PROGETTAZIONE E REALIZZAZIONE DEL DSRM “DATA SHARING AND SERVICE REPOSITORY FOR MAAS” 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	Iolanda Longobardi
Approvato da	Giuseppe Lo Presti
Versione attuale	1.2

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
1.2	Accenture	- Modifica denominazione da “DS&SRF” a “DSRM” - Adeguate modalità di ricezione clientId e client secret per i MO tramite la piattaforma - Integrazione autenticazione tramite API-KEY - Inserito segno grafico di evidenziazione delle parti modificate	15/12/2025

Approvazione

Indice

1. SCOPO DEL DOCUMENTO 4
1.1 SISTEMA IN OGGETTO 4
1.2 GLOSSARIO DEFINIZIONI ED ACRONIMI 4
1.3 RIFERIMENTI 5
2 AUTENTICAZIONE OAUTH2 7
3 AUTENTICAZIONE API-KEY 10

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 DSRM ai MaaS Operator e ai RAP.

1.1 SISTEMA IN OGGETTO

La piattaforma DSRM funge da layer di disintermediazione tra gli operatori di trasporto e gli operatori MaaS. Il DSRM 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 DSRM 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 DSRM;
- garantire la tracciabilità delle chiamate eseguite da ogni MaaS Operator.

1.2 GLOSSARIO DEFINIZIONI ED ACRONIMI

ACRONIMO	DESCRIZIONE
DSRM	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

1.3 RIFERIMENTI

RIF	TITOLO
1	Discussion paper "Data Sharing and Service Repository Facilities (Allegato 2_Requisiti_DSSRF_DopoProgettazione_Pubblicato 07.06.2022.docx)[1]
2	Disegno architetturale DSRM: Scenari architetturali alternativi
3	High level architecture

[1] https://assets.innovazione.gov.it/1654592242-allegato-2_requisiti_dssrf_dopoprogettazione_pubblicato-07-06-2022.pdf

4	DSRM Business Canvas
5	Piano dei fabbisogni
6	Remediation plan
7	Specifiche funzionali | Autorizzazione API
8	Specifiche funzionali | Gestione viaggi
9	Specifiche funzionali | Recupero viaggio
10	Specifiche funzionali | Gestione dati dinamici TPL e Accesso dati di sharing
11	Specifiche funzionali | Gestione Analytics
12	Specifiche funzionali | KPI
13	Specifiche funzionali | Registrazione e accreditamento sulla piattaforma DSRM
14	Specifiche funzionali | Accordi commerciali
15	Linee guida compilazione SIRI IT [2]
16	Linee guida per la compilazione del profilo italiano del NeTEx [3]

Tabella 2 - Elenco riferimenti

[2] https://github.com/5Tsrl/siri-italian-profile/blob/main/Linee%20guida/Linee%20guida%20compilazione%20SIRI%20IT.pdf
[3] https://github.com/5Tsrl/netex-italian-profile/tree/main/Linee%20guida

2 AUTENTICAZIONE OAUTH2

Per quanto riguarda l'autenticazione e l'autorizzazione delle chiamate ad API RESTful esposte dalla piattaforma DSRM 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.

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.

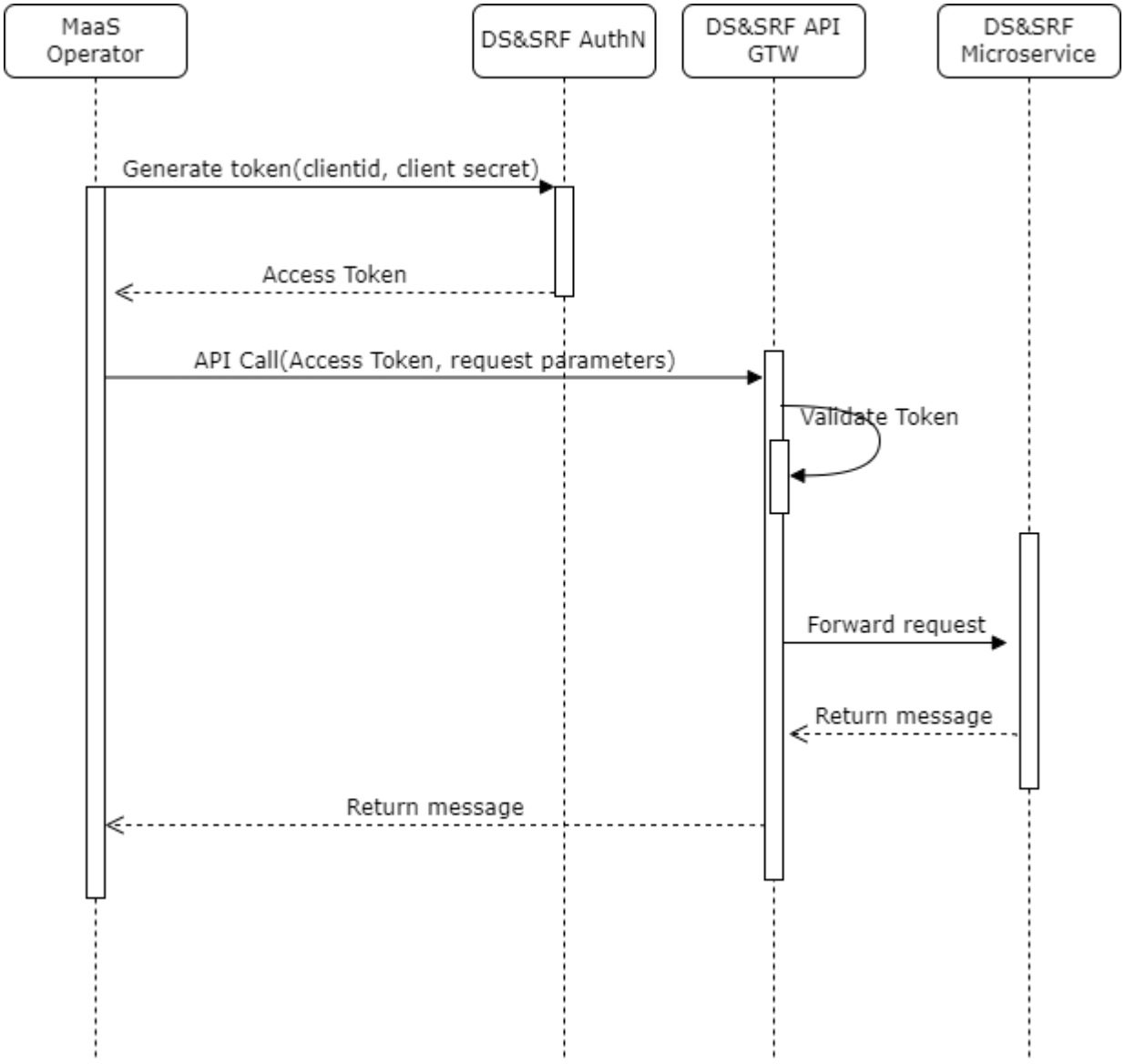

Figura 1: Flusso di autenticazione e autorizzazione delle chiamate API

A ciascun MaaS Operator verranno fornite un "client id" e un "client secret" necessari per ottenere l'"access token".

I MaaS Operator visualizzano le credenziali per accedere al flusso B2B solo dopo aver eseguito l'accreditamento alla piattaforma (si rimanda alla specifica di Registrazione e Accreditamento).

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 DSRM 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 3 - 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).

3 AUTENTICAZIONE API-KEY

Relativamente all'autenticazione B2B tra DSRM e RAP, oltre all'autenticazione OAUTH2 descritta in precedenza, verrà supportata anche l'autenticazione tramite API-KEY.

In particolare, il DSRM si autenticherà in modalità API-KEY verso i RAP che hanno richiesto tale modalità: l'autenticazione avverrà con un token statico, che può essere riutilizzato più volte.

La chiave statica verrà comunicata dal RAP di riferimento tramite canale esterno al portale e periodicamente si potrà concordare una variazione della chiave condivisa, in modo da minimizzare il rischio di furto della chiave stessa.

Visto

Il responsabile unico del procedimento

Giorgio Pizzi

GIORGIO PIZZI
10.02.2026
10:46:20
GMT+01:00

Il direttore di esecuzione del contratto

Alessandro Schiavetti

Alessandro Schiavetti
30.01.2026 10:24:22
GMT+01:00