API Security Guide
Oracle Banking Electronic Data Exchange for Corporates
Patchset Release 14.7.2.0.0

Part No. F89453-01

November 2023

ORACLE

API Security Guide

November 2023

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax:+91 22 6718 3001

www.oracle.com/financialservices/

Table of Contents

1. About this Manual

1.1 Introduction

Purpose:

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

Audience:

This guide is primarily intended for Developers for Oracle Banking Microservices Architecture and third party or vendor software's. Some information may be relevant to IT decision makers and users of the application are also included. Readers are assumed to possess basic operating system, network, and system administration skills with awareness of vendor/third-party software's and knowledge of Oracle Banking Microservices Architecture application.

1.2 Scope

1.2.1 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.

1.2.2 Understand the Purpose of this Guidance

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

1.2.3 Limitations

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

2. 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 to exchange data. The Oracle Banking Microservices Architecture Service API Gateway will cater to these integration needs.

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

- Inbound application integration – used when any external system needs to add, modify or query information within Oracle Banking Electronic Data Exchange for Corporates.
- Outbound application integration – used when any external system needs to be accessed for processing transactions within Oracle Banking Electronic Data Exchange for Corporates.

2.1 API Security

Oracle Banking Microservices Architecture application provides an API Layer (also known as the Service API Layer) which is used by external consumers to access Oracle Banking Microservices Architecture's 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

As stated before, in case the customer does not have OAM, an enterprise API Management layer should be implemented to protect the service API(s)

2.1.1 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 >>"
        }
        ]
}
```

2.1.2 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>>

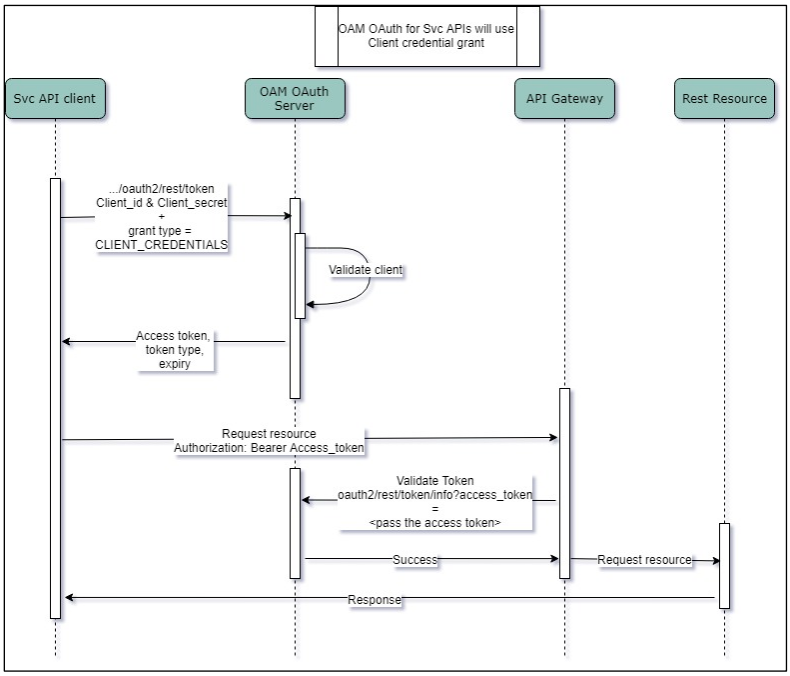
Sample Request Body:

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

2.1.3 API Security with OAuth

2.1.3.1 OAuth with OAM

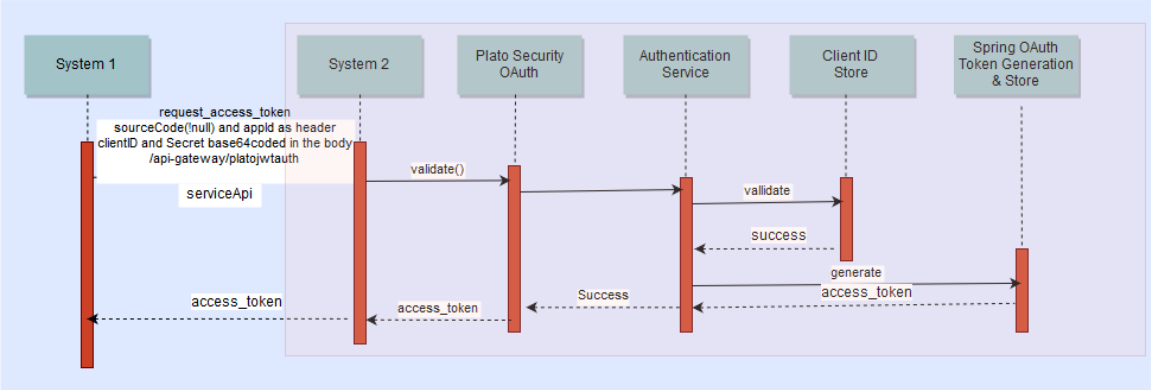
The flow is depicted below



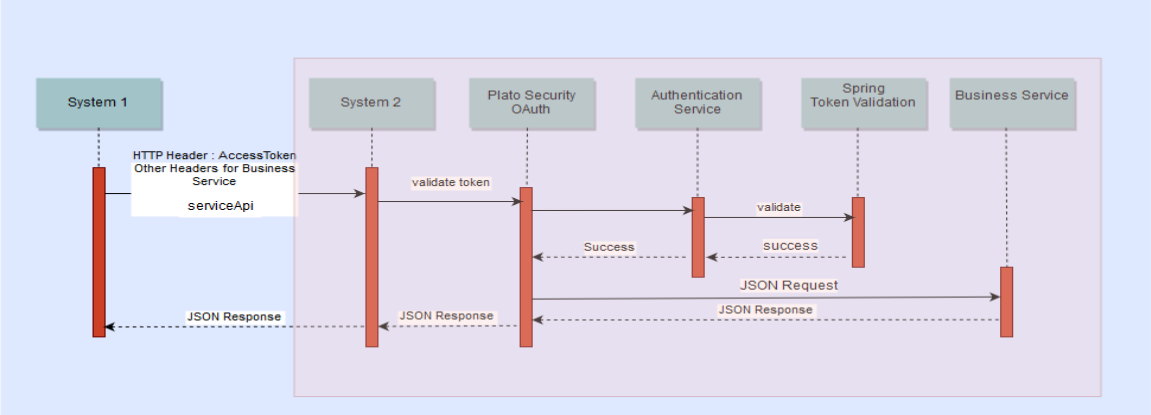
- API clients pass the client id & client secret and grant type as CLIENT CREDENTIALS, to get the access token, using the below endpoint
  - /oauth2/rest/token
- API Clients will pass the access token in the Authorization Header as Bearer token in their subsequent calls to access the Service APIs.
- Plato-Apigateway-router calls API Gateway validates the client access token on OAM Authorization server
- If valid, it passes the request on to the Svc APIs 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.

2.1.3.2 OAuth without OAM

The flow for token generation is depicted below:



The flow for accessing svc is depicted below:



- API clients pass the client id & client secret in the body and other required headers, to get the access token, using the below endpoint:

  http://<<hostname>>:<<port>>/api-gateway/platojwtauth/

- API Clients will pass the access token in the Authorization Header as Bearer token in their subsequent calls to access the Service APIs.
- 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 APIs 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.

2.1.4 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 in **Routing Hub Configuration User Guide** for the further details.

2.2 List of Services

Refer to the <**Product Application Program Interface Guide**> for the detailed inbound APIs.