PROGETTAZIONE E REALIZZAZIONE DEL DS&SRF “DATA SHARING AND SERVICE REPOSITORY FACILITIES” NELL’AMBITO DEL PROGETTO PNRR “MAAS FOR ITALY”

Specifiche funzionali | Autorizzazione API

Descrizione del documento

Nome del documento	Specifiche funzionali | Autorizzazione API
Delivery di riferimento	Gestione utenti e profilazione
Redatto da	Marco Marabitti
Approvato da	Michele Vigilante
Versione attuale	1.1

Status e revisioni

Versione	Owner	Modifiche	Data
1.0	Accenture	Prima emissione	30/03/2023
1.0_rev	MIT	Osservazioni e commenti alla 1.0	07/04/2023
1.1	Accenture	Recepimento osservazioni e aggiunta dettagli	12/04/2023

Approvazione

17/05/2023	Andrea Napoleoni	Firmato digitalmente da **Andrea Napoleoni** O = MiMS C = IT

Indice

1. SCOPO DEL DOCUMENTO

Il presente documento contiene la specifica funzionale sul meccanismo di autenticazione e autorizzazione per le API che verranno esposte dalla piattaforma DS&SRF ai MaaS Operator.

1. SISTEMA IN OGGETTO

La piattaforma DS&SRF (*Data Sharing and Service Repository Facilities*) funge da layer di disintermediazione tra gli operatori di trasporto e gli operatori MaaS. Il DS&SRF è strumentale alle funzioni che possono essere svolte, nell'ambito dello sviluppo dei progetti di Mobility as a Service.

All'interno di questo documento verrà descritto il meccanismo di autenticazione e autorizzazione per le RESTful API che saranno esposte dal DS&SRF ai MaaS Operator.
Il meccanismo di autenticazione ed autorizzazione delle API risulta rilevante per le seguenti finalità:

- garantire che solo i solo i sistemi software dei MaaS Operator aderenti al programma siano in grado di accedere alle funzionalità del DS&SRF;
- garantire la tracciabilità delle chiamate eseguite da ogni MaaS Operator.

2. GLOSSARIO DEFINIZIONI ED ACRONIMI

ACRONIMO	DESCRIZIONE
DS&SRF	Data Sharing & Service Repository Facility – in seguito anche "piattaforma"
MSP	Mobility Service Provider
MaaS	Mobility as a Service
NAP	National Access Point
RAP	Regional Access Point
PdV	Piattaforma di Vendita
OTP	Operatore di Trasporto Pubblico
MO	MaaS Operator
NeTEx	Network Timetable Exchange
SIRI	Service Interface for Real time Information
OpRa	Operating Raw Data and statistics exchange
DatEx II	Data exchange standard for traffic information
OAuth2	Open standard for Authorization v2

Tabella 1 - Elenco degli acronimi.

3. RIFERIMENTI

RIF	TITOLO
1	Discussion paper "Data Sharing and Service Repository Facilities"
2	Disegno architetturale DS&SRF: Scenari architetturali alternativi
3	High level architecture
4	DS&SRF Business Canvas
5	Piano dei fabbisogni
6	Remediation plan
7	Specifica Gestione viaggi

Tabella 2 - Elenco dei riferimenti.

2. SPECIFICA FUNZIONALE

Per quanto riguarda l'autenticazione e l'autorizzazione delle chiamate ad API RESTful esposte dalla piattaforma DS&SRF si propone di utilizzare il protocollo Oauth2 e nello specifico Client Credential Grant Type Flow, ossia l'uso di "client id" e "client secret" rilasciati a ciascun MaaS Operator per ottenere un Access Token che permetta la verifica dell'autenticazione del client stesso.

In fase pilota il processo per la richiesta e l'ottenimento delle credenziali sarà un processo manuale. I MaaS Operator coinvolti nel pilota dovranno far richiesta delle credenziali ai referenti progettuali da un rappresentante del MaaS. Le credenziali verranno quindi generate tramite le interfacce dell'api gateway 3Scale e verranno sottoscritte al prodotto di riferimento per le API MaaS. Le credenziali dovranno essere consegnate secondo canali sicuri al MaaS Operator.

Il diagramma di sequenza della figura 1 mostra gli step che il MaaS operator dovrà compiere per autenticarsi e gli step di validazione del token.

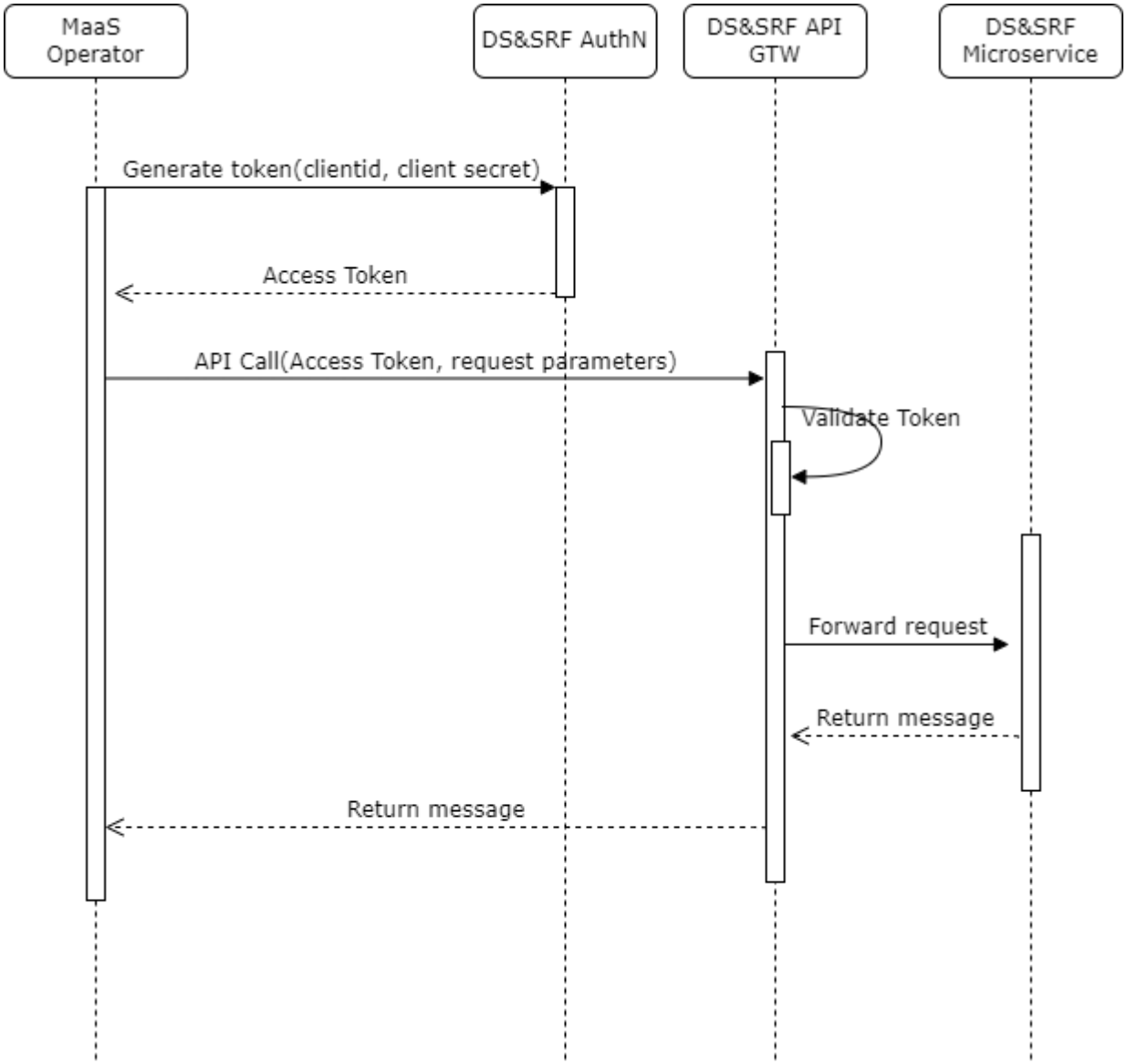

Figura 1: Flusso di autenticazione e autorizzazione delle chiamate API

A ciascun MaaS Operator verranno fornite un "client id" e un "client secret" necessari per ottenere l'"access token". In fase iniziale tali credenziali verranno generate manualmente e comunicate al MaaS operator seguendo canali di comunicazione sicuri.

In fase successiva i MaaS Operator potrebbero registrarsi in maniera automatica tramite un Developer Portal messo a loro disposizione. Tramite tale portale potranno richiedere le credenziali e sottoscriversi alle API che ritengono utili. Il processo di iscrizione e di sottoscrizione alle API potrebbe essere soggetto ad un iter approvativo prima di consegnare le credenziali al MaaS Operator.

Per ovvie ragioni di sicurezza in caso di ambienti diversi (ad esempio l'ambiente di integration test e l'ambiente di produzione) saranno fornite al MaaS Operator credenziali diverse.

Come primo step il MaaS Operator dovrà richiedere un access token. Per ottenere il token il MaaS Operator dovrà chiamare la seguente API.

La scelta del flusso di autenticazione chiamato credentials grant flow è dettata dal fatto che le interazioni tra MaaS Operator e DS&SRF saranno sempre interazioni tra sistemi di backend (machine to machine).

API Path	/oauth2/token	
HTTP Method	POST	
HTTP Request Headers	Content-Type	application/x-www-form-urlencoded
	Authorization	Basic *base64(clientkey:clientsecret)*
Request Body Parameters	grant_type	client_credentials
	scope	*Lista degli scope richiesti separate da virgola*
HTTP Response Headers	Content-Type	application/json
HTTP Response Codes	200	OK
	400	Bad request
	401	Unauthorized
200 Response Body Parameters	access_token	*<JTW token>*
	expires_in	*Secondi di durata del token*
	token_type	Bearer
	scope	*Lista degli scope accettati*

Tabella 1 - Api richiesta token

Il token ricevuto sarà un JSON Web Token (JWT). Un token JWT è composto da tre parti:

header.payload.signature

- **Header**: contiene la tipologia del token e l'algoritmo utilizzato per la cifratura
- **Payload**: contiene tutti i dati relativi al token, compresi la data di scadenza dello stesso ed eventuali claims
- **Signature**: header e payload vengono concatenati e poi sottoposti a cifratura secondo l'algoritmo specificato nell'header

Una volta ottenuto l'access token il MaaS Operator dovrà inserirlo nell'Authorization header di ciascuna chiamata API che eseguirà.

L'header avrà questa forma:

Authorization: Bearer <Access Token>

Il token avrà una durata temporale limitata per tanto sarà responsabilità del MaaS Operator client di ottenere un token valido ogni qualvolta necessario. La durata del token sarà configurabile, con valore iniziale suggerito pari a 5 minuti.

L'utilizzo di un API manager permetterà la definizione di piani diversi che ciascun MaaS Operator potrà scegliere in base alle sue necessità. Il piano sottoscritto imporrà delle limitazioni sul numero di chiamate che possono essere fatte dall'operatore. Può anche essere definito un piano senza limiti.

La validazione del token è un processo che avviene solitamente in tre passi e l'API Gateway interagisce con l' ID Provider in queste fasi:

- Per prima cosa viene verificata la firma del token. La validità della firma certifica che il contenuto del token non è stato manomesso.
- Verificata la validità del JWT si passerà a verificare che il client sia sottoscritto a quella API.
- Tramite gli scope sarà possibile eventualmente procedere all'ulteriore autorizzazione a livello di verbi http l'accesso a ciascun client (ad esempio un client potrebbe avere solo permessi di lettura sull' entità viaggi mentre un altro potrebbe necessitare di accedere anche in scrittura).

Visto

Il responsabile unico del procedimento

Giorgio Pizzi

GIORGIO PIZZI
Ministero delle Infrastrutture e dei Trasporti
19.05.2023 09:24:27
GMT+00:00