

Oracle® Banking APIs Cloud Service

OpenID Guide



Release 25.1.2.0.0

G51558-01

April 2026

ORACLE®

Copyright © 2006, 2026, Oracle and/or its affiliates.

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

| | |
|-----------------------------|----|
| Purpose | i |
| Audience | i |
| Documentation Accessibility | i |
| Diversity and Inclusion | i |
| Conventions | ii |
| Screenshot Disclaimer | ii |
| Acronyms and Abbreviations | ii |

1 OPENID

| | | |
|-----|--|---|
| 1.1 | Discovery/Well-known Endpoint Properties | 1 |
| 1.2 | DCR (Dynamic Client Registration) Properties | 2 |
| 1.3 | userinfo Properties | 3 |

2 MESSAGE SIGNING AND VALIDATION

| | | |
|-----|----------------------|---|
| 2.1 | Authorization Server | 1 |
| 2.2 | Resource Server | 1 |

3 HANDLERS

| | | |
|-----|----------------------|---|
| 3.1 | Authorization Server | 1 |
| 3.2 | Resource Server | 1 |

Index

Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)

Purpose

This guide is designed to help acquaint you with the Oracle Banking application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

Audience

This document is intended for the following audience:

- Customers
- Partners

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and

the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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. |
| <i>italic</i> | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| <code>monospace</code> | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

Table 1 Acronyms and Abbreviations

| Abbreviation | Description |
|--------------|---|
| OBDXCS | Oracle Banking Digital Experience Cloud Service |

1

OPENID

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

OBAPI has following configurations which when altered will affect the behavior of OpenID in various ways :

- [Discovery/Well-known Endpoint Properties](#)
- [DCR \(Dynamic Client Registration\) Properties](#)
- [userinfo Properties](#)

1.1 Discovery/Well-known Endpoint Properties

These properties contain the information about the URLs and certain parameters supported by ASPSP that needs to be displayed to the TPP when requested. The information is displayed through discovery endpoint.

Table: DIGX_FW_CONFIG_ALL_B

Category-Id : OAuthDiscoveryEndpointConfig

| Property ID | Description | Property Value |
|------------------------|---|---|
| issuer | This parameter represents Issuer's endpoint. | * {{ISSUER'S_URL}} Example:https:// server.example.com |
| authorization_endpoint | This parameter represents ASPSP's authorization endpoint. | * {{AUTHORIZATION_ENDPOINT_URL}} Example:https:// server.example.com/ connect/authorize |
| token_endpoint | This parameter represents ASPSP's token endpoint. | * {{TOKEN_ENDPOINT_URL}} Example:https:// server.example.com/ connect/token |
| userinfo_endpoint | This parameter represents ASPSP's userinfo endpoint. | * {{USERINFO_ENDPOINT_URL}} Example:https:// server.example.com/ connect/userinfo |
| jwks_uri | This parameter represents ASPSP's jwks uri. | * {{JWKS_URI}} Example:https:// server.example.com/ jwks.json |

| Property ID | Description | Property Value |
|--|--|---|
| registration_endpoint | This parameter represents ASPSP's Dynamic Client Registration endpoint. | * { {REGISTRATION_ENDPOINT_URL} } Example:https://server.example.com/connect/register |
| response_types_supported | This parameter represents ASPSP's supported response Types | code,code token,code id_token,code token id_token |
| grant_types_supported | This parameter represents ASPSP's supported grant types. | AUTHORIZATION_CODE,PASSWORD,CLIENT_CREDENTIALS,REFRESH_TOKEN |
| subject_types_supported | This parameter represents ASPSP's supported subject type. | public |
| id_token_signing_alg_values_supported | This parameter represents ASPSP's supported id_token signing algorithm. | RS256,PS256 |
| request_object_signing_alg_values_supported | This parameter represents ASPSP's supported request object signing algorithm. | RS256,PS256 |
| token_endpoint_auth_methods_supported | This parameter represents ASPSP's supported token endpoint authentication methods. | client_secret_basic |
| identityDomain | This parameter represents the default configured Identity Domain. | * { { IDENTITY_DOMAIN_NAME } } Example:UKOPENBANKING |
| token_endpoint_auth_signing_alg_values_supported | This parameter represents ASPSP's supported token endpoint auth signing algorithm supported. | RS256,PS256 |
| claims_parameter_supported | This parameter represents whether the 'claims' parameter is supported or not by ASPSP. | Value can be true or false |
| request_parameter_supported | This parameter represents whether the 'request' parameter is supported or not by ASPSP. | Value can be true or false |
| tls_client_certificate_bound_access_tokens | This parameter represents whether the TLS client certificate bound access tokens is supported or not by ASPSP. | Value can be true or false |
| claims_supported | This parameter represents ASPSP's supported claims. | acr,openbanking_intent_id |

1.2 DCR (Dynamic Client Registration) Properties

These properties contain the parameters related to Dynamic Client Registration.

Table: DIGX_FW_CONFIG_ALL_B

Category-Id : OAuthDCRConfig

| Parameter | Description | Property Value |
|-----------------|---|---|
| client_Type | This parameter represents the default configured Client Type. | CONFIDENTIAL_CLIENT |
| resource_server | This parameter represents the default configured Resource Server. | *{{ RESOURCE_SERVER_NAME }} Example: AIPISP2 |

1.3 userinfo Properties

These properties represent the mapping of OpenID claims to the corresponding claims available from user details in OBAPI. The parameter is the OpenID claim while it's value is the corresponding claim available from user details in OBAPI.

Any new parameter and its OBAPI counterpart can be configured by adding in below Table and Category-Id.

Table: DIGX_FW_CONFIG_ALL_B

Category-Id :OAuthUserInfoConfig

| Property ID | Description | Property Value |
|--------------|---|----------------|
| sub | This parameter represents Subject. | userName |
| name | This parameter represents User's name. | userName |
| given_name | This parameter represents User's given name. | firstName |
| family_name | This parameter represents User's family name. | lastName |
| middle_name | This parameter represents User's middle name. | middleName |
| email | This parameter represents User's email. | emailId |
| birthdate | This parameter represents User's date of birth. | dateOfBirth |
| phone_number | This parameter represents User's phone number. | phoneNumber |
| address | This parameter represents User's address. | address |

* – These values are a part of Day one configurations and are not factory shipped. These values are mandatory and if not provided will result in error.

2

MESSAGE SIGNING AND VALIDATION

OBAPI has message signing and validation configurations, which when altered will affect the response of Open Banking API's.

- [Authorization Server](#)
- [Resource Server](#)

2.1 Authorization Server

Table: DIGX_FW_CONFIG_ALL_B

Category-Id :OAuthUserInfoConfig

| Property ID | Description | Property Value |
|--------------------|---|---|
| oauthHandlerConfig | <p>This parameter is responsible for choosing the required Handler. The Parameter's value is the fully qualified name of the Handler Class.</p> <p>The handler is responsible for implementing methods/ validations that are over and above OpenID methods/ validations. By default DefaultOAuthHandler is used. It contains the methods to validate request Object Claims, fetch public key and private key, etc.</p> <p>UKOAuthHandler extends DefaultOAuthHandler and overrides the methods to implement the UK OpenBanking specific validations.</p> <p>Any new Handler to be written for UK OpenBanking should extend UKOAuthHandler and override the methods and the fully qualified name of the Handler should be given against this oauthHandlerConfig parameter.</p> | <p>*</p> <p>{{FULLY_QUALIFIED_HANDLER_CLASS_NAME}}</p> <p>Example:</p> <p>com.ofss.digx.app.sms.handlers.oauth.openid.uk.UKOAuthHandler</p> |

* – These values are a part of Day one configurations and are not factory shipped. These values are mandatory and if not provided will result in error.

2.2 Resource Server

Below are the properties required to be updated in the UK Open Banking. Please find the below properties, its purpose and OOTB values.

Table: DIGX_FW_CONFIG_ALL_B

Category-Id : OpenBankingConfig

| Property ID | Property Value(Out of the Box) | Purpose |
|---------------------------|--------------------------------|---|
| MESSAGE_SIGNATURE_HANDLER | - | <p>This property is responsible for choosing the required Handler. The Parameter's value is the fully qualified name of the Handler Class.</p> <p>The handler is responsible for implementing methods/ validations of OpenBanking. By default DefaultMessageSignatureHandler is used. It contains the methods to validate jwt token headers, fetch public key and private key, etc.</p> <p>Any new Handler to be written for UK OpenBanking should extend DefaultMessageSignatureHandler and override the methods and the fully qualified name of the Handler should be given against this property Id and committed in database.</p> <p>Example Query :</p> <pre> Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER) values ('MESSAGE_SIGNATURE_HANDLER', 'openBankingConfig','com .ofss.digx.appx .openbanking.uk.message. signature .handler.UKMessageSignat ureHandler', 'N',null,'Message signature handler','ofssuser', sysdate,'ofssuser',sysda te,'A',1); </pre> |

| Property ID | Property Value(Out of the Box) | Purpose |
|-------------------------|--------------------------------|---|
| MESSAGE_ENCRYPTION_FLAG | Y | <p>Flag to enable or disable the Message Signing and Validation.</p> <p>Set 'Y' to enable and 'N' to disable message signing and validations.</p> <p>Example Query :</p> <pre> "Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG,PRO P_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE,OBJECT _STATUS, OBJECT_VERSION_NUMBER) values ('MESSAGE_ENCRYPTION_FLA G','openBankingConfig', 'Y','N',null,'Open Banking payload signing and validation flag','ofssuser',sysdate ,'ofssuser',sysdate,'A', 1);" </pre> |

* – These values are a part of Day one configurations and are not factory shipped. These values are mandatory and if not provided will result in error.

3

HANDLERS

Handlers for OpenBanking provide extensibility. The following are the two sets of Handlers which can be utilised directly or can be extended to implement custom functionality.

- [Authorization Server](#)
- [Resource Server](#)

3.1 Authorization Server

The handler on Authorization Server is responsible for implementing methods/validations that are over and above OpenID methods/validations.

- If no configuration is provided, DefaultOAuthHandler is used by default. It contains the methods to validate request Object Claims, fetch public key and private key, etc.
- UKOAuthHandler extends DefaultOAuthHandler and overrides the methods to implement the UK OpenBanking specific validations.

Note

Any new Handler to be written for UK OpenBanking should extend UKOAuthHandler and override the required methods. Also the fully qualified name of the Handler should be given against this oauthHandlerConfig parameter.

3.2 Resource Server

The handler on Resource Server is responsible for implementing methods/validations of OpenBanking.

- If no configuration is provided, DefaultMessageSignatureHandler is used by default. It contains the methods to validate jwt token headers, fetch public key and private key, etc.

Note

Any new Handler to be written for UK OpenBanking should extend DefaultMessageSignatureHandler and override the required methods. Also the fully qualified name of the Handler should be given against MESSAGE_SIGNATURE_HANDLER property Id and committed in database.

Index

A

Authorization Server, [1](#), [1](#)

D

DCR (Dynamic Client Registration) Properties, [2](#)
Discovery/Well-known Endpoint Properties, [1](#)

H

HANDLERS, [1](#)

M

MESSAGE SIGNING AND VALIDATION, [1](#)

O

OPENID, [1](#)

R

Resource Server, [1](#), [1](#)

U

userinfo Properties, [3](#)