CASE STUDY

macro global®
creating value through innovation

# Fallback Solution – Modified Customer Interface

## Synopsis

According to Open Banking regulations, financial institutions (ASPSP) supporting payment account services must develop at least one interface for identification and secure communication with third-party providers (TPPs). ASPSPs can opt to offer a dedicated channel based on Application Programming Interface standards (APIs) or a Modified Customer Interface (MCI).

In this case study, we will discuss how Macro Global supported the financial institution to build a Modified Customer Interface solution enabling third-party providers to access the customer online payment accounts via Internet Banking channel in accordance with the requirements of Open Banking Regulations.

## Background

Financial institutions are combating the battle with complex Dedicated interfaces (API) and most banks have slipped the deadline. Unless banks in the UK have explicitly received a fallback interface exemption from their National Competent Authority (NCA), banks face the obligation to provide a Modified Customer Interface (MCI) for third-party providers in addition to the dedicated API interface. As per European Banking Authority (EBA) guidelines, fallback exemption criteria have been stringent and in order to comply with Open Banking RTS, banks should provide a strategic MCI solution as Fallback to the dedicated interface. On the other hand, financial institutions who have not published a dedicated API interface can develop the Modified Customer Interface solution as a fast means to comply.

Financial institutions (ASPSP) can decide whether to provides access to third-party providers (TPPs) through a dedicated interface or a modified version of the customer interface. If an ASPSP permits access to TPPs via a dedicated interface, Article 33(1) of RTS mandates the integration of contingency measures which should be triggered in the event of:

- Non-compliant performance of the interface; or
- Unplanned unavailability, a systems breakdown (when five consecutive requests for access to information for the provision of confirmation of funds or payment initiation services or account information services are not replied to within 30 seconds).

The contingency mechanism provides access using a modified version of the customer interface i.e., the non-dedicated channel (Internet Banking). If the third-party provider (TPP) cannot access the customer's designated payment account via the dedicated interface, as an alternative TPP must be enabled to access the information through the modified customer interface (MCI) until the dedicated interface is restored. The MCI solution must meet the requirements mandated for access interfaces when functioned as a contingency mechanism.

## Contingency Mechanism Outlook

Consistent with Open Banking Implementation Entity (OBIE) standards, financial institutions (ASPSPs) are likely to implement the Contingency Mechanism.

- If ASPSPs does not provide a Dedicated Interface at all.
- If ASPSPs do provide a Dedicated Interface but chose not to apply for an exemption from their National Competent Authority (NCA).
- If ASPSPs provide a Dedicated Interface but does not meet the RTS requirements for availability and performance (even if they have initially gained an exemption).
- If ASPSPs gain an exemption, but voluntarily chose to provide a Contingency Mechanism.

The contingency mechanism requirements are intended to ensure that third-party providers (TPPs) are redirected to the ASPSPs Internet Banking channel to access the information through the online interface the customers (PSUs) have with their ASPSP if an AISP/PISP/CBPII cannot access a customer's payment account via the dedicated interface due to unplanned unavailability of the dedicated API interface or system breakdown. Reliance on the contingency mechanism should be a temporary measure until the dedicated interface is restored to the required level of availability and performance as per the RTS Standards.

To comply with RTS requirements and to ensure continued performance in the event of failure, one of our clients who is a foreign bank in the UK opted to design the contingency measures which also serves as a 'Fallback' solution in case there is a delay in response from the dedicated interface. The non-dedicated channel is a typical internet banking login interface along with specific validations for the third-party provider (TPP) authorisation and specifications for consent management. The client's business challenge was to set up a new method of accessing the existing internet banking channel specifically for third-party providers over Transport Layer Security. Even though the cloned interface gives TPPs an alternative route via a different URL to access the customer interface and requires minimal technical involvement, maintaining the non-dedicated channel is difficult. Banks need to offer a proxy server in order to redact the personal data based on banks' policies since personal data are not supposed to be shared with third-party providers during the screen-scraping process.

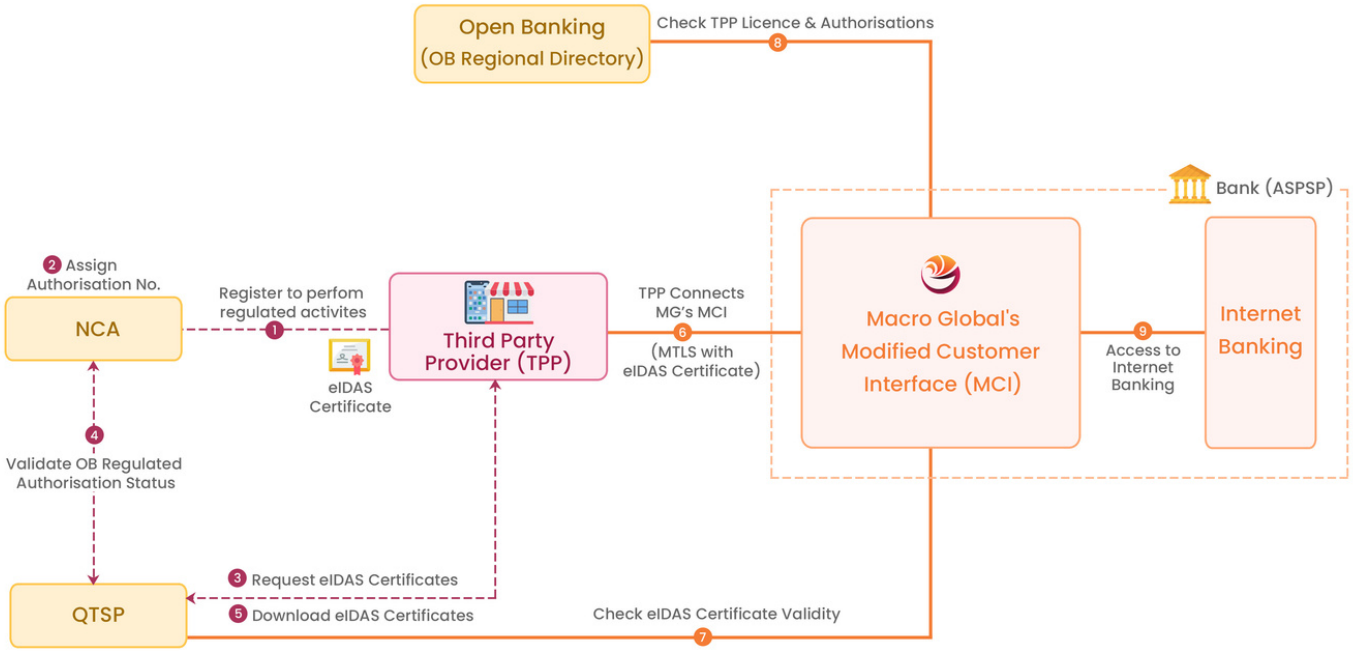
The client was seeking an integrated approach to provide end customers with an additional interface through which they can manage the third-party providers (TPPs) and allow them to make payments to ensure 24/7 access and improve operational efficiency.

## What we did – Macro Global's Modified Customer Interface Readiness

Macro Global's Open Banking subject matter experts engaged with the client to understand the live environment of the Internet Banking interface and shortfalls to build the fallback solution, the Modified Customer Interface (MCI).

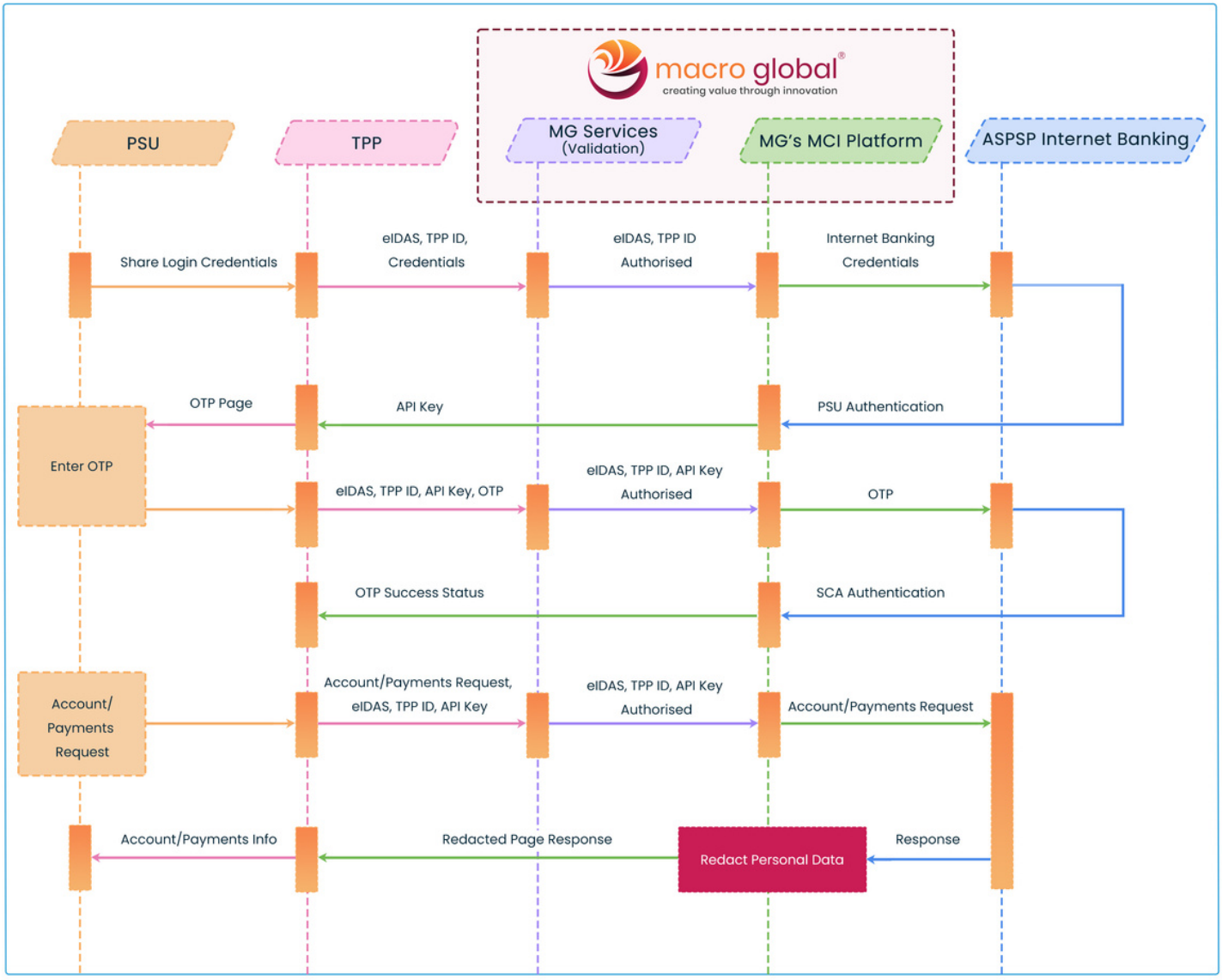
Through our extensive Open Banking experience, Our team of experts addressed the challenges faced by the client by enabling their customers to share the balance and transaction history and initiate payments with regulated third-party providers (TPPs) via Modified Customer Interface (MCI). Macro Global's MCI solution verifies and validates the eIDAS certificates presented by TPPs (authorised by Qualified Trust Service Providers (QTSP)) before accepting and exchanging the sensitive customer payment account data to achieve regulatory compliance and comply with Regulatory Technical Standards (RTS) mandates.

Macro Global deployed a web application firewall proxy server solution that helps to redact the customer's personal data and serves as a gateway into each of the web-based internet banking channel that is optimised for regulated account access by a third-party provider. TPP must provide an eIDAS QWAC (Qualified Website Authentication Certification) and our MCI service validates the certificate to ensure it is issued by a QTSP and perform real-time checks (well-formed and non-expired certificate). Upon secure connection mutually authenticated, TPPs are routed to the login page which is a splash screen of the ASPSPs Internet Banking channel. Macro Global's MCI solution is integrated with Screen Scrapping plus (SS+) technique to screen scrap the internet banking website and remove the customer personal data and shares the redacted page to TPP. When a customer personal data is redacted, it means certain information contained in the response page is concealed from view for privacy protection.



## How Macro Global's MCI Solution works

Macro Global's Modified Customer Interface (MCI) enables third-party providers (TPP) to access the payment service users (PSUs) designated payment accounts via the web-based internet banking channel. TPP's can login on behalf of a customer and perform the activities required to provide account information or confirmation of funds or payment initiation service in line with the consent provided by the payment service users.



- The payment service user (PSU) provides the internet banking login credentials in the third-party provider (TTP) application.
- TPP connects the Macro Global's MCI platform with eIDAS certificate and PSUs internet banking credentials.
- Macro Global's MCI service validates the eIDAS certificate with Open Banking and forwards the login credentials to the bank (ASPSP) for PSU authentication.
- TPP shares the One Time Password (OTP) screen for PSU to key in the OTP for Strong Customer Authentication and connects the Macro Global's MCI platform with OTP details and eIDAS certificate.
- ASPSP validates the OTP and Macro Global's MCI service authorises the TPP access.
- TPP forwards the accounts/payment request on behalf of the customer.
- Macro Global's MCI platform communicates with ASPSP Internet Banking to access the respective page and ASPSP provides access to the requested page.
- The response page is subjected to the banks' policy. Macro Global's solution screen scraps the response page and redacts the customer personal data (part of the information is obscured for security purposes).
- The redacted page will be shared with TPP either in JSON or HTML format.

## Outcome

Macro Global team helped the client to overcome their challenges in deploying the Modified Customer Interface (MCI) solution and meet the Open Banking RTS requirements. Macro Global's robust MCI solution is compatible and can be seamlessly integrated into any infrastructure irrespective of the technology choice and implementations (API requests/response and/or Internet Banking channel). The solution is designed as per FAPI specifications to enhance the performance and compliance of the platform against recognised standards.

More specifically, Macro Global's MCI solution provides the following benefits:

- FAPI Compliance (supported with TLS Ciphers)
- Validate eIDAS certificates
- Secure & Compliant with the latest version of transport layers (SSL/TL 1.2)
- Flexible and Scalable
- Customisable and easy deployment
- Seamless integration
- Sandbox environment for TPPs to test the connectivity and screen scrapping functionalities

## Our Success Story

Empower financial institutions to protect their brand, reputation and business from fraud and financial risk and secure the payment service user data.

Support Open Banking strategy by creating a unique platform of technologies that allows financial institutions to focus more on customer value.

Partnered with Microsoft Azure to protect the financial institutions' assets and emphasis on security, privacy, compliance, and transparency.

Our software-as-a-service (SaaS) model minimises the operational overhead and ongoing costs in Open Banking implementation.

Plug and play components that integrate into the Microsoft Azure ecosystem which allow rapid deployment of a working prototype.

# We are here to help you

If you want to learn more about our products or services or just have a question?

If you need advise from our expert team who understand your business better than our peers?

If you want to know how we transformed businesses using our unparalleled industry and domain expertise?

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

macro global®
creating value through innovation