# Scope

Under Payment Services Directive II Regulatory Technical Standards (PSD2 RTS) requirements there is a need for common and secure open standards of communication. As a result, Reliance Bank has published its modified customer interfaces (MCI) which will enable its customers to share their balance and transaction history with regulated Third Party Providers (TPPs) and enable them to make payments from their accounts.

This document is designed to assist TPPs and will provide details about Reliance Bank's MCI as well as outlining how a TPP would gain access to this interface.

# What is the modified customer interface?

As per PSD2 SCA RTS regulation, from 14 September 2019 ASPSPs (Account Servicing Payment Service Providers) are required to provide TPPs with access to at least one interface which enables TPPs to identify themselves towards the ASPSP. The RTS allows this to be via a dedicated interface or by allowing TPPs the use of the interfaces used for authentication and communication with our customers.

The modified customer interfaces we provide enables you to present a valid, OBIE issued eIDAS certificate to identify yourself and you are then able to access the specific services you require.

We provide a test facility (sandbox) to enable you to perform functional and connectivity testing of your applications and software by following customer authentication and online banking journeys for account information and payment initiation services. Information on how to access this, and also fuller technical documentation, is provided below.

## Connecting to the MCI

Reliance Bank uses the Open Banking UK Directory provided QTSPs list and the CRL list for TPPs regulatory status check for Production. TPPs that wish to connect with the Reliance Bank MCI Sandbox should register themselves with Open Banking Directory and get OBWAC from OBIE Test Directory.

Reliance Bank provides a MCI Sandbox environment to allow TPPs to connect to its Screen Scraping Plus integration. The Reliance Bank Sandbox environment can be connected to using OBWAC issued by the Open Banking Directory Sandbox environment. Reliance Bank also supports QWAC issued by QTSPs.

To register with us to use the Reliance Bank sandbox you will need to be authorised or registered, (as appropriate),

- By a competent authority; in the UK this is the FCA,
- As an AISP, PISP or CBPII,
- Or to have applied to the FCA or a comparable competent authority for the relevant authorisation.

### Registration process:

Contact us via info@reliancebankltd.com. Our support team will guide you in more detail through the process and the information we will need you to provide.
Information we will need from you as a TPP includes:

- Your company name and contact details
- Your competent authority registration number (or application reference)
- Your company's legal address
- Your TPP role - Account Information Service Provider (AISP), Payment Initiation Service Provider (PISP), Card based Payment Instrument Issuer (CBPII)
- Provide information about your interest to connect with Personal or Business Banking

Once the sandbox registration process is complete you will be provided with the following to support your sandbox access and use:

- The technical specifications for the modified customer interface
- A URL specific to you via which to access the sandbox
- Instructions giving you the information you need to access and use the sandbox

## Strong Customer authentication (SCA) & Channel Secure Communication (CSC)

As a TPP, to register for use of our customer modified interfaces you will need to be registered by a competent authority (the FCA in the UK), as an AISP, PISP or CBPII.

You will need to provide us with company information and a valid, OBIE issued eIDAS certificate in order for us to confirm your status as registered.

Once registered for access to the customer modified interfaces you will need to provide your certificate each time you access the interface.

### Customer Authentication

Access to customer modified interfaces requires the entry of login credentials supplied by customers. Except where exemptions are applied, the login credentials will include two-factor authentications in line with regulatory requirements for SCA. Information is provided in the technical specifications on the means to step up security and where exemptions to SCA are being applied by the Bank. Reliance Bank uses SMS or EMAIL mechanisms to provide SCA for its Customers for both Personal and Business Banking.

### Channel Secure Communication

Reliance Bank support QWAC & OB WAC certificates for TPP access and authorisation checks. Reliance Bank MCI only allows mutual authentication if the TPP provided certificate is valid at the time of connection. If the TPP certificate is revoked or expired Reliance Bank will deny the mutual authentication request for the MCI endpoints. The Reliance Bank endpoint is protected by standard server certificates signed by Root Certification Authority:
CN = Starfield Secure Certificate Authority - G2
OU = http://certs.starfieldtech.com/repository/

Reliance Bank provides Personal and Business banking from a single core system hence only single MCI endpoints are required to interact with both types of customer payment accounts.

## URLs for MCI

SANDBOX: https://mcitest.reliancebankltd.com/Logon.aspx

**PROD:** https://mci.reliancebankltd.com/Logon.aspx

## Contact us

To register for access to the sandbox or to ask a question about our open banking access provision for TPPs please contact us at info@reliancebankltd.com.

# Glossary & PSD2 RTS Sections

| Abbreviation | Description |
|---|---|
| MCI | Modified Customer Interface |
| AISP | Account Information Service Provider |
| ASPSP | Account Servicing Payment Service Provider |
| eIDAS | The eIDAS Regulation is an EU Regulation that sets out rules for electronic identification and trust services. |
| FCA | Financial Conduct Authority |
| OBIE | Open Banking Implementation Entity |
| PISP | Payments Initiation Service Provider |
| PSD2 | Second/Revised Payment Services Directive (Directive (EU) 2015/2366) |
| SCA RTS | COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication |
| SS+ | Screen Scraping Plus |
| TPP | Third Party Provider |
| QWAC | eIDAS Website Certificate issued by QTSP |
| OBWAC | Open banking UK Ltd issued certificate |

As stated in The Payment Services Regulations 2017 and COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing

Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication