RAiDiAM

Open Banking & PSD2
An Inflection Point for Digital Identity Assurance

Sponsored By

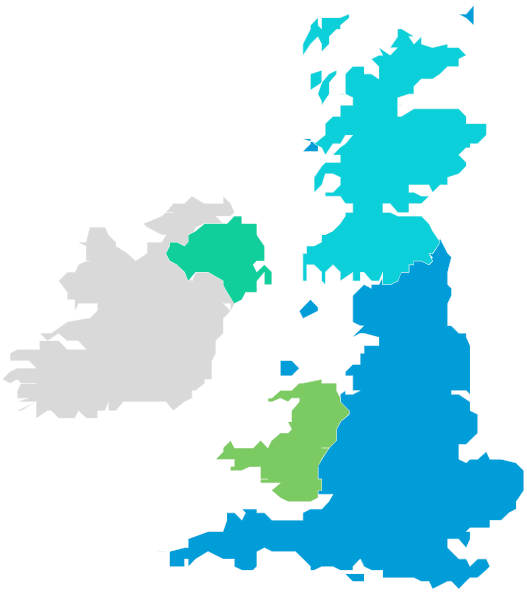
ilex International

TABLE OF CONTENTS

INTRODUCTION

The UK's Competition and Market Authority's (CMA) latest attempt to increase competition and consumer choice among banking service providers is taking shape in the form of the Open Banking initiative. The CMA is expanding the European Banking Authority's Payments Services Directive 2 (PSD2), in terms of the data that must be made available and is specifying more explicitly how this is done. The UK's existing and relatively static banking services landscape will be radically transformed through the delivery of standardised "Open APIs". [1]

These banking APIs will allow trusted payment parties (TPP) to deliver new and innovative financial and banking services that have the potential to radically shake up banks existing relationships with their customers, as well as raising significant identity assurance and access management challenges.



UNITED KINGDOM

60% of retail customers have been with their banking provider for 10 years or more

90% of SME customers bank with their retail-banking provider

Providing a standard set of APIs will be challenging for many functional and technical reasons. Perhaps most challenging from a security perspective will be the replacement of bespoke application protection mechanisms, protocols and internal standards with a single modern Identity and Access Management (IAM) capability that can integrate with third parties. This technical refresh, in a very sensitive area of retail banking, must be delivered within very aggressive timelines imposed by the regulatory authorities.

[1] https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

The Open Banking Implementation Entity (OBIE) and other regulatory bodies are considering 'OAuth 2.0', and some of its extensions, as the standards of choice for API security and identity federation. Security and API gateway products that adhere to these standards are available from numerous vendors, however, enhancements to the core and complementary standards are being proposed and ratified by technical governance bodies quite frequently.

Banks and other organisations in the financial services ecosystem should partner with vendors that are:

- Forward thinking
- Embrace open standards
- React quickly to threats
- Rapidly implement enhancements to their offerings

Organisations with these vendor partnerships will be best placed to ensure their API offering continually operates with the smallest threat surface possible and, as a result, will be well positioned to capitalise on new business opportunities that Open Banking services will bring.

The introduction of new identities in the form of third party digital actors necessitates a change in how banks manage access to, as well as ownership of digital resources. With traditional security perimeters being broken down, a new customer identity-centric approach to the delivery of technology services is required to ensure security postures remain within risk appetite. An identity-defined security model will best position banks for easier compliance with other identity and data governance regulations such as the forthcoming General Data Protection Regulation (GDPR).

OPENBANKING IN ACTION

Open Banking API offerings are broadly categorized into three services: Public information account information services (AIS) and payment initiation services (PIS). The CMA's high-level roadmap[2] schedules the delivery of APIs in the order of their security or risk levels. APIs requiring no security to implement will be delivered first, starting with the delivery of financial product descriptions and ATM / branch locations by the end of Q1 2017[3]. The aim is to have complete service offerings available by early next year.

Product information services – Public

- Banking product details (fees, interest rates)
- ATM and branch locations

Account information services – s Secured

- Account balance
- Transaction history

Payment initiation services – s Secured

- The ability to make a payment or transfer on behalf of a banks end client

These services, if secured using OAuth 2.0, introduce new identities with separate roles and responsibilities.

Resource owner: An entity capable of granting access to a protected resource. When the resource owner is a person, they are referred to as an end-user.

Resource server: The server hosting the protected resources, capable of accepting and responding to protected resource requests containing valid access tokens.

Client: An application making protected resource requests on behalf of the resource owner with its consent. The term "client" does not imply any implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices).

Authorisation server: The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorisation.

[2] https://www.openbanking.org.uk/about/

[3] HSBC's unsecured public services were released early January for public beta. https://developer.hsbc.com/

How these security identities and their roles apply to the roles defined by PSD2 is presented below in Figure 1. These diagrams demonstrate two of the common use cases envisaged by the regulator. On the left, a product comparison service wishes to offer an aggregated view of a bank's customer account information and is acting as an account information service provider (AISP). On the right, an online retailer, acting as a payments initiation service provider (PISP) wishes to initiate a payment from a banks customer account.

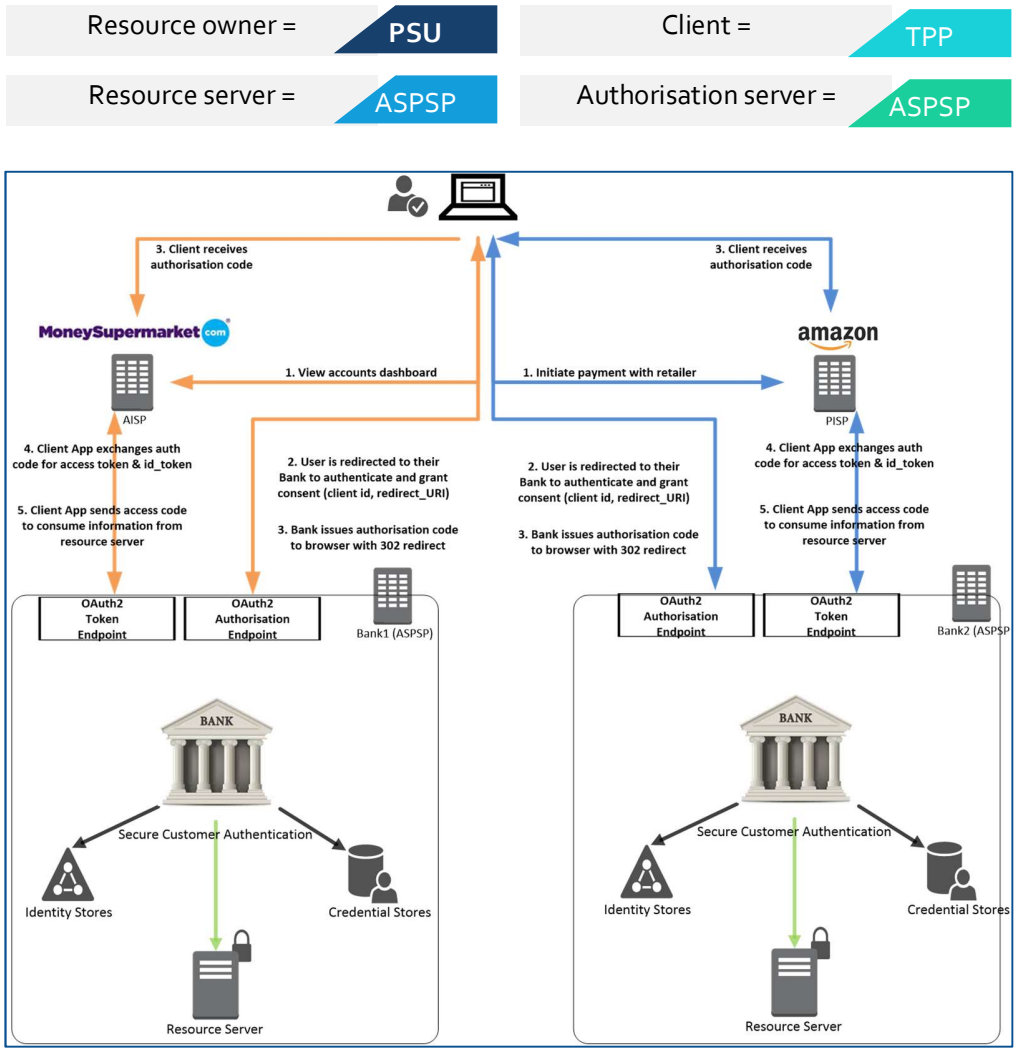


Figure 1 OpenBanking In Action?

The introduction of these new identities, services and 3rd party access mandates has the potential to significantly increase the threat surface that customer's digital assets are exposed to. In parallel, banks must contend with the conflicting customer demand for improved user experience, through reduced security friction, as well as ever higher customer and regulatory expectations for secure service delivery.

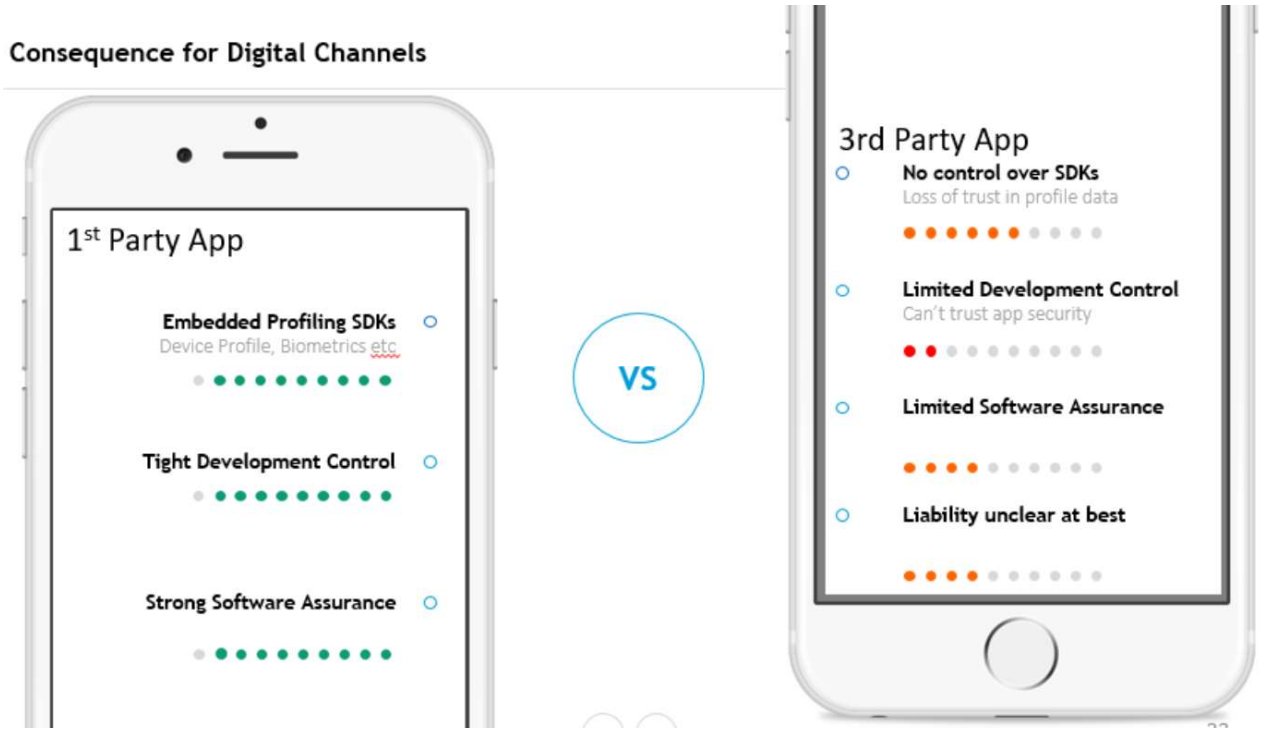
Adjusting to fundamental changes in the relationships that banks currently have with their customers, while achieving this dual mandate will require a modern, flexible Identity and Access Management capability as well as recognition that identity management is at the core of digital services delivery.

CUSTOMER NOT PRESENT

Achieving assurance in a headless world.

Today, customers of account servicing payment services providers interact almost exclusively with banking services via 1st party channels including mobile, telephony or Face2Face. These channels require customers to perform an appropriate degree of identification and verification before services or information is given.

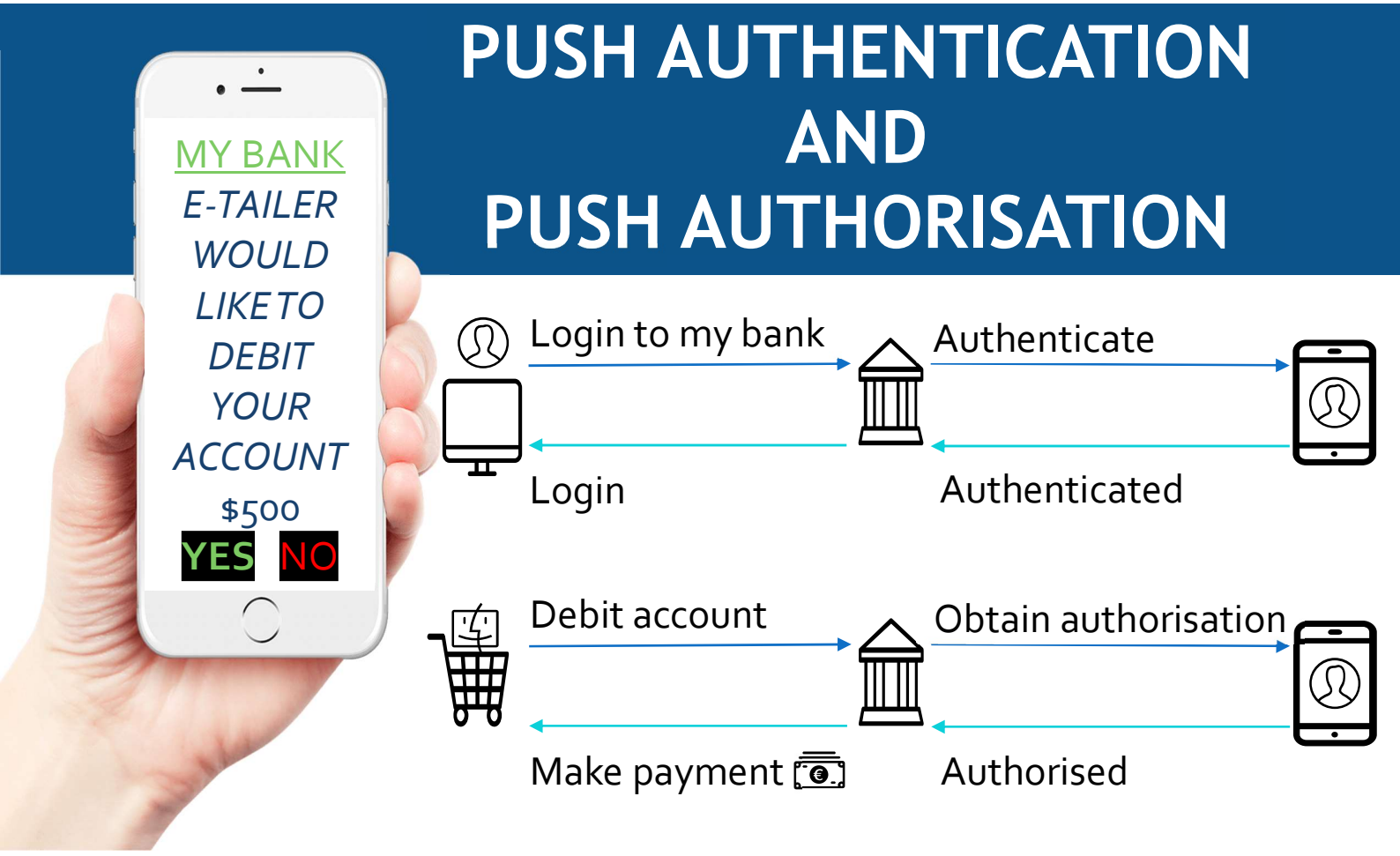
In an API channel consumed by third parties, bank's will need to address use cases where TPP's are performing operations on a customer's behalf when the **customer may not be present in the flow of the operation.** Banks must adjust security postures to reflect the loss of control, quality assurance and variable degrees of app security that may be used by customers to access banking services.[4]



[4]Bank's 1st party applications can be loaded up with numerous SDKs that can continuously analyze user behavior as a source of identity. These biometric factors could enable a reduction in security friction and improve customer's user experience. Third party applications will not be able to provide this same level of continuous authentication which will mean that other authentication / authorization mechanisms with different user experience and higher friction will be needed to provide appropriate levels of identity assurance.

Banks looking to reduce the risk inherent in *Customer Not Present* transactions could consider enhancing existing Identity Assurance / Authentication capabilities in existing 1st party applications. Augmenting authentication capabilities with authorisation capabilities banking applications could be used to obtain consent in the form of a signed transaction response.

By leveraging the power of push notification and the biometric security built into modern smart phones, banks can opt to bring customers into the decision-making process of a payment request in real time with minimal security friction.



By re-engaging and empowering the customer with tools to help manage third party use of their digital assets, Banks' customers can fully exploit the opportunities being made available by Open Banking. Without mechanisms to validate suspicious transactions initiated by third parties when "customer not present", the level of financial risk that banks can accept will be limited, reducing the value proposition third parties can offer to clients.

CONCLUSION

Digital identity assurance is at an inflection point. The coming swarm of digital financial asset management APIs will enable new and innovative services to be deployed at a pace unseen before in the history of the financial services industry, both in the UK and elsewhere.

API delivered services have the potential to significantly increase the threat surface banks are exposed to and pose new challenges for identity assurance. Delivery of an API channel will require significant investment in IT Security and IAM infrastructure. It will also require the re-engineering of business processes to manage the numerous new identity classes and their authorisations.

Positive user experience of an API channel will require an appropriate balance be found between **user experience security friction** and **fraud risk.** A high degree of identity assurance can be obtained with [5]minimal security friction through the adoption of new and innovative authentication and authorisation capabilities.

These tools will be vital in ensuring asset owners remain firmly in control over the access to and use of their digital assets. By empowering customers with the tools to safely manage and build their own trust relationships with third parties , OpenBanking and the desire for more open banks can be realized.

A RAiDiAM White Paper

Sponsored By

[5] Assuming the regulators are not too proscriptive about the security journey, see current definition of "Secure Customer Authentication" in PSD2

PSD2 Terms Glossary			
No	**Term**	**Definition**	**Example**
1	Account information service provider (AISP)	Any online provider that wishes to aggregate information on one or more payment accounts held with one or more payment service providers and who typically present customers with a single dashboard view of accounts.	Yodlee, Mint, First Direct, Money Supermarket including Banks.
2	Account servicing payment service provider (ASPSP)	All financial institutions that offer payment accounts (e.g. current accounts, credit cards) with online access. Under the legislation these institutions will be obliged to provide an API to allow authorised and registered third parties to initiate payments by the account holder as well as access to account information.	Banks e.g. RBS, Barclays, HSBC
3	Payment initiation service provider (PISP)	Any organisation (traditionally retailers but they could be any category of business accepting online payments) that initiates a payment where the merchant website consumes an API exposed by the Bank in order to initiate payments on the basis of a credit transfer.	Amazon, British Gas, O2
4	Third party payment service provider (TPPSP or TPP)	TPPs are the AISPs and PISPs - the 3rd parties alongside the banks and the customer in the payment process.	As above
5	Payment service user (PSU)	The end user of the payment service, typically the account holder of an ASPSP.	A bank retail customer
6	Regulatory technical standards (RTS)	A set of detailed compliance standards that specify the requirements of Strong Customer Authentication (SCA), the exemptions from SCA, requirements to protect the PSU's personal security credentials, and the requirements for common and secure open standards for all parties above.	n/a
7	Card scheme	Card Schemes are payment networks linked to payment cards such as debit or credit cards, of which a bank or any financial institution can be a member.	Visa, Mastercard, Amex
8	Access to accounts (XS2A)	Enables financial institutions and non-financial players (collectively TPPs) to obtain access (granted by PSU) to the bank accounts of European customers.	n/a
9	Application programming interface (API)	An API is a set of commands, functions and protocols which developers can use to allow one piece of software to interact with another to exchange data, particularly over the web. In the context of PSD2, ASPSPs will expose APIs externally to enable TPPs to interact and provide account information and payment services.	n/a