API Security Guide
Oracle Banking Credit Facilities Process Management
Release 14.7.3.0.0

Part Number F95945-01
March 2024

ORACLE
FINANCIAL SERVICES

Table of Contents

1. ABOUT THIS MANUAL 1

1.1 INTRODUCTION 1
1.2 SCOPE 1
1.2.1 Read Sections Completely 1
1.2.2 Understand the Purpose of this Guidance 1
1.2.3 Limitations 1

2. SECURING API SERVICES 2

2.1 API SECURITY 2
2.1.1 Register OAuth Clients with API Gateway 2
2.1.2 Modify Token Expiry of Registered OAuth Client 3
2.1.3 API Security with OAuth 4
2.1.4 Access APIs through Oracle Banking Routing Hub 5
2.2 LIST OF SERVICES 5

1. About this Manual

1.1 Introduction

Purpose:

This guide provides security-related usage and configuration recommendations for Oracle Banking Credit Facilities Process Management. 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 Credit Facilities Process Management 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 Credit Facilities Process Management 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 Credit Facilities Process Management to exchange data. The Oracle Banking Credit Facilities Process Management 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 Credit Facilities Process Management.
- Outbound application integration – used when any external system needs to be accessed for processing transactions within Oracle Banking Credit Facilities Process Management.

2.1 API Security

Oracle Banking Credit Facilities Process Management application provides an API Layer (also known as the Service API Layer) which is used by external consumers to access Oracle Banking Credit Facilities Process Management'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 OAUTH users can be registered with Oracle Banking Credit Facilities Process Management 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>>

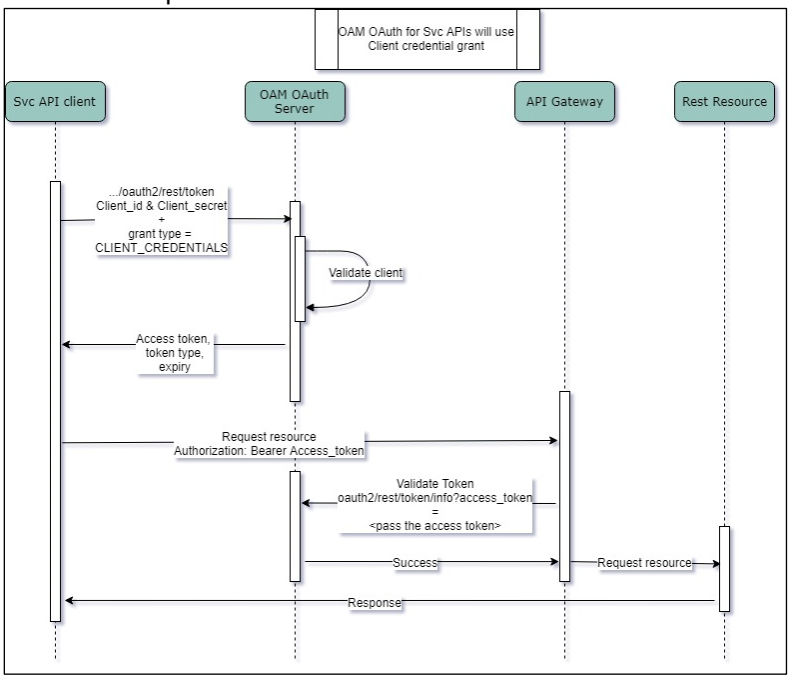
Sample Request Body:

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

2.1.3 API Security with OAuth

2.1.3.1 OAuth with OAM

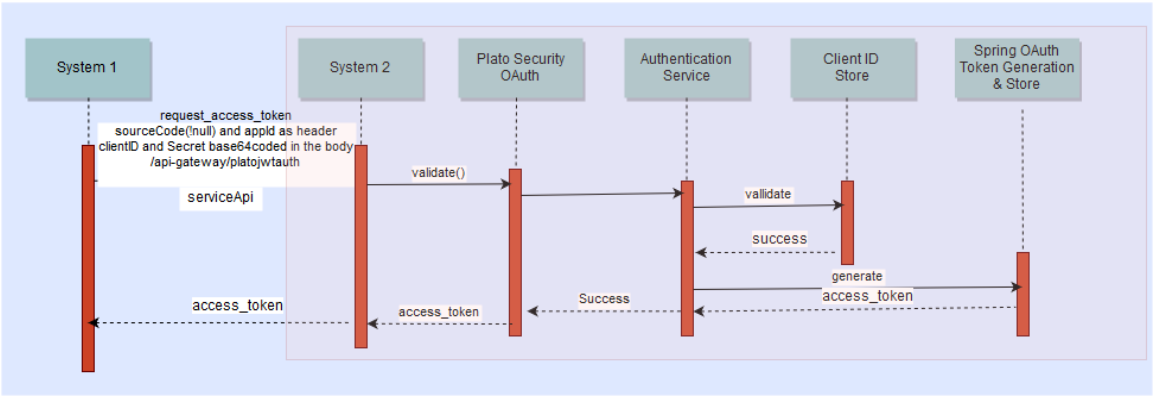
The flow is depicted below



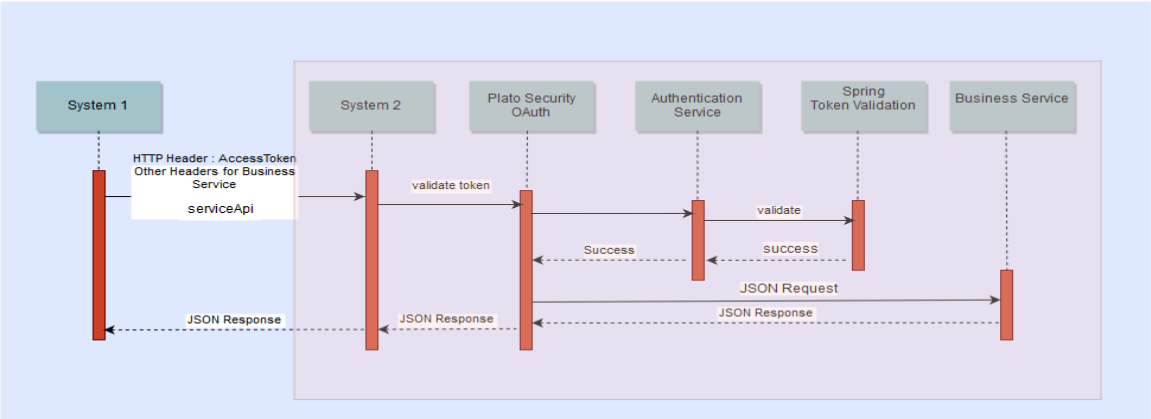
- API clients pass the client id & client secret and grant type as CLIENT CREDENTIALS, to get the access token, using the below endpoint
    - /oauth2/rest/token
- API Clients will pass the access token in the Authorization Header as Bearer token in their subsequent calls to access the Service APIs.
- 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.
- 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 Credit Facilities Process Management, 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

Service End Point	Method Name	Method Type	Description
/service/v1/applicationSubmit	applicationSubmit	POST	To Submit a Credit Application
/service/v1/collateral	createCollateralService	POST	To Submit a Collateral Application

/service/v1/collateral/{collateralId}	UpdateCollateralService	PUT	Update an existing collateral
/service/v1/collateral/{collateralId}	GetCollateralServiceById	GET	Retrieves Collateral by ID
/service/v1/collateral/main/ customer/{customerId}	GetCollateralMainByCustomerId	GET	Retrieves Collateral by Customer Id
/service/v1/releaseCollateral/{collateralId}	createCollateralReleaseRequest	POST	Creates a new Collateral Release Request
/service/v1/reviewCollateral/{collateralId}	createCollateralReviewRequest	POST	Creates a new Collateral Review Request
/service/v1/facility	createFacility	POST	Adds a new Facility Details
/service/v1/facility/{partyId}	getAllFacilities	GET	Retrieves the existing Facility Details for the given party Id
/service/v1/facilityMaintanence	getFacilityMaintenance	GET	To fetch the Facility template tree structure as a list
/web/v1/newFacilityRequest	createNewFacilityRequestDetails	POST	This service will create a new application for Credit Proposal with party, facility and collateral details
/service/v1/amendFacilityRequest	amendNewFacilityRequestDetails	POST	This service will create a new application in Credit Amendment process with an existing party and modified facility and collateral details
/service/v1/facilityClosure	validateAndInitiateClosure	POST	Initiates Facility Closure
/service/v1/review	initiateReview	POST	Initiates Facility Review
/service/v1/cpextension	initiateCPExtension	POST	Initiates Facility Extension
/service/v1/instance	addInstanceMain	POST	Adds a new covenant instance
/service/v1/linkage	AddLinkageMain	POST	Adds a new covenant linkage
/service/v1/linkage/update	UpdateCvntLinkage	PUT	Update an existing Covenant Linkage
/service/v1/cvntlinkage/{applicationNumber}	GetAllLinkagesByPartyId AndAppNumber	GET	Retrieves the list of existing covenant linkages based on application number
/service/v1/applications/{applicationId}	getApplicationDetailsById	GET	Retrieves the application service Details by Application Id
/service/v1/applications/ status/{applicationId}	GetApplicationStatusById	GET	Retrieves the application status details by Application Id

API Security Guide

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

https://www.oracle.com/industries/financial-services/index.html

Copyright © 2019, 2024, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.