

UK Open Banking Consent Management User Guide
Oracle Banking Digital Experience
Patchset Release 22.2.5.0.0

Part No. F72987-01

October 2024

UK Open Banking Consent Management User Guide

October 2024

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/

Copyright © 2006, 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.



Table of Contents

1. Preface	1-1
1.1 Purpose	1-1
1.2 Audience	1-1
1.3 Documentation Accessibility	1-1
1.4 Critical Patches	1-1
1.5 Diversity and Inclusion	1-1
1.6 Conventions	1-1
1.7 Screenshot Disclaimer	1-2
1.8 Acronyms and Abbreviations	1-2
2. Open Banking Functional Overview	2-1
2.1 Open Banking functionality for UK Open Banking standards	2-1
3. UK Open Banking	3-1
3.1 TPP registration	3-1
3.2 Consent Management	3-2
3.3 Consent Capture	3-2
3.4 Consent Listing	3-4
3.5 Consent Revocation	3-5
3.6 Revoke Access for TPP	3-5
3.7 Manage Tokens	3-7
3.8 UK Open Banking APIs	3-9
4. References	4-1

1. Preface

1.1 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

1.3 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.

1.4 Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at [Critical Patches, Security Alerts and Bulletins](#). All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by [Oracle Software Security Assurance](#).

1.5 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.

1.6 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.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1.7 **Screenshot Disclaimer**

The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

1.8 **Acronyms and Abbreviations**

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

2. Open Banking Functional Overview

To read this document, understanding the following terms is important:

ASPSP – Account Service Payment Service Provider. Generally, these are the banks and other Financial Institutions that have the customer data

TPP – Third Party Provider. A player of the Open Banking ecosystem that gets data from the ASPSPs

AISP – Account Information Service Provider. It is a type of TPP

PISP – Payment Initiation Service Provider. It is a type of TPP

PSU – Payment Service User. These are the customers of ASPSPs

2.1 Open Banking functionality for UK Open Banking standards

As a part of this module, OBDX and OBAPI support the following features (the exact functionality for each standard is mentioned in the respective sections)

1. TPP registration
2. Consent Management
 - a. Consent Capture
 - b. Consent listing
 - c. Consent revocation
3. Open Banking APIs as per the respective regulatory requirements
 - a. Retail APIs
 - b. Corporate APIs

This document covers details of the above features and has references to other documents that contain more details on the topic.

3. UK Open Banking

3.1 TPP registration

To enable Open Banking, TPP needs to register with OBDX. For this, the following steps are necessary:

- Identity Domain Maintenance
- Resource Server Maintenance
- Client Maintenance

For further information, please refer to the OBAPI Core manual at:

ORACLE BANKING APIS BASE -> Core.pdf

Section Name: OAuth 2.0

3.2 Consent Management

3.3 Consent Capture

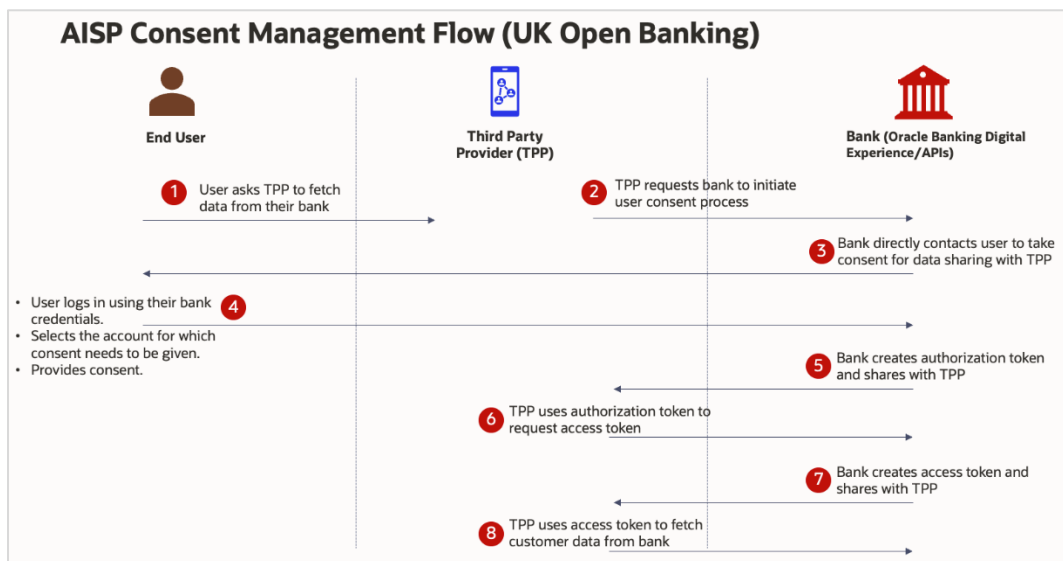
OBDEX/ OBAPI support APIs as well as UX for Payment Service User (PSU) consent capture for a request from Third Party provider (TPP)

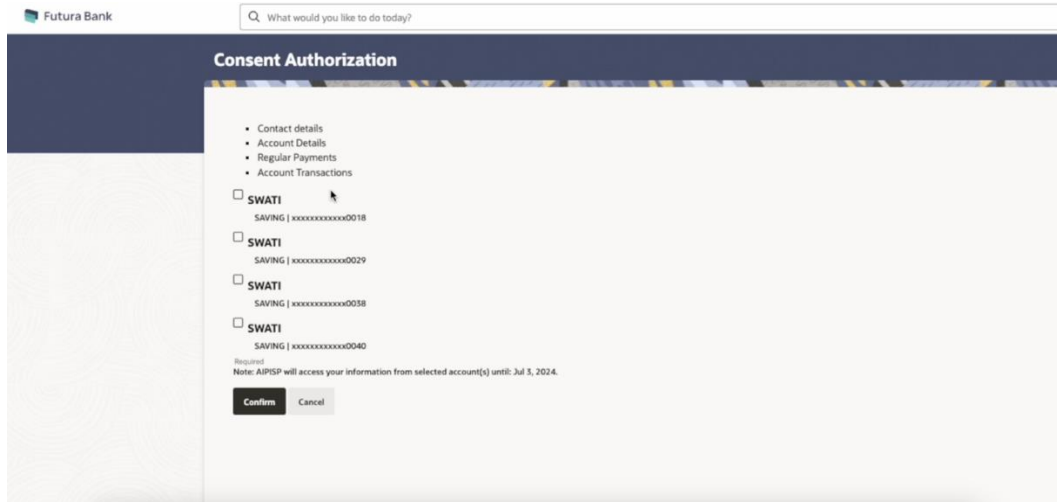
Prerequisite: TPP has registered with the ASPSP as a client to avail UK Open Banking services.

AISP Flow:

1. During data request, TPP contacts ASPSP with their credentials
2. ASPSP then directly contacts PSU to acquire consent for sharing the data with the TPP
3. During this process, PSU sees the list of accounts that they have with the ASPSP and then selects the account for which the consent needs to be given
4. Once consent is given by the PSU to ASPSP, ASPSP generates an authorisation token and shares the same with the TPP
5. TPP uses this authorisation token and gets the access token from the ASPSP
6. TPP can use this access token to access customer's data for the specified time

Note: In UK Open Banking an Account is identified using the Sort Code and Account number combination.

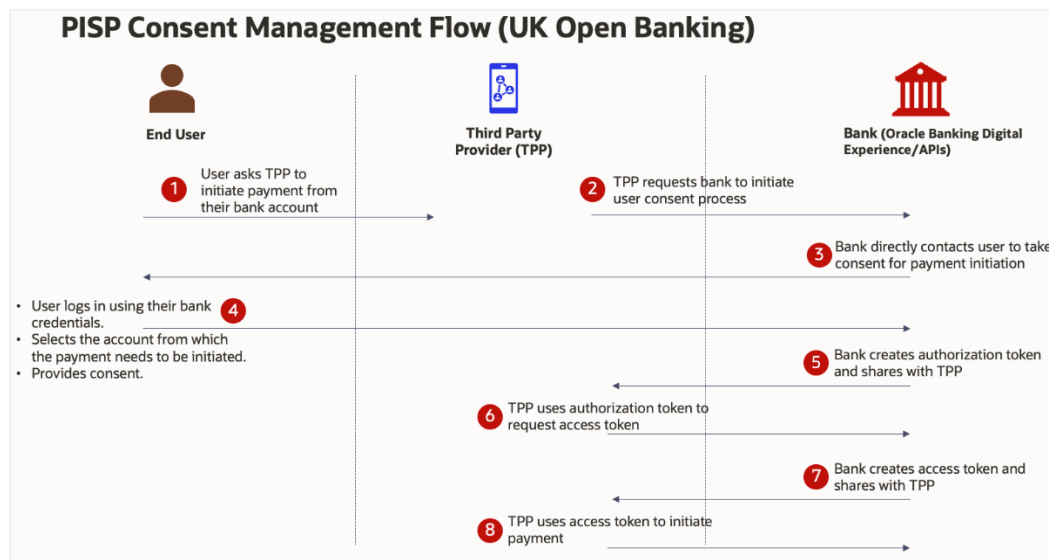




AISP Consent Capture Screen - UK Open Banking

PISP Flow:

1. During payment initiation request, TPP contacts ASPSP with their credentials and payment details
2. ASPSP then directly contacts PSU to acquire consent for allowing payment initiation from their accounts.
3. During this process, the PSU sees the list of accounts that they have with the ASPSP and then selects the account from which the payment needs to be initiated.
4. Once consent is given by the PSU to ASPSP, ASPSP generates an authorisation token and shares the same with the TPP
5. TPP uses this authorisation token and gets the access token from the ASPSP
6. TPP uses this access token to initiate the payment



PISP Consent Capture Screen with Account Selection - UK Open Banking)

Futura Bank

What would you like to do today?

Confirm Payment Account

- ☐ main Account Vashi
SAVING | xxxxxxxxxxxx0056
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0080
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0047
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0078
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0069
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0014
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0058
- ☐ SWATI THITE
SAVING | xxxxxxxxxxxx0158

Required

3.4 Consent Listing

PSU can log in to the internet/ mobile banking application of the ASPSP and see the list of consents that they have provided to various TPPs.

How to reach here:

Dashboard > Toggle Menu > Menu > Account Settings > Access & Consent > Manage Consents
OR
Dashboard > My Profile icon > Settings > Access & Consent > Manage Consents

Expiration Date Table

Search

Roger Bohr

- Passwords & Security
- Device Registration
- Preferences
- Access & Consent**
- Alerts

Manage Consents

Access Point: AIPSP

336 Record(s)

Consent ID	Consent Type	Creation Date	Expiration Date
r3ggugq2iap9fdd	Accounts	1/9/2023, 9:19 AM	12/30/2023, 12:00 AM
l2tzbhd001kysy	Accounts	1/10/2023, 9:15 AM	12/30/2023, 12:00 AM
uma6p20548yxp04	Accounts	1/9/2023, 3:35 AM	12/31/2023, 12:00 AM
9sl1sdj3nt2vs26z	Accounts	1/9/2023, 9:03 AM	12/30/2023, 12:00 AM
ltbwchetymdrdht	Accounts	1/9/2023, 9:05 AM	12/30/2023, 12:00 AM
y1f3chmif16pyv5r	Accounts	1/11/2023, 4:09 AM	12/30/2023, 12:00 AM
giqaklqnsqvexz	Accounts	1/11/2023, 5:07 PM	12/30/2023, 12:00 AM
ep4pcb7qys87y7g	Accounts	1/12/2023, 4:46 AM	12/30/2023, 12:00 AM
bkjlnr5ltzpbftti	Accounts	1/12/2023, 5:38 AM	12/30/2023, 12:00 AM
jcnody8l8kue4d5	Accounts	1/12/2023, 6:29 AM	12/30/2023, 12:00 AM
85to7l01q694layc	Accounts	1/12/2023, 7:18 AM	12/30/2023, 12:00 AM
bcujmq1vo0haq4c1	Accounts	1/12/2023, 7:41 AM	12/30/2023, 12:00 AM
fvhw775xd5v74xl	Accounts	1/12/2023, 10:36 AM	12/30/2023, 12:00 AM
eyl68lqr1g9lsn	Accounts	1/9/2023, 5:38 AM	12/30/2023, 12:00 AM

3.5 Consent Revocation

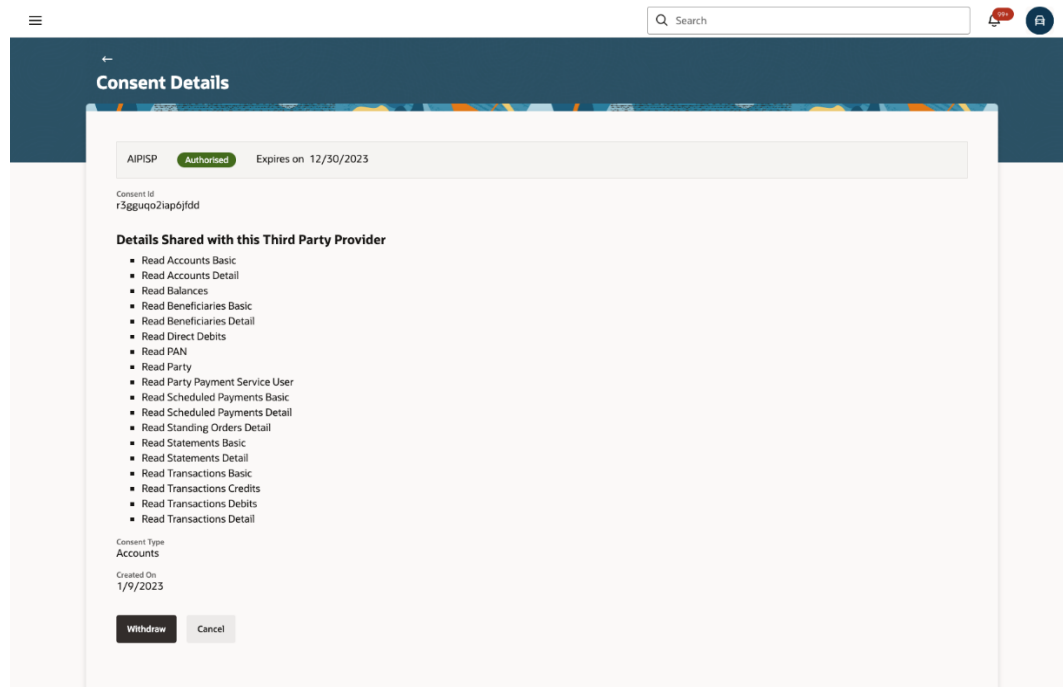
PSU can log in to the internet/ mobile banking application of the ASPSP and see the list of consents that they have provided to various TPPs.

How to reach here:

Dashboard > Toggle Menu > Menu > Account Settings > Access & Consent > Manage Consents
OR

Dashboard > My Profile icon > Settings > Access & Consent > Manage Consents

From the list of Consents, the PSU can see the details of Consent and can revoke the same.



3.6 Revoke Access for TPP

Through this section, user can revoke the access that they have provided to various Third party Service Providers to access their account data and to initiate payments.

How to reach here:

Dashboard > Toggle Menu > Menu > Account Settings > Access & Consent > Revoke Access
OR

Dashboard > My Profile icon > Settings > Access & Consent > Revoke Access

Revoke Access

Revoke Action

Rogerr Bohr

Passwords & Security

Device Registration

Preferences

Access & Consent

Alerts

Revoke Access

Client Type

AISP

CBPii

Select Account

xxxxxxxxxxxx9802

Current Balance : €9,622,140.80

Submit

Your connected service providers

You have provided permissions for these service providers to access data from your account

Select a provider to manage

19 Record(s)

Manage Columns

Client Name	Account Number	Sort Code	Access Range	Action
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	5/31/2024 To 7/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/6/2024 To 7/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/14/2024 To 6/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/14/2024 To 6/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/14/2024 To 6/30/2024	Manage
UKClient	xxxxxxxxxxxx9802	HEL	9/29/2024 To 12/2/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	2/8/2024 To 3/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	5/31/2024 To 7/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/6/2024 To 7/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	6/18/2024 To 6/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	7/5/2024 To 7/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	7/8/2024 To 7/30/2024	Manage
Test TPP3 <div>Expired</div>	xxxxxxxxxxxx9802	HEL	8/20/2024 To 8/30/2024	Manage
UKClient <div>Expired</div>	xxxxxxxxxxxx9802	HEL	5/25/2024 To 6/30/2024	Manage

Manage Third Party Provider Access

Service Provider Details

UKClient

Account Status

Expired

The data we access

Contact details

Account Details

Regular Payments

Statements

Account Transactions

You started sharing your data on

5/31/2024

Access to this data expires

7/30/2024

You should contact UKClient to fully understand the implication of withdrawing access.

Back

Cancel Permission

Field Description

Field Name	Description
Third Party Application Name	The names of the third party applications are displayed. Select a third party application to define access to the application.
Current and Savings/ Term Deposits/ Loans and Finances	Select a product to define account and transaction level access to the third party.
Select Accounts	Select the account to provide the account and transaction level access to the third party.
Transactions	Once you select an account, all the transactions through which the account can be accessed are displayed. Select any or all transactions to provide account access for the transactions to the third party application.

1. Select the third party application for which you wish to define fine grained access. The system will display the list of accounts under each of the account types along with the transactions.
2. From **Select Account** list, select the account to provide the account and transaction level access to the third party.
3. Click **Submit**.
OR
Click **Back** to navigate back to previous page

3.7 Manage Tokens

The consents and access to Third Parties are provided on the basis of Access Tokens. Each Third Party is given an Access Token by the bank to access customer's data.

Through this section, these Access Tokens can be managed.

How to reach here:

Dashboard > Toggle Menu > Menu > Account Settings > Access & Consent > Manage Tokens
OR
Dashboard > My Profile icon > Settings > Access & Consent > Manage Tokens

Manage Tokens

The screenshot displays the 'Manage Tokens' page in the Futura Bank settings. On the left, the 'Access & Consent' menu item is highlighted. The main content area shows the 'Manage Tokens' section with the 'Access Token' radio button selected. Below this is a dropdown menu labeled 'Please Select Client Name' with 'AIPISP' chosen. There are 'Search' and 'Clear' buttons. A table lists issued tokens with columns: 'Issued At', 'Expires At', 'Type Of Access', and 'Status'. The table contains five rows of data, each with a 'Revoke' link in the status column.

Issued At	Expires At	Type Of Access	Status
2/6/2023	2/6/2023	Accounts Inquiry	Revoke
2/10/2023	2/10/2023	Funds Check	Revoke
2/10/2023	2/10/2023	Accounts Inquiry	Revoke
2/10/2023	2/10/2023	Accounts Inquiry	Revoke
2/10/2023	2/10/2023	Accounts Inquiry	Revoke

Field Description

Field Name	Description
Token Type	Displays the token type i.e. Access Token or Refresh Token of the client whose information need to be access from the resource server.
Please Select Client Name	The Client Name if the client needs to be searched based on client name.

2. In the **Token Type** field, select the token of the client whose information need to be access from the resource server.
3. From the **Please Select Client Name** list, select the appropriate client to be searched

3.8 UK Open Banking APIs

- OBAPI supports APIs of the UK Open Banking standard's version 3.1.10.
- The list of the APIs supported in OBAPI can be found in this document - UK Open Banking APIs - OBAPI v22.2.5.0.0.pdf
- Support is available for Retail as well as Corporate persona for Account Information Services and Payment Initiation Services including approval support for payments

4. References

For further details on the Berlin Group Open Banking configuration, refer to the following OBAPI user manual: **UK Open Banking Configuration Guide.pdf**