Oracle® Banking Microservices Architecture

API Security Guide

Release 14.7.1.0.0
F77050-01
May 2023

ORACLE

Oracle Banking Microservices Architecture API Security Guide, Release 14.7.1.0.0

F77050-01

Contents

Preface

Introduction

This guide provides security-related usage and configuration recommendations for Oracle Banking Microservices Architecture. It also describes the procedures required to implement or secure certain features, but it is not a general-purpose configuration manual.

Audience

This guide is primarily intended for IT department or administrators deploying Oracle Banking Microservices Architecture and third party or vendor software's. It includes the information related to IT decision makers and users of the application.

> **Note:**
>
> Readers are expected to have basic operating system, network, and system administration skills with an awareness of vendor/third-party software's and knowledge of Oracle Banking Microservices Architecture application.

Scope

Read Sections Completely

Each section should be read and understood completely. Instructions should never be blindly applied. Relevant discussion may occur immediately after instructions for an action, so be sure to read whole sections before beginning implementation.

Understand the Purpose of this Guidance

The purpose of the guidance is to provide security-relevant code and configuration recommendations.

Limitations

This guide is limited in its scope to security-related guideline for developers.

Acronyms and Abbreviations

List of Topics

Table 1 List of Topics

Topics	Description
Securing API Services	This topic provides the information on securing the API services.

1

Securing API Services

This topic describes about Securing API Services.

Different applications deployed on disparate platforms and using different infrastructure need to be able to communicate and integrate seamlessly with Oracle Banking Microservices Architecture in order to exchange data. The Oracle Banking Microservices Architecture Service API Gateway cater to these integration needs.

The integration needs to be supported by the Gateway can be broadly categorized from the perspective of the Gateway as follows:

- **Inbound application integration:** It is used when any external system needs to add, modify or query information within Oracle Banking Microservices Architecture.
- **Outbound application integration:** It is used when any external system needs to be accessed for processing transactions within Oracle Banking Microservices Architecture.

1.1 API Security

This topic describes about the API Security.

The Oracle Banking Microservices Architecture application provides the API Layer (Service API Layer) which is used by external users to access the Oracle Banking Microservices Architecture functionality.

Access to this API layer is granted only via the following methods:

- OAuth with OAM (Oracle Access Manager)
- OAuth without OAM
- Oracle Banking Routing Hub

If the customer does not have OAM, they can use OAUTH without OAM or enterprise API Management layer should be implemented to protect the service API(s).

Register OAuth Clients with API Gateway

New Oath users can be registered with Oracle Banking Microservices Architecture using the below endpoint.

`http://<hostname>:<port>/api-gateway/createOauthUsers`

Sample Headers:

- Header: **appId**: SECSRV001
- Header: **Content-Type**: application/json
- Header: **userId**: <USERID>

- Header: **Authorization**: Bearer <<JWT Access Token>>

Sample Request Body:

```
{
          "UserList": [
              {
                  "clientId": "<< clientId >>",
                  "clientSecret": "<< clientSecret >>",
                  "validity": "<< Validity in seconds >>"
               },
               {
                  "clientId": "<< clientId >>",
                  "clientSecret": "<< clientSecret >>",
                  "validity": "<< Validity in seconds >>"
               }
               ]
}
```

Modify Token Expiry of Registered OAuth Client

Token expiry time can be updated using the below endpoint:

`http://<hostname>:<port>/api-gateway/modifyvalidity`

Sample headers:

- Header: **appId**: SECSRV001
- Header: **Content-Type**: application/json
- Header: **userId**: <USERID>
- Header: **Authorization**: Bearer <<JWT Access Token>>

Sample Request Body:

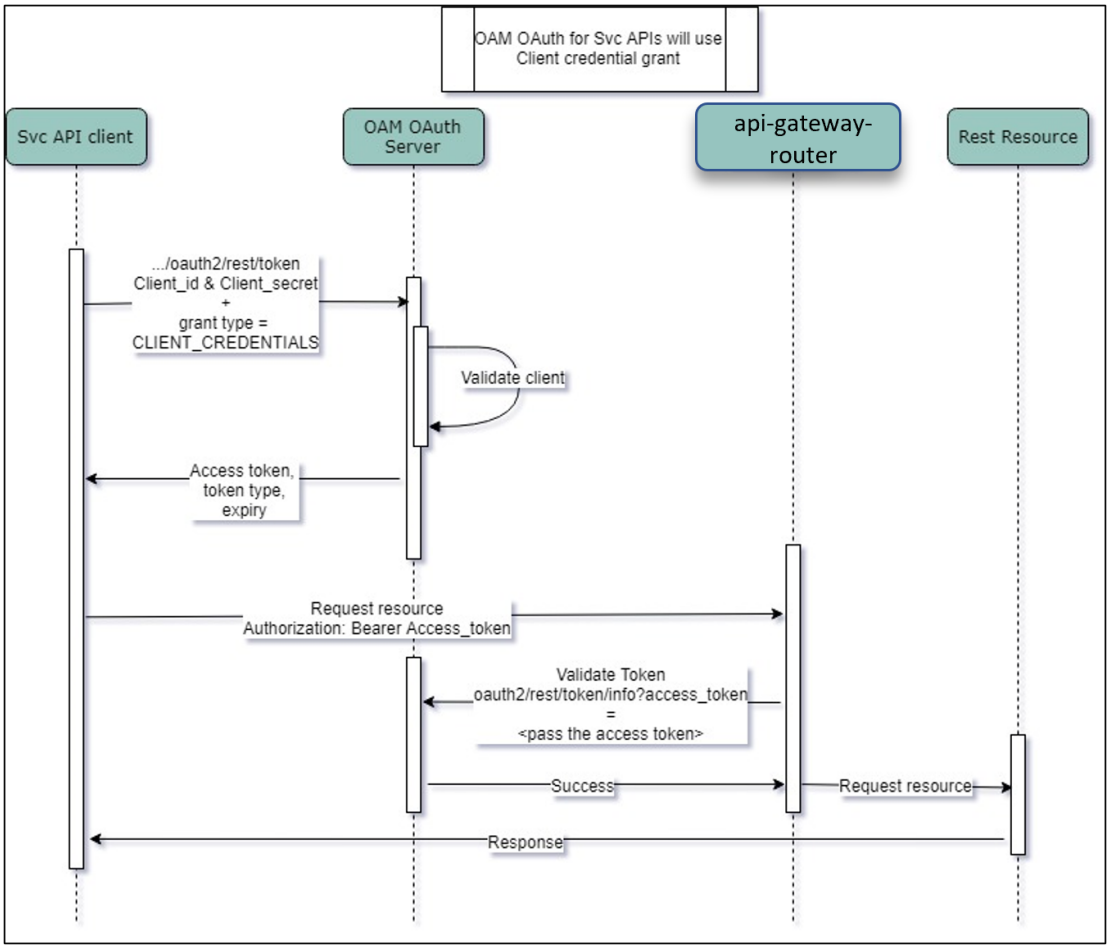
```
{"client_id":"<< clientId >>","validity":"<< Validity in seconds >>"}
```

API Security with OAuth

Oauth with OAM

The flow is explained below.

Figure 1-1 Oauth with OAM

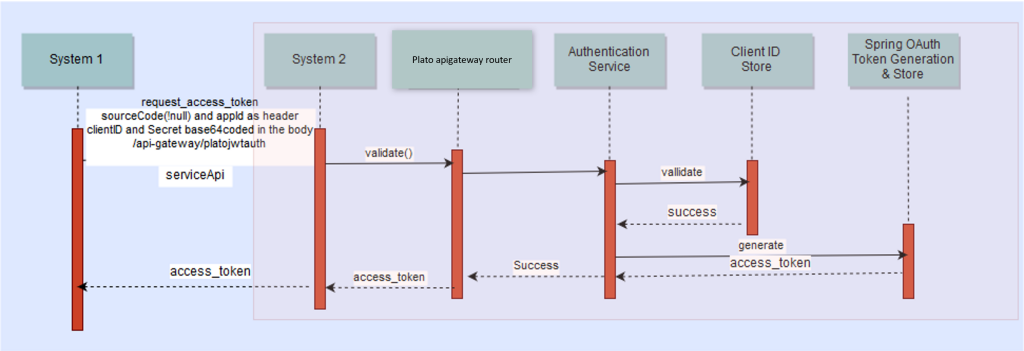


- API clients pass the client ID & client secret and grant type as CLIENT CREDENTIALS. To get the access token, use the endpoint `/oauth2/rest/token`.
- API clients passes the access token in the authorization header as bearer token in their subsequent calls to access the Service API's.
- Plato-Apigateway-router calls API Gateway validates the client access token on OAM Authorization server.
- If valid, it passes the request onto the Svc API's and gets the response.
- The client can refresh to get a new token before the current token expires. If the token expires, they can pass the client ID and client secret to get a new token.

OAuth without OAM

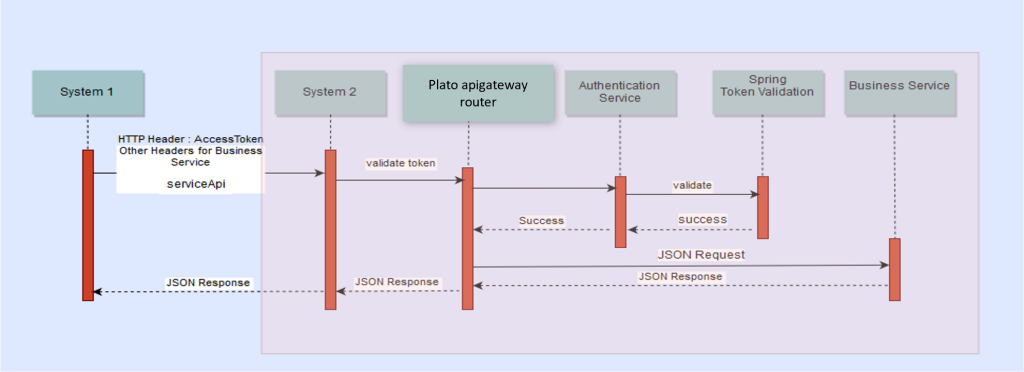
The flow for token generation is depicted below:

Figure 1-2 OAuth without OAM



The flow for accessing svc is depicted below:

Figure 1-3 OAuth without OAM - Accessing svc flow



- API clients passes the client id & client secret in the body and other required headers. To get the access token, use the endpoint. `http://<<hostname>>:<<port>>/api-gateway/platojwtauth/`.
- API clients passes the access token in the authorization header as bearer token in their subsequent calls to access the Service API's.
- Plato-apigateway-router calls Plato-api-gateway for validation before is routed to service.
- API Gateway validates the client access token on Authorization server.
- If valid, it passes the request on to the Svc API's and gets the response.
- The client can choose to get a new token (refresh) before the expiry of the current token. In case the token expires, they will pass the client Id and client secret to get a new token.
- Also, an additional facility of increasing the token is provided.

Access APIs through Oracle Banking Routing Hub

If the external services (services in bank or consulting) need to access APIs in Oracle Banking Microservices Architecture modules, the services will first have to generate an

access token using Oracle Banking Routing Hub endpoints and then use the token to authorize themselves to access the endpoints.

Refer to **Authentication** section under **Implementation** topic in **Routing Hub Configuration User Guide** for the further details.

1.2 List of Services

This topic information about the List of API Services.

Refer to the **REST API Documentation** for the detailed inbound APIs.

Index