CASE STUDY

macro global®

creating value through innovation

Enhancing Customer Experience with App-to-App Authentication

Synopsis

Rapid shift to technology innovation and demanding customer expectations are driving major changes across the financial service industries and with the growth of digital banking and spread of internet penetration, each individual is leaving a huge digital footprint amid the service providers. In today's digital era overshadowed by real-time access to the application, authentication needs to be at the right way and the innovation of Open Banking endorses the connectivity of banking that strives to enable data sharing by reducing time expensive authorisation steps.

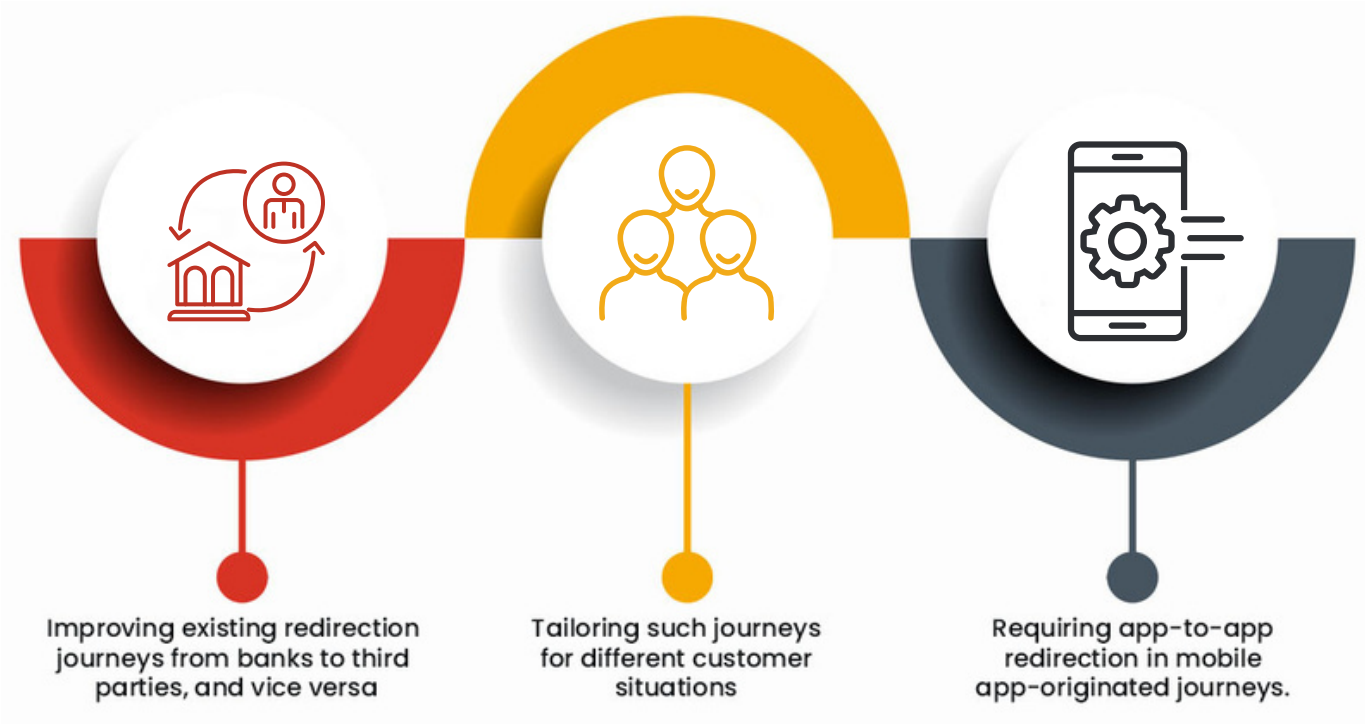
Open Banking empowers individuals to leverage their own data and nurture innovation propelling the digital economy foreword. Mobile banking fosters both strong security and enhanced user experience where customers prefer to authenticate through their mobile device and no longer need to use their bank cards for every transaction.

In this case study, we will examine how a rapidly changing financial environment is urging our clients to re-engineer their business operations and Macro Global's support in leveraging Redirection authentication to enable real-time connectivity and interaction between the user and market players (service providers).

Overview - Authentication Methods

To comply with the Open Banking framework, banks should open up APIs for third-party providers and enable a hassle-free customer journey for consent authorisation by payment service users (PSU). The Open Banking standards support both app-based redirection and decoupled authentication to allow a PSU to use the same authentication mechanisms when utilising the account information or payment initiation or card-based payment instrument issuer service by accessing the ASPSP directly. The subjected authentication flow requires fewer steps and payment service users encounter less friction.

The Open Banking Implementation Entity (OBIE) has mandated a number of recommendations for the financial institutions (banks) ensuring customer experience and comply with relevant regulations which include:

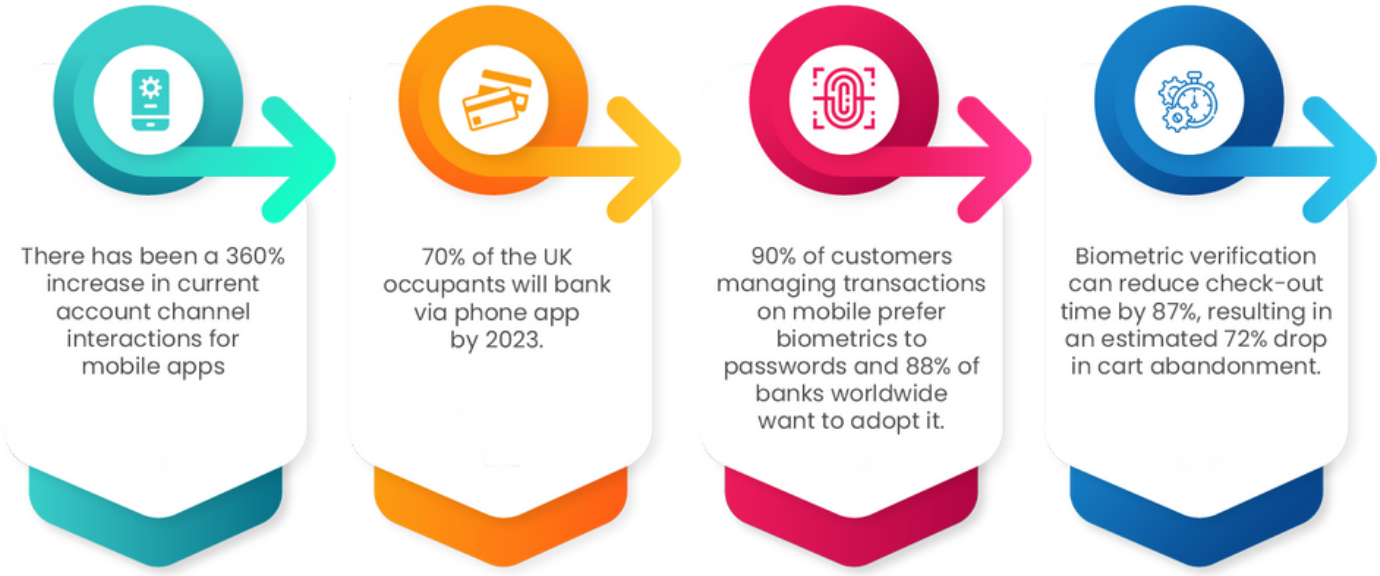


App-to-App Mechanism

The Financial Conduct Authority (FCA) has mandated that PSUs must be able to authenticate using the authentication methods they are accustomed to use via the ASPSP banking application ('app') on a mobile phone if accessing accounts through TPP service. App-based redirection authentication has an array of possible experiences for a payment service user (PSU) based on the device on which the PSU is consuming the TPP (AISP/PISP/CBPII) service and whether the PSU has an ASPSP mobile application installed or not.

App-to-App is a mechanism that allows mobile apps performing OAuth2 or OpenID Connect based authentication to offer a much simpler faster flow if the user already has an app provided by the authorisation server owner installed on their mobile device.

Customers are increasingly using mobile apps for banking payments and prefer biometrics for authentication.



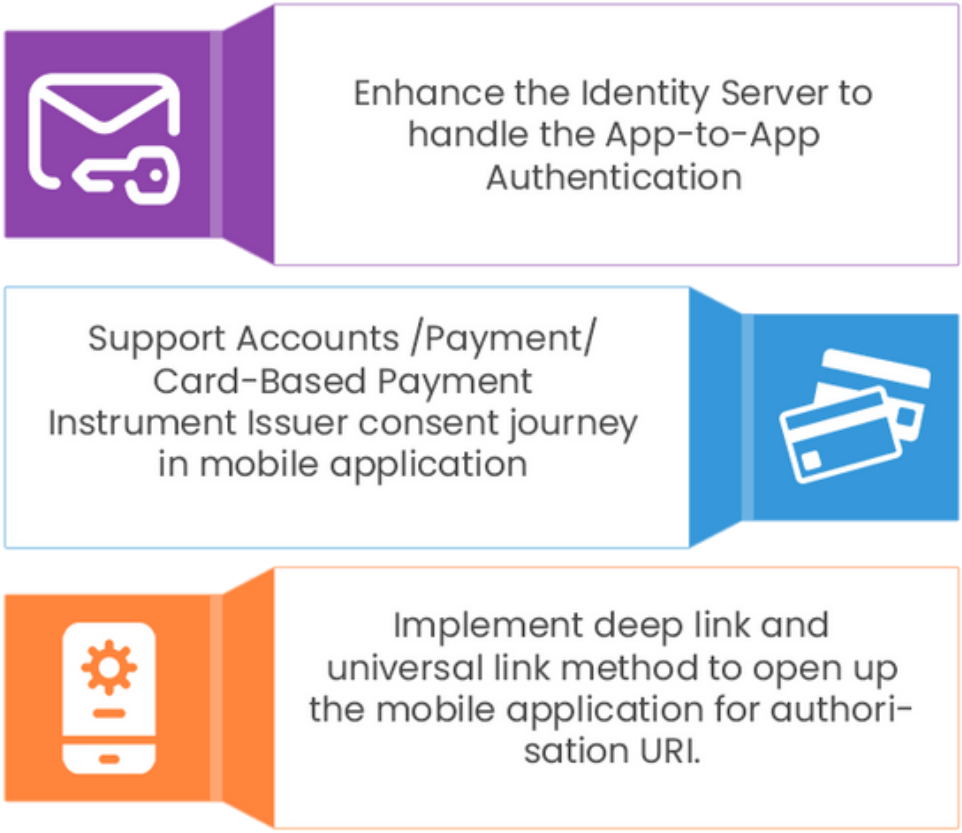
Business Background

Our client, a leading foreign bank (ASPSP) with a branch in the UK serving customers in retail banking, private banking and corporate banking sector recognised the need of innovating and improving both their products and the organisational services to stay ahead in the competitive edge. Macro Global has a long-term relationship with the bank and has partnered to achieve a successful transition by implementing a secure end-to-end Open Banking solution. Our platform accelerated confidence for the bank where payment services users (PSUs) will go through the consented Open Banking journey and manage their online consents from one central hub and unlock the power of their data.

On successful implementation within the mandated deadline, our client applied for exemption from the contingency mechanism in order to comply with the Open Banking Implementation Entity (OBIE) standards. The Financial Conduct Authority reviewed the exemption submitted by our client and upon further discussion, FCA advised the bank to implement the App-based authentication method (App-to-App mechanism) since our client delivered financial services through Mobile banking for seamless accessibility which enabled their customers to manage accounts via mobile application.

The current implementation of redirection was predominantly browser-based where the payment service user is redirected from the third-party provider app or website to the ASPSP's website for authentication. Our client faced sustainability challenges to implement the app-based redirection approach (App-to-App mechanism) enabling PSU to use their ASPSP mobile app for authentication. In order to implement App-to-App authentication and comply with the FCA mandate, our client engaged with Macro Global to achieve the mandated requirement.

Complexities in implementing App-to-App authentication

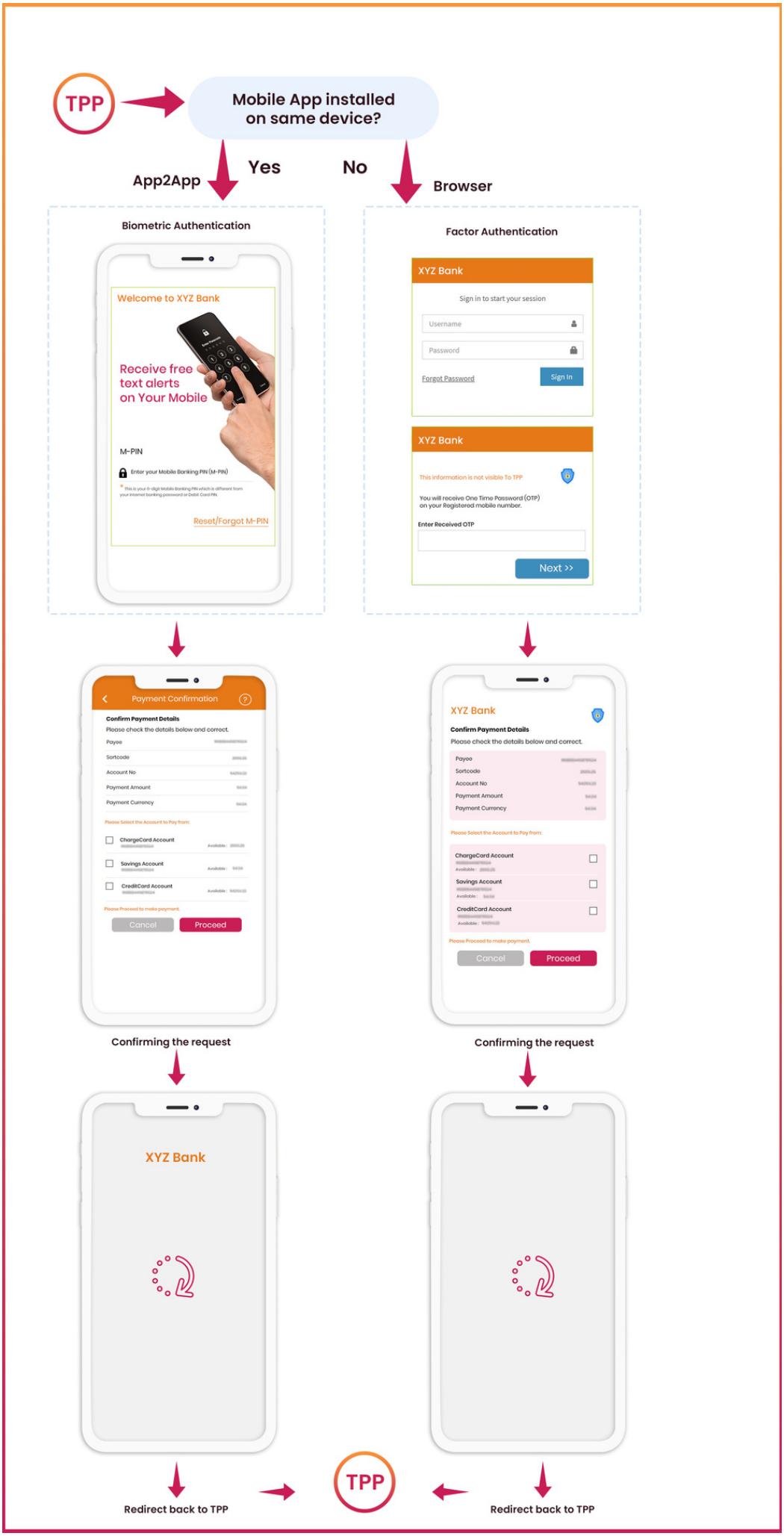


What we did - App-to-App Switch

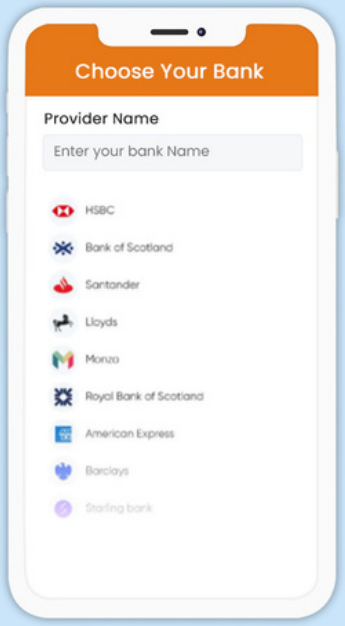
Macro Global's Open Banking subject matter experts engaged with the client to understand the shortfalls to implement the App-to-App authentication. Mobile app-to-app integration is the process of interconnecting one app to another app for optimising and exchanging consented data via API. Triggers in one app drive actions in another and data from one application are mapped and transferred to the other application.

Macro Global's app-to-app authentication allows the payment service user to complete the authentication using ASPSP's mobile app. Deep linking and universal linking adds value from an end-user standpoint potentially enhancing the user experience and improve app discoverability. Third-party providers (TPPs) are provided with new useable endpoints which deep links the PSU into our client (ASPSP) mobile app installed on their device to complete the account information or payment initiation or card-based payment instrument issuer authentication journey. Upon authentication journey completion, the payment service user will be redirected back to the TPP app. The app-to-app mechanism ensures that user journeys does not include redundant process that creates a barrier to adoption by third parties and payment service users.

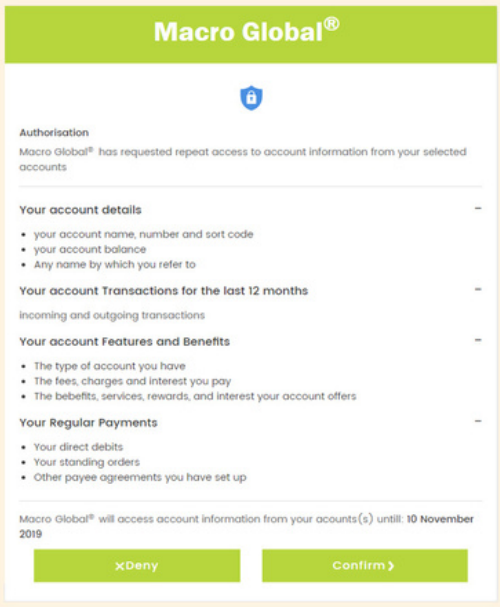
App-to-App redirection allows the third-party providers (TPP) to redirect the payment service user (PSU) from the TPP application (in a mobile web browser or mobile app) to the ASPSP's mobile app, installed on the PSUs device. The TPP app transmits the details of the request along with PSU preferences (e.g., product type, one-step authentication) and deep link the PSU into the ASPSP's application login screen. The PSU is then authenticated through the TPP app using the same credentials/methods as normally used when the PSU directly accesses their account using the app (typically biometric). If the PSU does not have the ASPSP's mobile app, they should experience a redirection flow when the PSU authenticates with the ASPSP directly without additional steps (e.g., redirection to the ASPSP's mobile website).



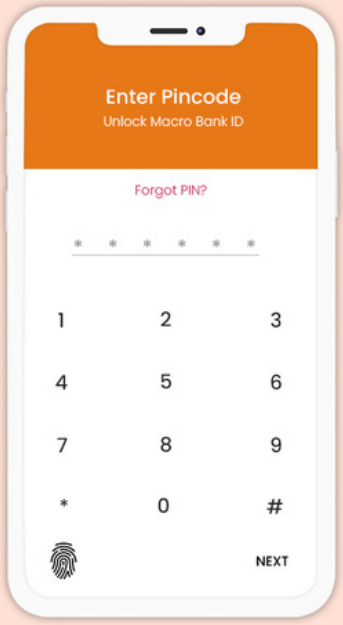
Macro Global's App-to-App Process Touchpoints



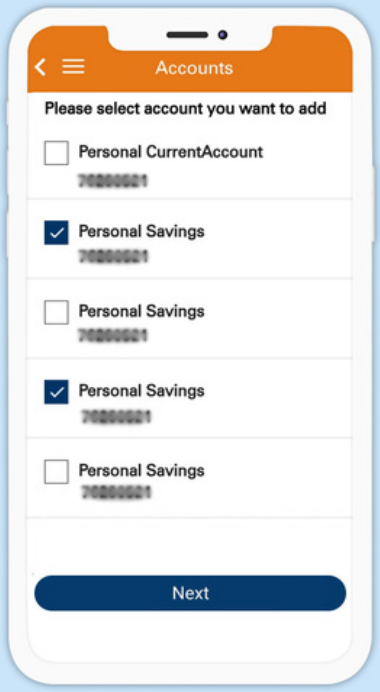
PSU initiates the request and selects the bank in the TPP interface



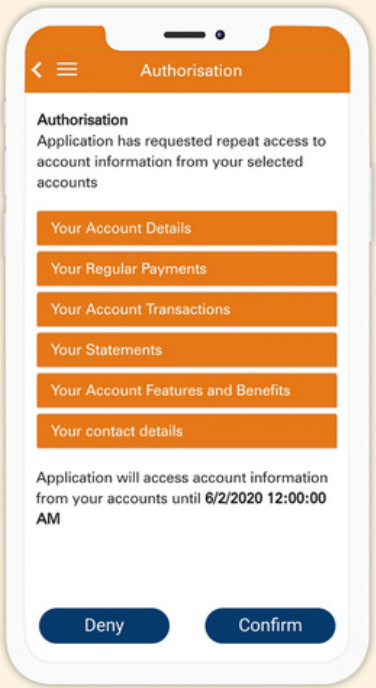
PSU gives consent for the requested service



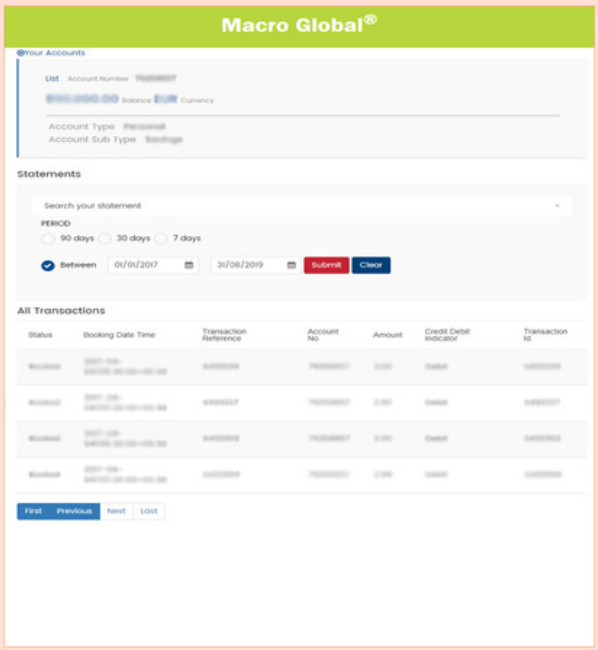
App launches and provides authentication screen. Based on configuration, either PIN or Biometric options are available.



PSU is authenticated and appropriate journey loaded (For AISP journey user need to select the bank account)



PSU goes through the request service and provides consent.



PSU redirected to TPP application with selected bank account details.

- Payment service user (PSU) sign-in the third-party provider app and choose the bank and trigger the Accounts/Payment/Card-based payment instrument issuer request.
- TPP calls the authorise endpoint (Macro Global Identity Server) with a signed JWT request.
- Macro Global Identity Server validates the TPP request and sends a response with the Consent URL to TPP.
- TPP receives and opens the Consent URL and simultaneously the mobile app verifies the Consent URL opened in the device.
- ASPSP's mobile app will be opened automatically for bio-metric authentication if the mobile application is installed on the device. Otherwise, the consent URL will be opened on the browser for browser-based two-factor authentication.
- PSU logins the ASPSP's mobile app using the biometric authentication.
- On successful PSU authentication, the ASPSP's mobile app initiates the AIS/PIS/CBPII Consent journey.
- The PSU verifies the AIS/PIS/CBPII Consent request and provides the consent. If PSU agrees on the consent, Macro Global Identity Server redirects the details (authorisation code and Id_token) to TPP.
- TPP calls the token endpoint with the authorisation code. Macro Global Identity Server validates the request and issues the access token.
- TPP calls the Macro Global AIS/PIS/CBPII Consent Request API using the access token.
- Macro Global AIS/PIS/CBPII Consent Request API validates the TPP request and provides the consented details and PSU can view the respective details in the TPP application.

App-to-App Redirection - Beneficial for Customers (PSU)

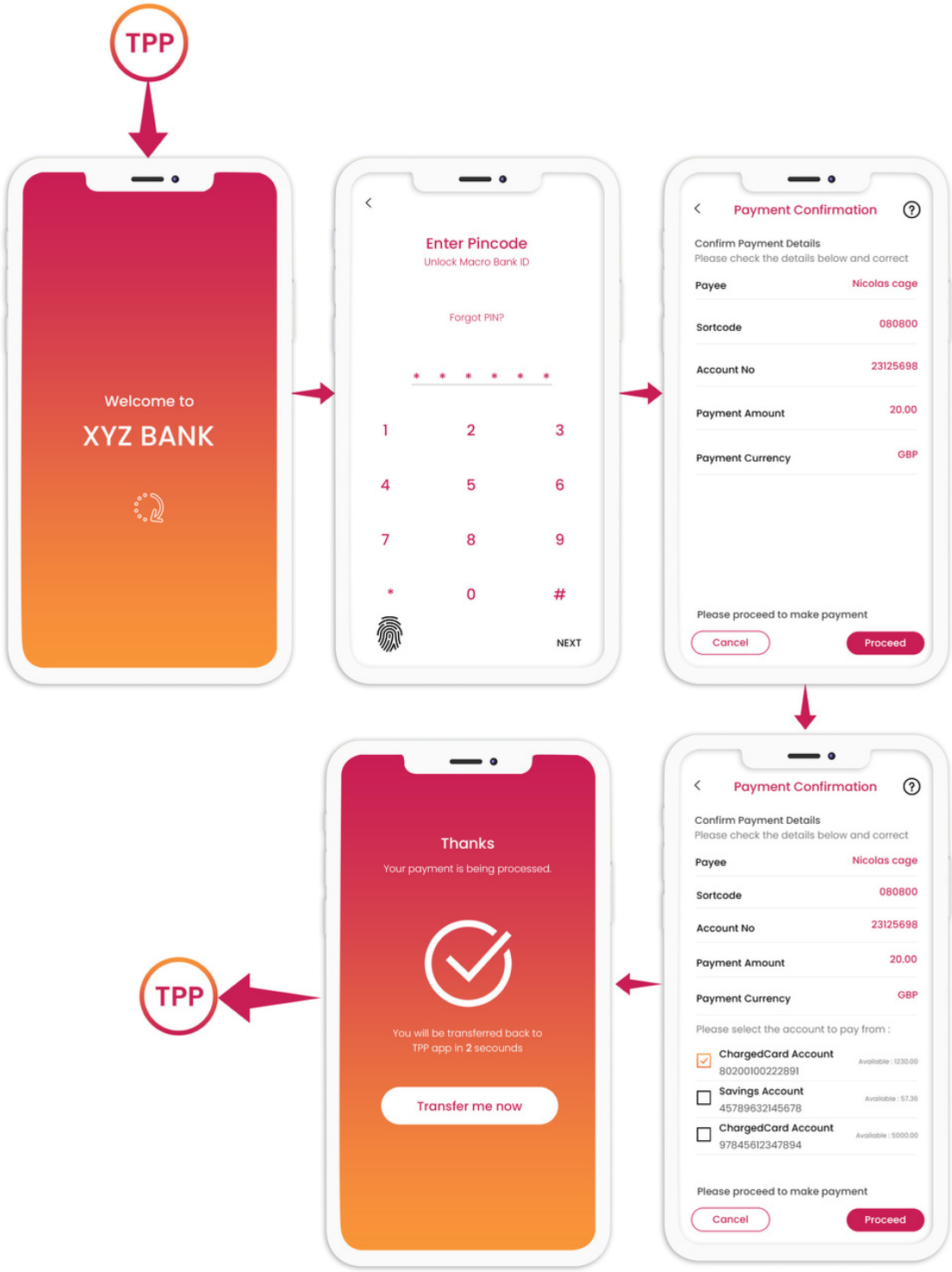
App-to-App Authentication provides a seamless journey for the PSU, which bypasses the built-in browser (e.g., Google Chrome) on their mobile device and open the Bank mobile application for authorisation by incorporating the consent journey. Customers are becoming digitally native, and increasingly use mobile apps for managing finance and payments. Consumer research data by Open Banking show most users prefer app-based journeys using biometric security elements such as fingerprints and face-ID which:

- smoothens the user consent journey to connect to banks, increasing conversion ratios
- enhance user experience and strengthen the engagement with the third-party app

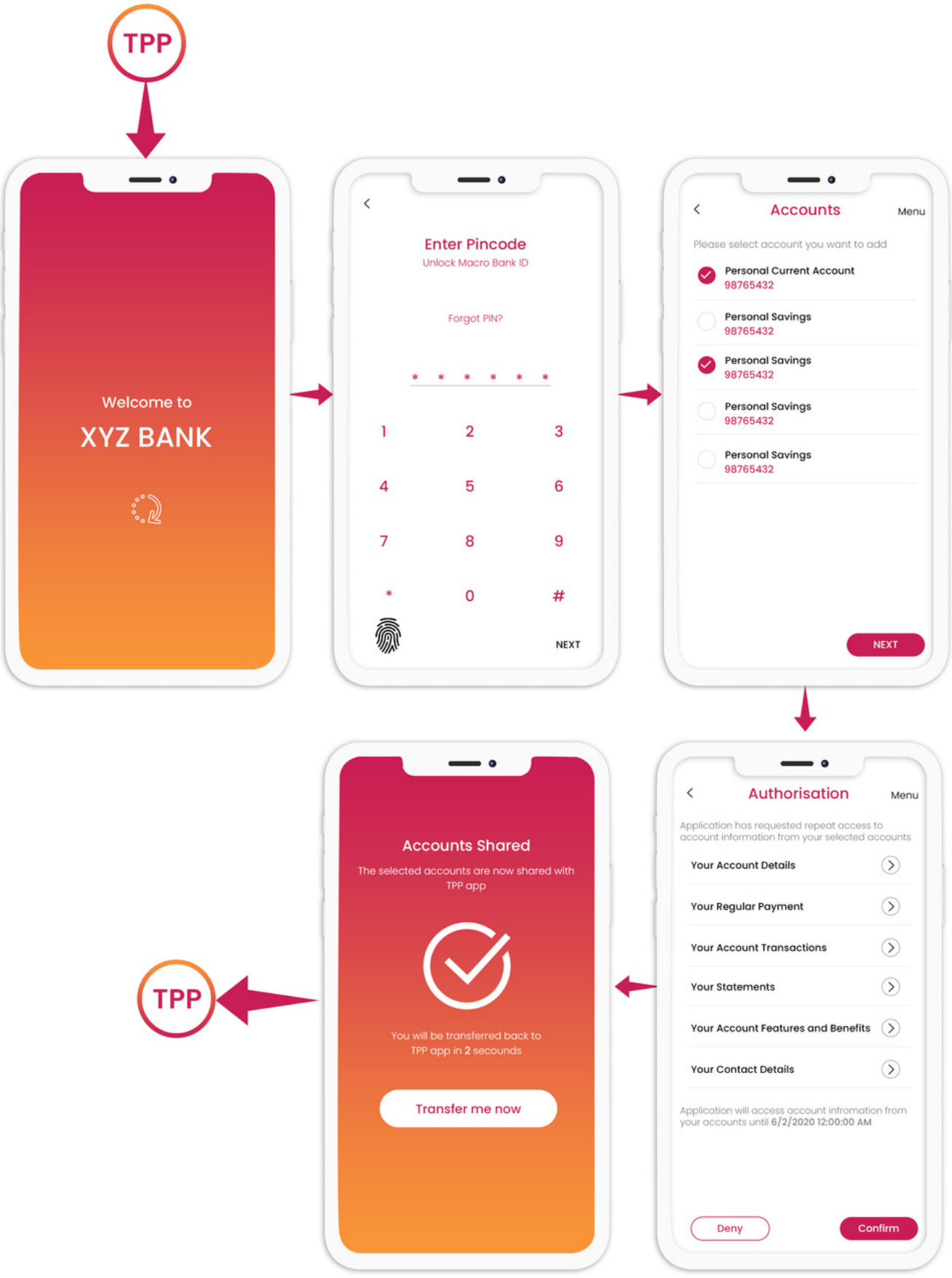
Payment Service User Journey

Payment service users (PSU) authenticate using the bank's (ASPSP) mobile app installed on the same device on which the PSU is consuming the AISP/PISP/CBPII service. This enables the PSU to authenticate with the ASPSP when using an AIS/PIS/CBPII service through the ASPSP app-based authentication method which they use when accessing the ASPSP mobile channel directly. The redirection invokes the ASPSP mobile app to allow the PSU to authenticate and in order to create a seamless user experience, the payment service user should not provide any PSU identifier or other credentials to the ASPSP if their current ASPSP app does not require the subjected process.

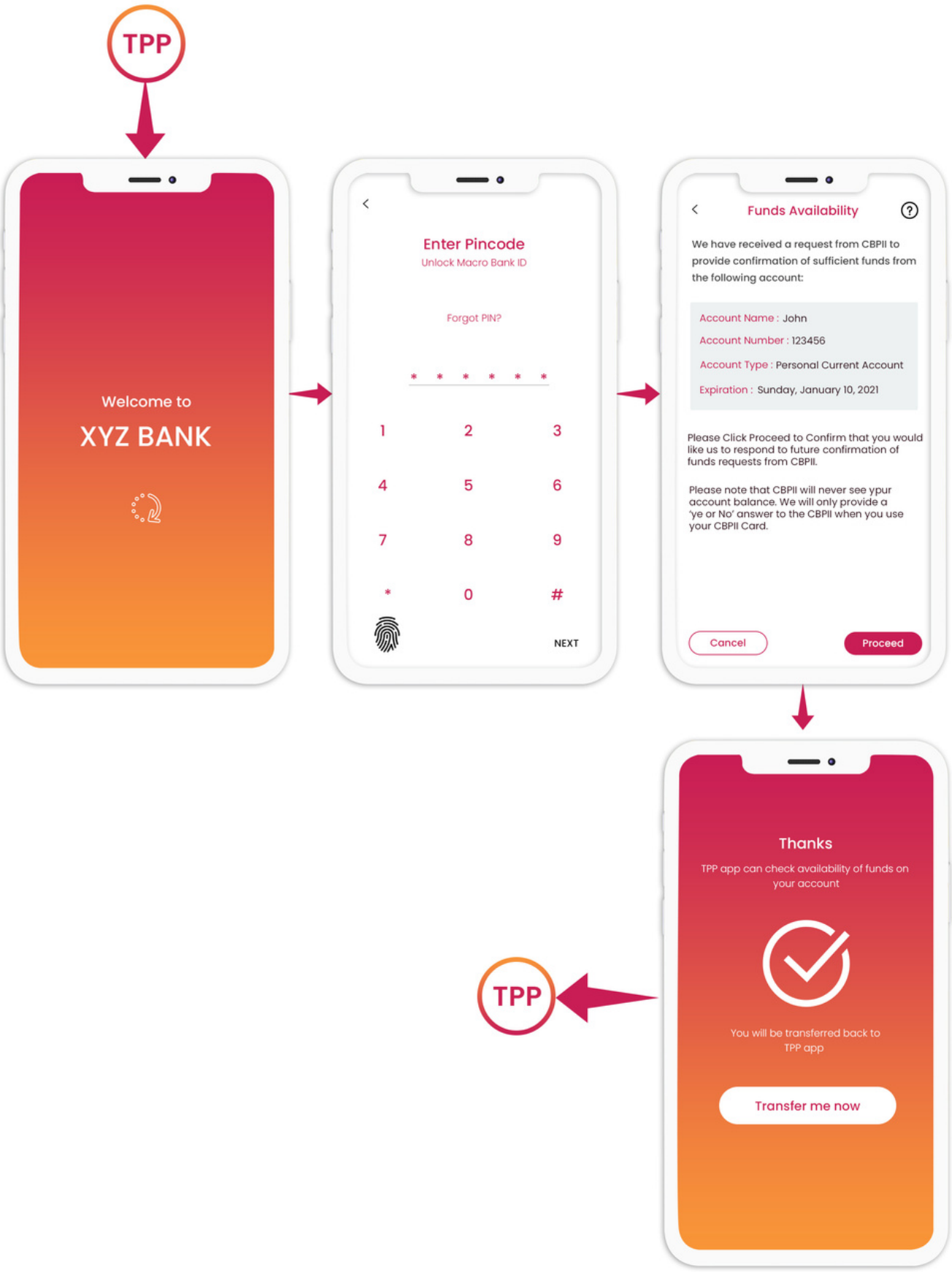
Payment Initiation Service User Journey



Account Information Service User Journey



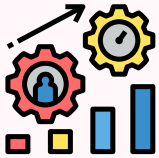
Confirmation of Funds User Journey



Our Success Story

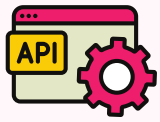
At Macro, we recognise strong partnerships empowering true value for our clients. We have successfully implemented Open Banking solution addressing key use cases for our clients supporting retail and corporate banking.

Enhanced consent journey process by improving the customer experience which enabled our client to drive business performance and innovative growth opportunities.



Provide an accredited Open Banking Platform with the client's architecture principles combined with our alignment of technology vision and domain experts.

Accelerated Regulatory Compliance with core Open Banking technologies (API Management, Identity and Access Management)



Comprehensive security scanning and penetration testing ensuring the highest degree of security and quality.

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