Introduzione alla Piattaforma CART

Redatto da	Ugolini Grazia	Piattaforme e Infrastrutture per i servizi on-line e la cittadinanza digitale
Approvato da	Sergio Papiani	Ufficio per la transizione al digitale Infrastrutture e tecnologie per lo sviluppo della società dell'informazione
Versione	1.0	
Data emissione	20/07/2020	
Stato		

Indice generale

1 Introduzione

Il CART è l'infrastruttura di RT dedicata a regolare le comunicazioni applicative sia con i soggetti esterni a Regione che tra soggetti interni al dominio regionale. Gli obiettivi principali dell'infrastruttura CART sono i seguenti:

- mettere in sicurezza l'accesso alle API;
- censire le API 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 dialogo degli applicativi, in maniera trasparente rispetto alle modalità di interscambio utilizzate con l'esterno (es: SPCoop, modiPA, …).

Alla base dell'operatività dell'infrastruttura ci sono due servizi finalizzati alla gestione delle API:

- un registro centrale delle API gestite, utilizzato per il censimento delle API e delle varie modalità di accesso alle stesse;
- un insieme di nodi che fungono da API Gateway, regolando gli accessi alle implementazioni delle API da parte degli applicativi autorizzati, in accordo alle politiche regionali ed alle normative nazionali di interoperabilità.

2 Gli aspetti organizzativi

Le API del CART sono classificate in collezioni, denominate "Servizi". Una collezione può anche contenere un'unica API. Ogni servizio è individuato come l'insieme minimo di API necessarie per l'utilizzo di una singola funzionalità. Ad esempio, l'adesione al set minimo di funzionalità dell'RFC 101 richiede l'attivazione per ogni singolo aderente di due API:

- la fruizione dell'API di RFC101_InvioEvento
- l'Erogazione dell'API di RFC101_InvioEvento_Ack

Nel loro insieme queste due API costituiscono un singolo servizio (RFC101), a cui può essere richiesta l'adesione.

Per ogni Servizio viene sempre individuato almeno:

- un referente del servizio, che dovrà essere sempre afferente all'Ente erogatore del servizio. Il suo compito è quello di autorizzare le nuove richieste di adesione e di monitorare, utilizzando gli strumenti messi a disposizione dal CART, l'andamento del servizio nel tempo;
- un referente tecnico del servizio, preferibilmente un indirizzo presidiato, a cui rivolgersi nel caso di anomalie nell’interazione con le implementazioni delle API appartenenti al servizio.

2.1 La registrazione di nuove API

La registrazione di nuove API o di nuove versione delle API esistenti avviene tramite la compilazione di opportuni moduli di registrazione, diversi in funzione del tipo di API WSDL o REST.

I moduli richiedono di specificare tutte le informazioni necessarie per la corretta gestione della registrazione dell'API e delle successive richieste di fruizione della stessa API, tra cui le interfacce delle API (WSDL per le API SOAP, OpenAPI per le API REST), gli endpoint dei servizi di backend verso cui saranno girate le richieste in arrivo e i requisiti di sicurezza e di disponibilità per l'accesso alle API.

In fase di registrazione, viene anche valutato se la nuova API è parte di un servizio esistente, o se debba essere registrata come parte di un nuovo servizio.

Se l'API prevede accesso tramite 'token', il CART chiederà al supporto ARPA la registrazione di un "audience", con lo stesso nome dell'API, dedicata al controllo degli accessi. I client autorizzati all'accesso all'API dovranno infatti avere il nome dell'API come valore del claim 'audience' del token utilizzato per l'accesso, oltre ovviamente a tutti gli altri paramentri previsti dalle politiche di accesso all'API (es: spid-level).

Dopo la registrazione, un nuovo endpoint sarà disponibile per l'accesso all'API. Inizialmente, a meno che l'APi non sia ad accesso pubblico, non esistono applicativi autorizzati all'accesso all'API e qualunque tentativo di accesso a quell'endpoint restituirà quindi un errore di mancata autorizzazione.

Successivamente, mediante le richieste di adesione al servizio di cui l'API fa parte, si potranno autorizzare all'accesso i client fruitori.

2.2 Le Richieste di Adesione ai Servizi

La richiesta di adesione viene avviata da un referente dell'Ente aderente o anche da referenti delle ditte fornitrici, se esplicitamente delegati a questo tipo di operazione. In ogni caso la richiesta dovrà indicare un referente dell'Ente aderente, che resta il responsabile dell'adesione al servizio, ed almeno un referente tecnico degli applicativi interessati all'adesione.

In generale, una nuova adesione si articola nelle seguenti fasi:

- la richiesta di adesione;
- l'autorizzazione da parte del referente del Servizio;
- la fase di configurazione, che può essere più o meno articolata in funzione della complessità del servizio.

Allo stato attuale la gestione delle richieste di nuove adesioni viene avviata tramite l'apertura di un ticket, inviando mail a "cartdesk@regione.toscana.it" ed indicando il servizio a cui si intende aderire. CartDesk fornirà quindi un modulo di adesione (specifico per il servizio) che include tutte le informazioni tecniche necessarie, da compilare da parte del richiedente. Una volta ricevuta la scheda compilata da parte del richiedente, CartDesk procederà alla richiesta di autorizzazione al referente del servizio.

Appena ottenuta l'autorizzazione, sarà avviata la fase di configurazione dell'infrastruttura CART. In questa fase CartDesk potrà interagire con altri supporti regionali per la registrazione di credenziali necessarie all'attivazione del servizio. Le principali interazioni avvengono con:

- il supporto dei "sistemi IT regionali" per la generazioni di chiavi e certificati X509 necessari per l'accesso ai servizi con autenticazione client https;

- il supporto ARPA per la generazione di client-id e relativo secret OAUth2 necessari per l'accesso ad API protette da token.

Al termine della fase di configurazione, CartDesk comunicherà al richiedente le URL di accesso alle API e le credenziali di accesso per ognuna di esse.

Il processo è analogo per l' ambiente di stage e per quello di produzione.

3 L'accesso alle API del CART

Le API gestite dal CART sono accessibili, esclusivamente tramite protocollo https, a 3 diversi indirizzi:

- api.regione.toscana.it: riservato agli accessi da Internet alle API erogate da Regione Toscana. Su questo endpoint è stato riservato il contesto '/sanita' per le API relative al dominio della Sanità regionale;
- api.rt.tix.it: è sostanzialmente un punto di accesso alternativo alle stesse API esposte da api.regione.toscana.it, raggiungibile però esclusivamente dagli applicativi installati sulla rete privata regionale del TIX;
- api.rete.toscana.it: è il punto di accesso dedicato alle API delle Amministrazioni del territorio regionale diverse da Regione Toscana; le API di ogni amministrazione sono indirizzate da un contesto con l'identificatore dell'Amministrazione erogatrice della API. Es:
    - https://api.rete.toscana.it/CPisa/sample-api/v1/...

Per ognuno di questi punti di accesso sono definiti diversi "canali", che possono differenziarsi per il livello di servizio offerto o perché dedicati a specifici domini applicativi, o anche per la diversa versione dell'implementazione della stessa infrastruttura CART.

I canali sono individuati da semplici identificatori del tipo "CXX", che vengono utilizzati come parte dell'endpoint di accesso al servizio, come ad esempio:

- https://api.regione.toscana.it/C01/sample-api/v1/…
- https://api.regione.toscana.it/C02/sample-api/v1/…
- https://api.rete.toscana.it/C01/CPisa/sample-api/v1/…
- https://api.rete.toscana.it/C02/CPisa/sample-api/v1/...

Al momento della richiesta di adesione ad un servizio, il richiedente può chiedere di accedere ad una API utilizzando un applicativo client preesistente, che ovviamente dovrà essere compatibile con le modalità di accesso a quella API, oppure richiedere la registrazione di un nuovo applicativo client. Nel primo caso il CART autorizzerà l'applicativo indicato all'accesso alla nuova API, mentre nel secondo caso sarà registrato un nuovo client e le credenziali comunicate al richiedente.

La prima modalità è tipicamente utilizzata quando la stessa applicazione ha bisogno di accedere a più API. Naturalmente è sempre possibile usare credenziali multiple per

accedere alle diverse API, ma questo rende la gestione delle credenziali ed il monitoraggio degli accessi al servizio certamente più macchinoso, ed è quindi da evitare.

Allo stesso modo è da evitare, per quanto generalmente possibile, l'utilizzo delle stesse credenziali per far accedere applicazioni client diverse ad una stessa API.

In sostanza, ogni singola applicazione client deve essere registrata sul CART alla prima richiesta di accesso, per poter poi ottenere incrementalmente autorizzazioni ulteriori, a mano a mano che sorgano ulteriori esigenze di accesso ad altre API.

Qualunque sia la modalità utilizzata, al termine dell'iter di adesione, l'applicazione client potrà accedere alle API, utilizzando una delle tipologie di accesso previste:

- "HTTP Basic", modalità deprecata, ma ancora supportata per compatibilità con il passato. In questa modalità, utenza e password vengono fornite dalla gestione CART al referente dell'adesione.
- "HTTPS", in questo caso per l'accesso alle API è richiesta la "client authentication" HTTPS. L'archivio contenente sia la chiave privata che il certificato X509 viene generalmente fornita dal CART tramite comunicazioni sicure con il referente dell'adesione.
- Token Authentication: in questo caso l'accesso all'API è gestito tramite Bearer Authentication. Il Token deve essere rilasciato da una delle fonti di autenticazione riconosciute da Regione Toscana, che possono anche variare per specifiche API. Tipicamente il Token viene ottenuto dal client tramite negoziazione OAUTH2 con gli Authorization Server di Regione Toscana (ARPA).

Se la richiesta di adesione è riferita ad API che prevedono accesso tramite 'token', i token presentati dai client per l'accesso alla API dovranno avere il nome della API nel claim 'audience' del token presentato per l'accesso, oltre ovviamente a tutti gli altri parametri previsti dalle politiche di accesso all'API (es: spid-level).

4 Aspetti relativi all’integrazione applicativa

Gli API Gateway del CART espongono le stesse interfacce applicative native dei servizi, così come definite dalle interfacce applicative, espresse in linguaggio WSDL nel caso di API SOAP e OpenAPI nel caso di API REST. Pertanto gli applicativi continuano ad operare sostanzialmente come se stessero interagendo direttamente con l’applicativo che implementa l’API, a meno della URL invocata dai client, che diventa quella del Gateway, anziché quella del servizio finale.

Ci sono tuttavia alcune informazioni aggiuntive che è utile che il Gateway possa trasmettere agli applicativi con cui interagisce, sia ai client che invocano le API che alle implementazioni delle API a cui vengono girate le richieste applicative, come descritto nelle prossime sezioni.

4.1 Modalità di Integrazione degli applicativi server

Nel caso degli applicativi server, i Gateway del CART, per ogni richiesta gestita, introducono i seguenti header HTTP nella richiesta HTTP girata alla implementazione della API:

- ‘X-CART-id’, valorizzato con un identificativo unico di transazione generato dal CART;
- ‘X-CART-clientId’, valorizzato con il nome con cui è stato censito sul CART l’applicativo che ha originato la richiesta.

Nel caso la richiesta sia di tipo OAuth, all’implementazione della API potrà essere fornito il token originale, e/o i seguenti header CART aggiuntivi contenenti le informazioni presenti nel token.

Header Name	Header Value
X-CART-fiscalNumber X-CART-name X-CART-familyName X-CART-email X-CART-ivaCode	Informazioni estratte dall’access token, se presenti
X-CART-oauthClientId	identificativo dell’applicazione client che ha generato il token Oauth
X-CART-scope	elenco degli scope, separati con una virgola, eventualmente presenti nel token Oauth
X-CART-roles	elenco dei ruoli dell’utente, separati da virgola. In questa modalità vengono forniti soltanto i ruoli di un utente e non i relativi attributi

4.2 Modalità di Integrazione degli applicativi Client

Nel caso degli applicativi client, i Gateway CART, per ogni richiesta in arrivo introducono il seguente header HTTP nella risposta restituita al client:

- ‘X-CART-id’, valorizzato con un identificativo unico di transazione generato dal CART;

Il Gateway può inoltre produrre, in caso di anomalie nella gestione della richiesta, due diverse tipologie di errori:

- Errori Client: identificabili da un codice http 4xx su API REST o da un fault code di tipo “Client” su API SOAP. Indicano che sono stati rilevati dal Gateway problemi nella richiesta ricevuta dal client (es. errore autenticazione, autorizzazione, validazione contenuti…).
- Errori Server: identificabili dai codici http 502, 503 e 504 per le API REST o da un fault code “Server” generato dal gateway e restituito con codice http 500 per le API SOAP.

Per ciascun errore il Gateway riporta le seguenti informazioni:

- lo “status code” http per le API REST o il fault code per le API SOAP;
- un codice di errore, indicato nell’header http “GovWay-Transaction-ErrorType”, che riporta l’errore rilevato dal gateway (es. AuthenticationRequired, TokenExpired, InvalidRequestContent …);
- un payload http, contenente maggiori dettagli sull’errore, opportunamente codificato come “Problem Details” per le API REST o Soap Fault per le API SOAP.

La codifica degli errori prodotta dal CART permette alle applicazioni client di discriminare tra errori causati da una richiesta errata, per i quali è quindi necessario intervenire sull’applicazione client prima di effettuare nuovi invii, ed errori dovuti allo stato dei servizi invocati, per i quali è invece possibile continuare ad effettuare la richiesta, come dettagliato nella tabella seguente.

Tabella 1: Gestione degli Errori

REST / SOAP	GovWay-Transaction-ErrorType	Retry
400 / Client	Errori 400 (Bad Request)	No
401 / Client	Errori 401 (Authentication Error)	No
403 / Client	Errori 403 (Authorization Deny)	No
404 / Client	Errori 404 (NotFound)	No
409 / Client	Errori 409 (Conflict)	No
429 / Client	LimitExceeded - Errori 429 (Rate Limiting)	No

REST / SOAP	GovWay-Transaction-ErrorType	Retry
429 / Client	TooManyRequests - Errori 429 (Rate Limiting)	Sì
502 / Server	Errori 502 (Bad Gateway)	Sì se idempotente
503 / Server	Errori 503 (Service Unavailable)	Sì
504 / Server	Errori 504 (Endpoint Request Timed-out)	Sì se idempotente

Nei casi in cui è prevista la rispedizione, GovWay genera un header “Retry-After” che indica al client il numero di secondi di attesa prima di ripetere la richiesta.

5 Le principali funzionalità gestite dal CART

Le modalità standard CART per la richiesta di registrazione e di accesso alle API assicurano alcune funzionalità di base, come in particolare:

- l'autenticazione delle applicazioni client;
- la verifica di autorizzazione per l'accesso alle specifiche API richieste;
- la gestione a norma dei protocolli di interoperabilità, dove richiesto (SPCoop, modiPA);
- il monitoraggio applicativo delle API gestite (analytics).

L'infrastruttura operata dal CART è in grado poi di erogare numerose ulteriori funzionalità di interesse per gli specifici progetti, tipicamente negoziate con i responsabili di progetto nella fase di registrazione delle API. Di seguito un elenco delle principali ulteriori funzionalità gestibili:

- politiche evolute di autorizzazione basate sui contenuti dei messaggi, espresse anche tramite policy XACML;
- validazione dei contenuti dei messaggi di richiesta e di risposta;
- Politiche di rate limiting;
- caching delle risposte;
- trasformazione dei contenuti;
- consegna condizionale a destinatari multipli.

6 L'analisi del comportamento delle API (API Analytics)

I dataset di log delle pda del CART possono essere resi disponibili come indici ELK, al fine di permettere ai vari progetti applicativi di realizzare dashboard mirate per le proprie specifiche esigenze, integrando i dati degli indici del CART con i propri indici applicativi.

Gli indici CART sono opportunamente documentati in modo da permetterne un pieno utilizzo nei più diversi contesti.

CART mantiene comunque un proprio repository di monitoraggio "general purpose", in grado di permettere ai gestori del CART e ai responsabili dei servizi il monitoraggio dell'andamento dei servizi.

Allegato A – Standard di Riferimento

Le modalità di integrazione descritte in questo documento fanno riferimento a vari standard consolidati ed ai documenti di specifica riferiti nella tabella seguente, a cui si rimanda per ulteriori informazioni in proposito.

Specifica	Riferimento	Utilizzo nel CART
ModiPA	https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/master/index.html	Supporto delle Linee Guida di Interoperabilità con Soggetti esterni
OpenAPI	http://spec.openapis.org/oas/v3.0.3	Utilizzato per la specifica delle API REST
WSDL	https://www.w3.org/TR/wsdl.html	Utilizzato per la specifica delle API SOAP
HTTP asic Auth	https://tools.ietf.org/html/rfc7617	Autenticazione degli applicativi client tramite credenziali composte da username e password (deprecato)
The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246	Usato per l' autenticazione HTTPS dei client
Problem Details for HTTP APIs	https://tools.ietf.org/html/rfc7807	Utilizzato per rappresentare l'errore prodotto dalla gestione delle API REST.
OAuth 2.0 Authorization Framework	https://tools.ietf.org/html/rfc6749	Da parte dei client applicativi per la negoziazione dei token con gli Authorization Server di RT
OpenID Connect 1.0 Core (OIDC)	http://openid.net/specs/openid-connect-core-1_0.htm	
OAuth 2.0 Authorization Framework: Bearer Token Usage	https://tools.ietf.org/html/rfc6750	Da parte dei client applicativi per l'autenticazione alle API CART protette da Token
JSON Web Token (JWT)	https://tools.ietf.org/html/rfc7519	Formato dei Token