Oracle® Banking Branch

API Security Guide

14.7.0.0.0
F75182-01
November 2022

Oracle Banking Branch API Security Guide, 14.7.0.0.0

F75182-01

Contents

Preface

This guide provides security-related usage and configuration recommendations for Oracle Banking Branch. It may outline procedures required to implement or secure certain features. This guide is not for general-purpose configuration.

Audience

This guide is primarily intended for Developers of Oracle Banking Branch and the third-party or vendor software. Some information that may be relevant to IT decision-makers and users of the application are also included.

> **Note:**
>
> Readers are assumed to possess the basic operating system, network, and system administration skills with an awareness of vendor/third-party software and knowledge of Oracle Banking Branch application.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Scope

The scope of this guide is as follows:

Table Scope

Scope	Description
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 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 guidelines for developers.

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this guide:

Table Acronyms and Abbreviations

Acronym/Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CSRF	Cross-Site Request Forgery
ECC	Elliptic Curve Cryptography
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
JPQL	Jakarta Persistence Query Language
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
OJET	Oracle JavaScript Extension Toolkit
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
SHA-1	Secure Hash Algorithm 1
SMS	Security Management System
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Algorithm
XSS	Cross Site Scripting

List of Topics

This guide is organized into the following topics:

Table List of Topics

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

1

Securing API Services

Different applications deployed on disparate platforms and using different infrastructure should be able to communicate and integrate seamlessly with the Oracle Banking Branch in order to exchange data.

The Oracle Banking Branch Service API Gateway will 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:

Table 1-1 Integrations

Integration	Description
Inbound Application Integration	This integration is used when any external system needs to add, modify or query information within Oracle Banking Branch.
Outbound Application Integration	This integration is used when any external system needs to be accessed for processing transactions within Oracle Banking Branch.

1.1 API Security

The Oracle Banking Branch provides an API Layer (Service API Layer) for external users to access Oracle Banking Branch 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

> **Note:**
>
> If the customer does not have OAM, an 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

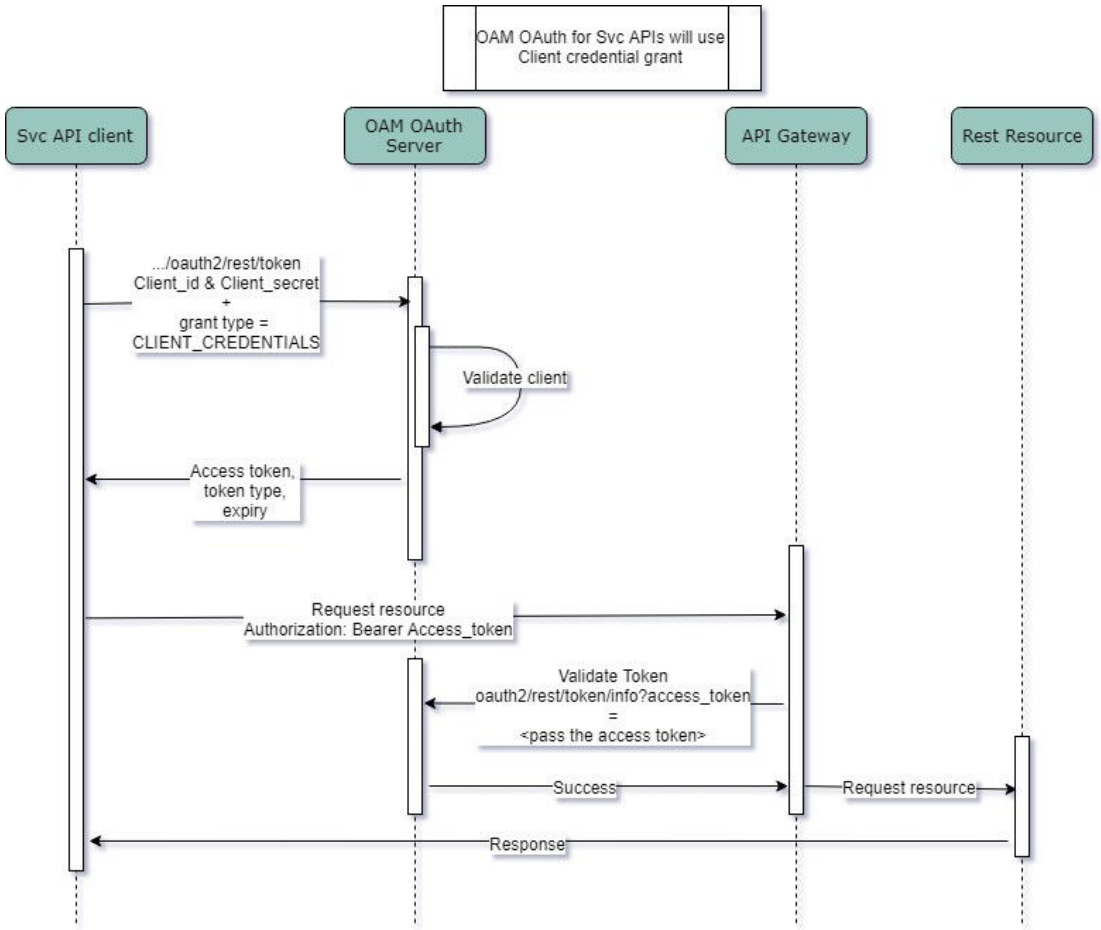
```
{"client_id":"<< clientId >>","validity":"<< Validity in seconds >>"}
```

API Security with OAuth

OAuth with OAM (Oracle Access Manager)

The flow is explained below.

Figure 1-1 OAuth with OAM (Oracle Access Manager)



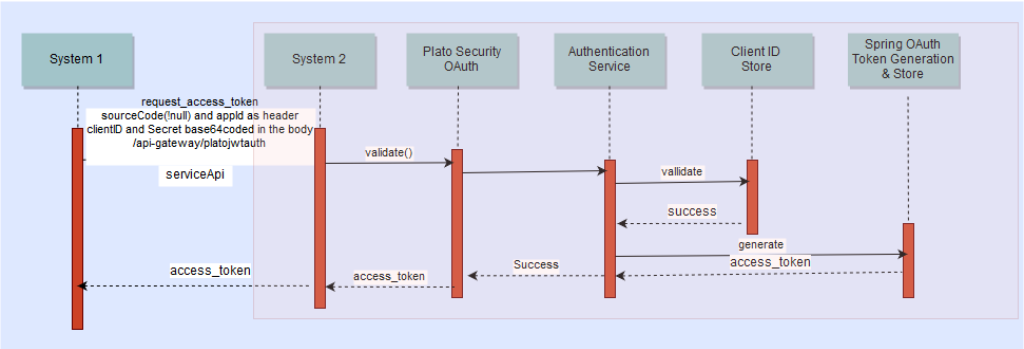
The process flow is as follows:

- API clients pass the client ID and 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 a Bearer token in their subsequent calls to access the Service APIs.
- API Gateway validates the client access token on the 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.

OAuth without OAM

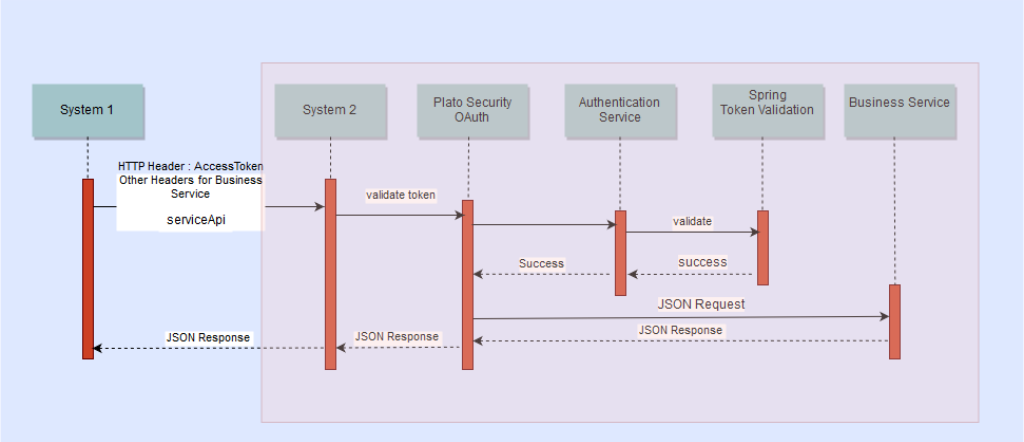
The flow for token generation is depicted below:

Figure 1-2 OAuth without OAM - Token Generation



The flow for accessing SVC is depicted below:

Figure 1-3 OAuth without OAM - Accessing SVC



The process flow is as follows:

- API clients pass the client ID and 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 a Bearer token in their subsequent calls to access the Service APIs.
- API Gateway validates the client access token on the 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 for 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 provides information about the List of API Services.

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