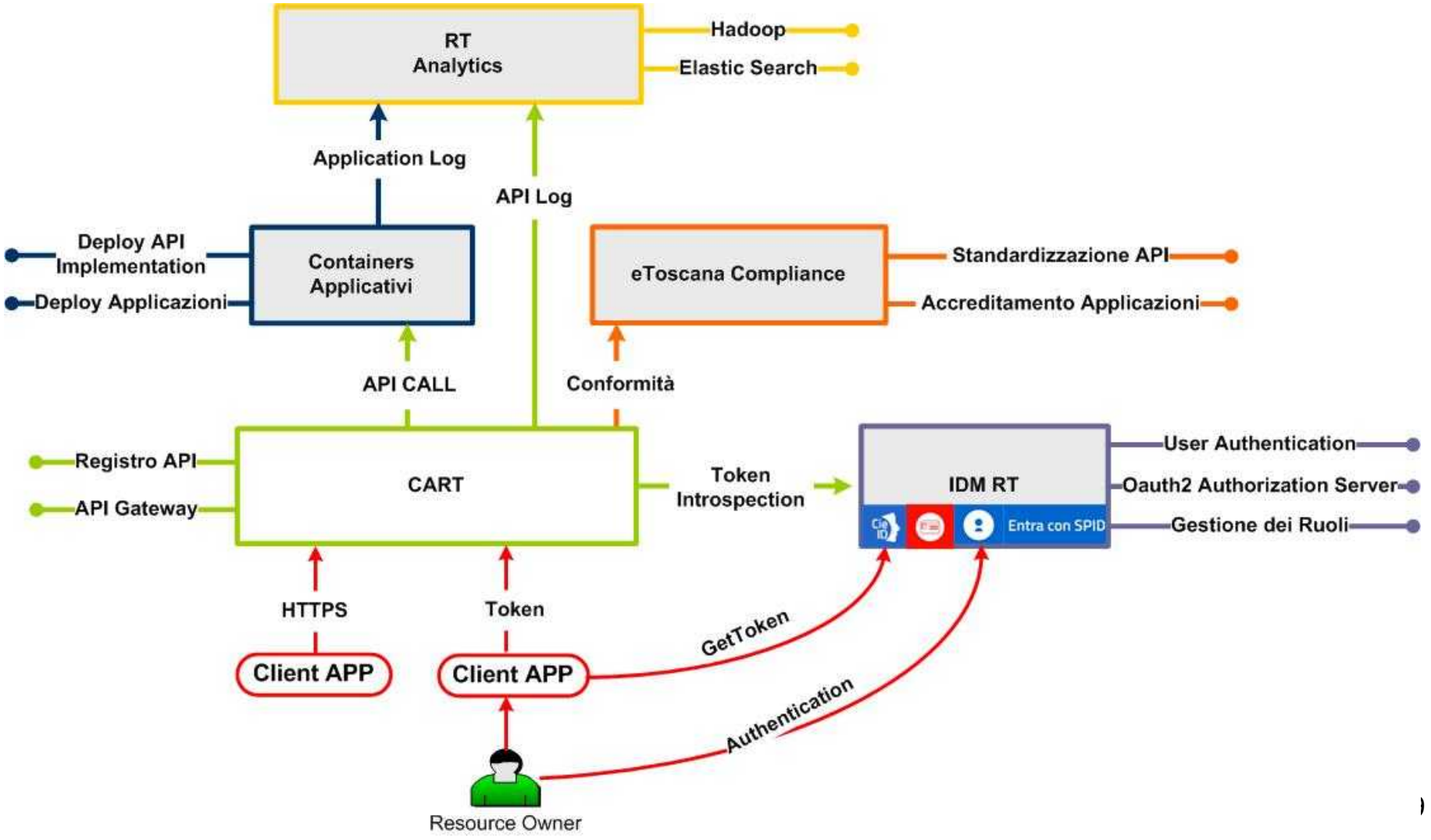
I profili di Interoperabilità in ModI

Pattern/Funzioni	HTTPS	Autenticazione Soggetto Mittente	Autenticazione Applicativo Fruitore	Certificazione Data Richiesta	Autorizzazione accesso API	Unicità della Richiesta	Integrità del Messaggio	Non Ripudio	Non Ripudio della Ricezione
ID_AUTH_CHANNEL_01	✓								
ID_AUTH_CHANNEL_02	✓	✓							
ID_AUTH_REST/ SOAP_01			✓	✓	✓				
ID_AUTH_REST/ SOAP_02			✓	✓	✓	✓			
INTEGRITY_REST/ SOAP_01			✓	✓	✓	✓	✓		
Archivio Messaggi								✓	
Gestione Prova Ricezione									✓
Input richiesto...		Certificato X509 Soggetto	Certificato X509 Applicativo		Identificativo API (Audience)				

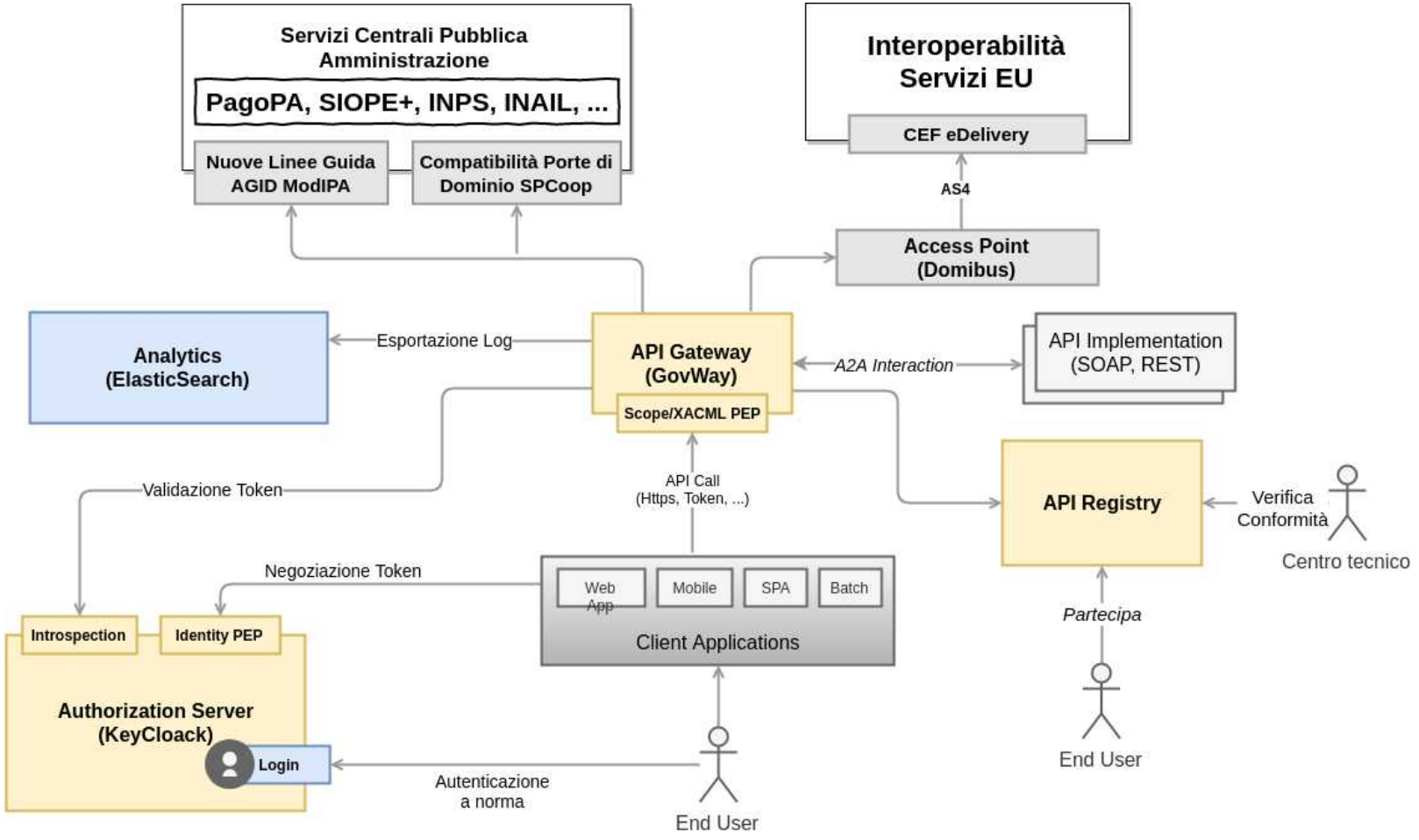
ModI: Pattern e Profili di Interoperabilità

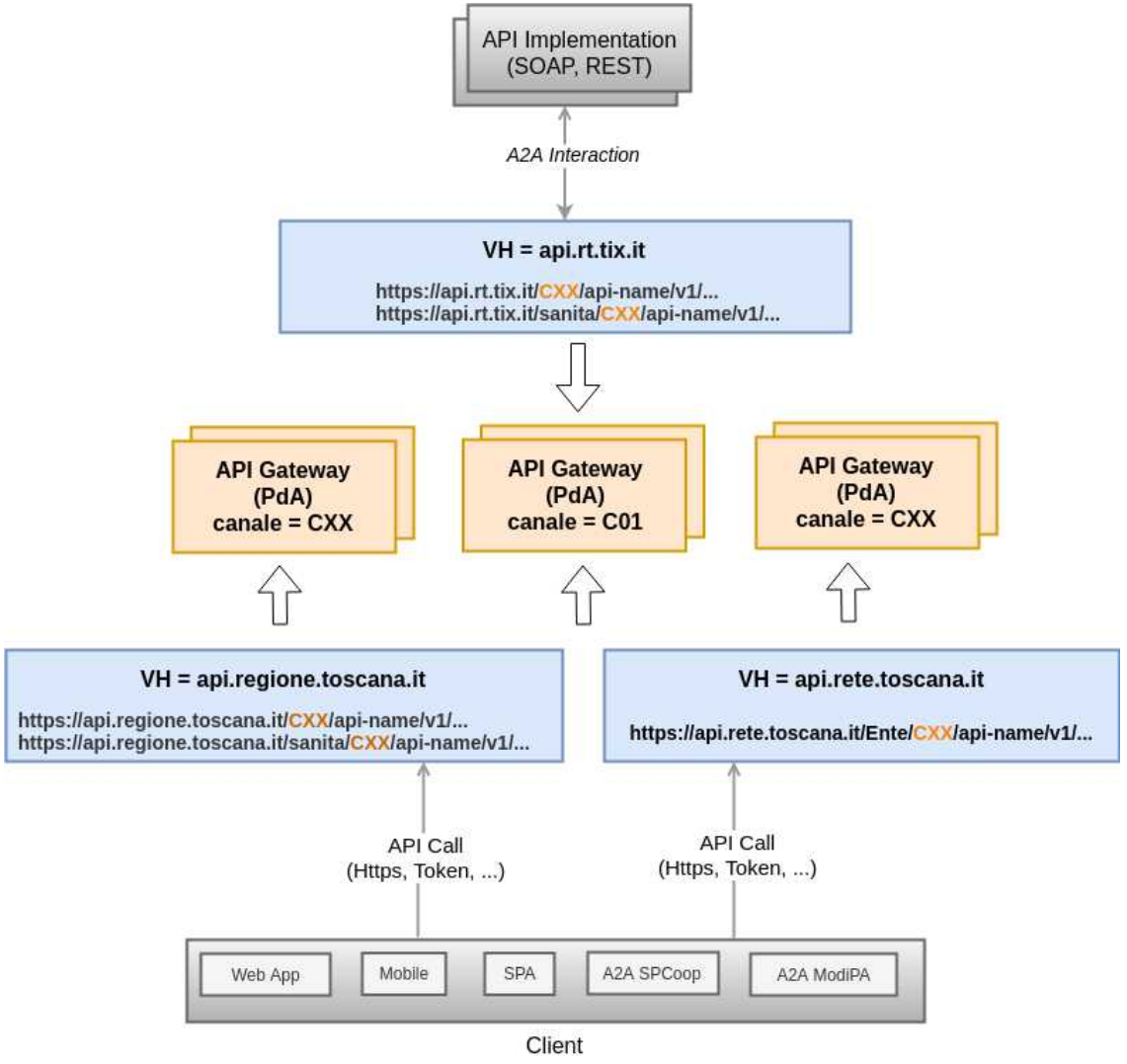
Confidenzialità e Autenticazione Fruitore

Non Ripudiabilità della Trasmissione


RT
Analytics
Hadoop
Elastic Search
Application Log
API Log
Deploy API
Implementation
Deploy Applicazioni
Containers
Applicativi
eToscana Compliance
Standardizzazione API
Accreditamento Applicazioni
API CALL
Conformità
Registro API
API Gateway
CART
Token
Introspection
IDM RT
User Authentication
Oauth2 Authorization Server
Gestione dei Ruoli
Entra con SPID
HTTPS
Token
GetToken
Client APP
Client APP
Authentication
Resource Owner

Il modello architetturale attuale del CART




API Implementation
(SOAP, REST)
A2A Interaction
VH = api.rt.tix.it
https://api.rt.tix.it/CXX/api-name/v1/...
https://api.rt.tix.it/sanita/CXX/api-name/v1/...
API Gateway
(PdA)
canale = CXX
API Gateway
(PdA)
canale = C01
API Gateway
(PdA)
canale = CXX
VH = api.regione.toscana.it
https://api.regione.toscana.it/CXX/api-name/v1/...
https://api.regione.toscana.it/sanita/CXX/api-name/v1/...
VH = api.rete.toscana.it
https://api.rete.toscana.it/Ente/CXX/api-name/v1/...
API Call
(Https, Token, ...)
API Call
(Https, Token, ...)
Web App
Mobile
SPA
A2A SPCoop
A2A ModiPA
Client

Principali Funzionalità

- Pieno supporto dei paradigmi REST e SOAP
- Autenticazione e autorizzazione basata su HTTPS o su Token JWS
- Tracciamento a Norma
- Validazione dei contenuti
- Politiche di Rate Limiting
- Caching delle Risposte
- Trasformazione dei Contenuti
- Consegna condizionale a destinatari multipli
- Integrazione Analytics ELK
- Supporto delle Nuove Linee Guida di Interoperabilità AGID (ModiPA)
- Supporto delle specifiche europee di interoperabilità applicativa (CEF eDelivery)

Il Nuovo Portale del CART

- In fase di completa riprogettazione
- Drastica semplificazione della user experience rispetto alle versioni precedenti
  - Presentazione dei servizi come collezioni di singole API (erogazioni e/o fruizioni)
  - Gestione delle richieste di adesione ai servizi, anziché delle richieste di erogazioni e di fruizioni di API diverse
  - Funzionalità diagnostiche evolute disponibili ai vari profili di utenza
- Rilascio previsto per maggio 2021

Le modalità di Ingaggio

- Registrazione nuove API (sempre gestita via Ticket)
  - Richiesto un referente del Servizio per l'autorizzazione delle successive richieste di adesione
  - Richiesto un referente tecnico dell'API Implementation
- Adesione alle API (al momento gestita via Ticket per singola API, prevista da Portale di Gestione per aggregazione di API)
  - Richiesto un referente dell'Ente Aderente
  - Richiesta la referente tecnico dell'applicazione client

Registrazione nuove API

- Viene richiesto quanto segue:
  - WSDL o OpenAPI dell'Interfaccia. Se non disponibili, indicare
    - Il tipo di API (SOAP 1.1, SOAP 1.2, HTTP)
    - Se HTTP, i metodi HTTP utilizzati (POST, GET, …)
  - Base URL dell'API Implementation
  - Le modalità di accesso alle API
    - Pubblica, HTTPS, OAuth: la stessa API può essere erogata con modalità diverse
- All'API Implementation sono sempre inoltrati due nuovi header http
  - X-CART-id: identificativo unico della transazione
  - X-CART-clientId: identificativo dell'applicativo richiedente
- Al Client fruitore viene sempre restituito l'header http X-CART-id

Le Modalità di Accesso alle API HTTPS

- Il Client viene identificato dal certificato
- E’ possibile l’Autorizzazione puntuale sul certificato mittente
- E’ possibile anche l’Autorizzazione per ruolo
  - gestito su CART sulla base dei certificati assegnati agli applicativi

Le Modalità di Accesso alle API OAuth

- Viene sempre registrato su ARPA una “audience”, generalmente uguale al nome dell’API
- I client OAuth devono essere esplicitamente autorizzati su ARPA ad ottenere l’audience nel token
- Caso Client Credentials
  - Autorizzazione sul valore del claim “aud” presente nel token
  - Se richiesto, autorizzazione puntuale sul claim “clientId” presente nel token
- Autorization Code
  - Autorizzazione sul valore del claim “aud” presente nel token
  - Verifica della presenza del claim fiscal_number
  - Verifica del livello minimo di autenticazione richiesta (claim auth_level)

Informazioni comunicate all'API Implementation

All'API Implementation può essere inoltrato il token originale, o anche i contenuti del token già decodificati nei seguenti header http (se presenti nel token)

- X-CART-id
- X-CART-clientId
- X-CART-fiscalNumber
- X-CART-name
- X-CART-familyName
- X-CART-email
- X-CART-ivaCode
- X-CART-oauthClientId
- X-CART-scope
- X-CART-roles

L'API Implementation può eventualmente interagire direttamente con l'Authorization Server usando il token ricevuto dal Gateway

Ulteriori controlli di autorizzazione OAuth

- Se utilizzati, gli scope vengono rilasciati da ARPA:
  - in funzione del client richiedente
  - eventualmente, in funzione dei ruoli dell'utente coinvolto (per il flusso 'authorization code')
- Questo permette di filtrare l'accesso alle API o anche alle risorse sulla base dello specifico client o anche del ruolo dell'utente, semplicemente controllando lo scope presente nel token
- La funzionalità può essere eventualmente attivata al momento della registrazione dell'API
  - Specificando l'associazione tra singole risorse e scope richiesti per l'accesso
  - Specificando l'associazione tra ruolo utente e scope