Response to
Open Banking in Australia

Date: 21 September 2017
Author: Raidiam Services Limited (Raidiam).

Disclaimer

All views and recommendations in this response document are the views of Raidiam and do not represent the views or recommendations of Open Banking Limited, nor of any other person or organisation. Furthermore, this information is provided without warranty of any kind, express or implied. In no event shall Raidiam be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the information in this document.

Contents

Management summary

This document is a formal response to the ‘Review into Open Banking in Australia’ Issues Paper, dated August 2017.

This document has been prepared by Raidiam, a leading Identity and Access Management consultancy. A number of Raidiam’s partners have been the core architects in developing the functional standards and security overlays for the Open Banking ecosystem in the United Kingdom (UK). Raidiam is also providing support services relating to implementation of these Open Banking standards to a number of leading banks in the UK.

Raidiam believes there are many significant insights to be gained from the implementation of the Open Banking ecosystem in the UK, which can be directly applied to Open Banking in Australia.

We have a number of specific recommendations detailed in this document, which can be summarised as follows:

1. Build upon existing experience from similar Open Banking efforts globally.
2. Build a roadmap for Open Banking in Australia that sets the path for the short, medium and long term.
3. Ensure regulatory framework, governance model (including liability model) and long term funding are in place as early as possible, as the absence of these will cause significant delays during design and implementation.
4. Adopt elements and build on regulatory frameworks that have been established internationally (e.g., PSD2, the UK CMA Order, European GDPR).
5. Mandate all ASPSPs in Australia provide access to data via a standardised interface.
6. Mandate the use of modern, open standards.
7. Reuse OBIE standards for the functional API payloads and the OBIE security framework, as both have had significant industry review in the UK and are reusable with minor changes for the Australian context.
8. Reuse, where possible, standards developed by the UK OBIE for Open Data and Read/Write APIs - tailored to an Australian context.
9. Ensure primacy of the consumer when setting the policy around data privacy, and consent management.

Response to consultation

Introduction

In this response document, Raidiam has provided analysis and recommendations relating to each of the sections covered by the Issue Paper.

The context and background for Open Banking in Australia are closely aligned to what is happening in Europe and the UK, and so our response is based on our detailed understanding of what is happening in these markets.

We will use a number abbreviations, such as ASPSP, which is short for Account Servicing Payment Service Provider (i.e., the banks, building societies and credit card operators who will provide the API endpoints). A full list of abbreviations is provided in the Glossary.

What is ‘Open Banking’?

Open Banking is an effort to reduce the customer ‘lock-in’ that is apparent in financial services. That customer ‘lock-in’ has resulted in reduced competition in the financial services market and it therefore displays behaviour resembling a monopoly i.e. lack of responsiveness to customer needs and high margins.

Reducing that ‘lock-in’ is the goal of Open Banking and current developments in this area are taking inspiration from the technology industry and the ‘API economy’.

It is widely accepted that Open Banking implies the introduction of APIs which will allow third party developers to build customer facing applications on top of (legacy) banking and financial infrastructure.

Open Banking is a global concept and is being either considered, promoted or mandated in many markets. In the UK, Open Banking has effectively been written into law by the Competition and Markets Authority (CMA) as the CMA Order. More details about the international context and the CMA Order are covered later in this paper.

Open Banking in the UK has created standards for, Open Data and Read/Write (closed/restricted) Data.

UK Open Data

The UK Open Data API standard covers the following six areas:

- Location, service, and accessibility information about ATMs.
- Location, service, accessibility, and opening time information about Branches.
- Product information about retail Personal Current Accounts (PCA).
- Product information about retail Business Current Accounts (BCA).
- Product information about Business Unsecured Loans (SME).
- Product information about Commercial Credit Cards (CCC).

Each of the 9 largest retail banks and building societies in the UK (the CMA9) must make these APIs available for all of their brands, without restriction to any developer via a set of completely open and publicly available APIs. This is because there is no business case which requires developers to identify themselves to the API providers, and it removes all possible barriers to entry. In effect, the APIs are treated the same as information which is currently available on the website of any provider, with the added advantage that the data is codified to a standard to make comparison easier.

See https://www.openbanking.org.uk/open-data-apis/.

UK Read/Write Data

The UK Read/Write API standard covers the following:

- Read APIs: account and transaction information relating to a specific customer's account.
- Write APIs: initiation of a payment instruction from a specific customer's account.
- A security framework that is used to managed access to the Read/Write Data.

These APIs are considered closed or restricted, and as such are protected by a security framework which is detailed in the subsequent section of this response relating to securing data. Significant work has also been undertaken in the UK to standardise how a customer's consent is managed through the flows, ensuring the customer is centrally in control of the process.

See https://www.openbanking.org.uk/read-write-apis/.

Considerations

There is arguably a limited case for creating a standard for ATM and Branch information in other markets, since the data already exists in a structured format and this service could easily be provided by one or more third parties, including the major search engines.

There is however a strong case for creating an Open Data standard for product information, as this can be used by third parties in conjunction with Read APIs to provide comparison and switching services. This is certainly the intent behind the CMA mandating both Open Data and Read Data as part of the UK standard.

Furthermore, there is significant value in a Write API which allows third parties to initiate payments, as this can open up a number of innovative alternatives to current payment methods.

What are the likely benefits and costs of Open Banking?

Benefits

The benefits of Open Banking would be very hard to quantify in exact financial terms, but they are significant for all parties.

- This is a fantastic opportunity for ASPSPs who wish to embrace Open Banking, as they can ultimately provide better services to their customers via any number of innovative third party applications.
- This is a significant opportunity for challenger banks, as they will be able to compete at the ‘same table’ as larger, more established brands.
- Open Banking also offers a great opportunity for FinTechs and third parties, as they will be able to develop better and more reliable products and services, and also for a lower cost, than via currently available methods such as screen scraping.
- Ultimately, this will benefit end customers, who will have access to better financial products and services.
- There will also be a significant business opportunity for vendors and consultancies who can help ASPSPs and third parties develop, implement and support the standards.
- A lower competitive barrier through a central registration regime will allow ASPSPs and third parties to focus on innovation rather than striking contracts with each other.
- Charities and the 4th sector can build applications that focus on disadvantaged segments of customers that ASPSPs do not have an interest in serving in a differentiated manner (e.g. banking apps for mentally challenged persons with PoA etc.)
- Over time, there should also be a reduction in the cost of processing payments for SMEs, small clubs, schools etc, through the automation and reduction of charges from cards & acquirers.

Costs

Overall the costs to implement Open Banking in the UK are large (in the hundreds of millions of GB pounds). There are four main areas.

Firstly, there will be a central cost relating to the creation and governance of the standards. This will include a setup cost to develop the standards and help all parties with implementation.

There will also be ongoing costs to evolve the standard over time and to provide services such as technical support and dispute resolution. It is not yet clear what the ongoing costs will be, nor who will pay for them.

Thirdly, there will be costs for each of the ASPSPs and third parties to implement and support these APIs. These costs will vary from company to company, and will include development costs (for building and running/supporting the software and infrastructure) as well as other costs, such as insurance. These costs could be £100m or more per annum for a large bank with millions of customers and expensive on-premise technology.

Finally there is a potential risk of increased fraud and the associated costs. This is because for years we have been training consumers not to share their sensitive financial data. There will thus be costs associated with raising public awareness of Open Banking, and the safe use of the Open Banking ecosystem.

Considerations

Central setup costs would be significantly reduced by implementing standards which have already been proven, and there are many lessons to be learnt from what is happening in the EU, and in particular in the UK.

Furthermore, central ongoing/run costs could be mitigated by having a subscription model for ASPSPs, rather than relying entirely on central/public funding.

Free access to Open Banking APIs for third parties will help speed up adoption and allow smaller players to enter the market.

The more that is standardised (e.g. the details of the functional APIs and the security model), the lower the costs will be for ASPSPs and third parties to implement, as there will be less ‘re-inventing the wheel’ for each participant.

Finally, to mitigate against fraud, there should be increased consumer facing communications to increase consumer awareness. Whilst the bulk of this should come from ASPSPs and third parties, it is also worth considering some form of centralised communications, as this could be more efficient.

International context

Open Banking is a global concept. However, the context and background for Open Banking in Australia are perhaps most closely aligned to what is happening in Europe and the UK.

In Europe there are two specific drivers for Open Banking, PSD2 and GDPR.

PSD2

The Second Payment Services Directive (PSD2) is a fundamental piece of payments-related legislation in Europe, which entered into force in January 2016. PSD2 is the result of a review of the original Payment Services Directive and requires payment service providers (PSPs) to make a significant number of changes to existing operations. The Directive requires that all Member States implement these rules as national law by 13 January 2018.

In summary, PSD2 sets out regulations for how ASPSPs must allow customers to be able to access their data via third parties (AISPs and PISPs). Related to this are the Regulatory Technical Standards (RTS) which define rules for strong customer authentication (SCA) and secure communication under PSD2. If PSD2 is the 'what', then RTS is intended to be the 'how'.

However, RTS is still in draft and not yet agreed. There remain a number of significant challenges:

- From ASPSPs, who are lobbying for stronger controls and the abolition of screen scraping and direct access, and
- From established third parties, who are lobbying for reduced barriers and direct access. In any event, once agreed, it will be a further 18 months before RTS must be implemented.

PSD2 in Europe will be governed by The European Banking Authority (EBA), an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.

The final draft of RTS is available at https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf. While RTS contains quite a lot of detail about how the 'alternative interface' should work, especially relating to security, it does not specifically mandate a common standard for APIs.

GDPR

The General Data Protection Regulations (GDPR) are a set of rules which have been put in place to protect individuals in a number of areas. They cover, for example, the right to be informed, the right of access, and the right to data portability. Many of these rights are highly relevant for Open Banking.

GDPR places specific and stringent legal obligations on both data controllers and data processors. There are significant implications for how Financial APIs should work, and in particular for the obligations of all ASPSPs and third parties. There are potentially crippling financial penalties for organisations which breach the regulations.

GDPR will come into force from May 2018. Governance is left to each EU member state, and in the UK, this falls under the Information Commissioner's Office (ICO), the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

More information about GDPR (in the UK context) can be found at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

The CMA Order

The UK Government has agreed that both PSD2 and GDPR will apply to banking in the UK, even after the UK has left the EU. However, the UK has an additional driver for Open Banking, the CMA Order.

In August 2016, the Competition & Markets Authority (CMA) published their final report on their retail banking market investigation. This included the creation of The Retail Banking Market Investigation Order 2017 (the CMA Order).

Full details of the CMA Order can be found at https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017.

Whilst the RTS will (eventually) set out some clear rules around security and access, there is a significant risk that each ASPSP will develop their own implementation, with unique API data structures and a bespoke security interface. This could cause fragmentation and be a major barrier to adoption by third parties.

The CMA Order goes a step further, in that it requires the nine largest retail banks in the UK (the CMA9) to adopt and adhere to a single unified standard for APIs. Whilst the CMA Order requires compliance with PSD2 and GDPR, it stops short of full coverage in a number of areas, specifically:

- It relates only to Personal and Business Current Accounts, with no coverage of Private Banking, Corporate Banking, Card Schemes, Wallets, Mortgage accounts and Lending Accounts.
- It relates only to UK Sterling accounts and payments.
- The mandate only covers the CMA9, although other ASPSPs can chose to follow the standards if they chose.

It is possible that at some stage in the future the remit of the CMA Order may extend to completely match the coverage of PSD2.

There are two main deadlines for the CMA Order:

- Stage One of the CMA Order relating to Open Data APIs (see below) was delivered by the CMA9 on 31 March 2017.
- Stage Two of the CMA Order relating to Read/Write APIs (again, see below) is due to be delivered by the CMA9 on 13 January 2018. This coincides with the original date when PSD2 is due to come info force.

Another core part of the CMA Order was the creation of the Open Banking Implementation Entity (OBIE). The OBIE is an independent body with the mandate to develop the standards and central infrastructure for Open Banking in the UK. The OBIE is currently trading as an limited company, Open Banking Limited, see https://www.openbanking.org.uk.

It is expected that the OBIE will evolve into a permanent body which iterates and governs the standard in the UK. However, the details of this are yet to be confirmed.

Other initiatives

There are many other Open Banking initiatives across Europe and Globally, for example:

- The OpenID Foundation's Financial API (FAPI) Working Group has developed an open standard for securing financial APIs (see http://openid.net/wg/fapi/). The UK's security profile is based on this standard and OBIE are active participants in helping shape the future of the FAPI standard.
- ISO 20022 is a universal standard for financial messaging (see https://www.iso20022.org/, and there are draft plans for a JSON API ISO 20022 standard, although this may be some way off. In the meantime, the UK Open Data standards contain a mapping to current XML based ISO messaging.
- The Berlin Group, a-European payments interoperability coalition of banks and payment processors have announced their NextGenPSD2 Initiative to provide a harmonised API standard for accessing bank accounts (see https://www.berlin-group.org/single-post/2017/06/13/PRESS-RELEASE---Berlin-Group-NextGenPSD2-announced-creation-of-European-PSD2-API-standard).
- STET is a payment platform owned by six major French banks. They have recently announced an Open Banking API standard (see https://www.stet.eu/assets/files/PSD2/API-DSP2-STET_V1.2.2.pdf).

There are also a growing number of (often commercial) entities who have developed their own flavours of Open Banking API specifications. Albeit to our knowledge, none of these are agreed (by any market) as an open standard.

Considerations

To create equivalents of PSD2, GDPR and the CMA Order from scratch in Australia could take a long time and incur great expense.

As stated above, there are many learnings which can be taken from PSD2, GDPR and the CMA Order, not to mention the many other initiatives globally.

The challenge will be what to adopt, what to build on, and what to ignore.

What the Review will examine?

What data should be shared and between whom?

In Europe, the PSD2 regulations have mandated that ASPSPs must allow customers to access data through third parties that are registered with a national competent authority (NCA). In the UK specifically, the Competition and Markets Authority (CMA) has mandated the standardisation of Open Banking APIs for freely available ATM, branch and product information, as well as the standardisation of APIs for Read/Write data access.

Open Data

The UK has taken a phased delivery approach to the Open Banking standards. The initial phase was focused was on standardising the access to freely available ATM, branch and product data. Followed by a minimum viable product (MVP) approach to delivering Read/Write data access - with a focus on the key data required to support use cases such as account aggregation services.

Standardising freely available product data will enable third party developers to facilitate better comparisons between ASPSP's product offerings, and increase market competition. The UK OBIE has taken a thorough approach to agree the structure of how product data will be represented in the standard, based on the core set of elements required to make a reasoned product comparison. This has included several industry wide workshops with ASPSPs and third parties, and collaborative working through through several iterations of publishing material and seeking structured feedback.

The scope of the Open Data standard for the initial release has been driven by:

- The CMA Order, which has prescribed that:
    - Product information cover key areas around pricing, fees, charges, features, benefits, and eligibility
    - ATM location and accessibility information
    - Branch location and accessibility information
- Feedback from product comparison providers

Read Data

The OBIE has coordinated a thorough process to agree a standard in the UK. This has included several industry wide workshops with ASPSPs and third parties, and collaborative working through several iterations of publishing material and seeking structured feedback. The end result has been a Read/Write API standard that has been agreed across the CMA9 ASPSPs in the UK to be implemented by January 2018 - which has had significant third party and industry review.

The Read API data in the UK Open Banking standard covers these key areas:

- Account identification details

- Account balance information
- Account transaction data
- Regular payment information (such as the list of active direct debits and standing orders that have been set up against the account)

Along with the standardisation of the functional API data payloads for the Read data - the OBIE has also standardised the functional flows for how this restricted data will be access. Including how a customer’s consent is managed through the process.

The scope of the Read API data standard for the initial release has been driven by:

- What data is required to meet core CMA use cases such as product comparison, and account aggregation; and
- What data is available in existing ASPSP online channels - to minimise impact to delivery programmes

However, we see this data being extended to meet further future use cases, and prioritised in a pipeline fashion.

Write Data

In addition to the focus on sharing account data via an Open Banking standard - there has also been a focus in the UK and Europe on opening up access to initiate payments via the Open Banking standard (Write API access). We believe that the access to payments via Open Banking APIs are crucial to the flourishing of the Open Banking ecosystem and will encourage FinTech innovation.

The minimum viable product (MVP) for initial release of the Open Banking ecosystem has focused on the ability to initiate a single immediate payment. However, there is a growing belief in the industry that the current MVP release does not go far enough in challenging the position of the incumbent payment providers (such as card schemes). A more holistic set of payment initiation APIs would also include other payments types such as the ability to make:

- Future dated payments
- Deferred or contingent payments
- Recurring payments
- International and cross border payments
- Bulk payments

Along with the standardisation of the functional API data payloads for Write data - the OBIE has also standardised the functional flows for how payments will be made. Including how a customer’s consent is managed through the process.

Recommendations

Options for who should share data for the Australian Open Banking programme include:

- All Australian ASPSPs (banks, card providers and e-money wallet providers) to provide access to data with a standard interface.
- The largest ASPSPs (i.e., Australia's big four banks) to provide access to data with a standard interface, and the remaining ASPSPs to provide access in an unstandardised fashion. This is the approach mandated by the CMA in the UK - though there are clear incentives for smaller ASPSPs in the UK to adopt the UK OBIE standard.
- Entirely optional - with ASPSPs to adopt whatever standard interface they wish.

Our recommendations on who should share data to whom are:

- **All** Australian ASPSPs should provide access to data via a standardised interface, though this could be phased - as:
    - This will level the playing field for all ASPSPs
    - A standardised interface will provide the development community seeking to use Open Banking interfaces in Australia with clarity and simplicity - increasing adoption
    - Reduce barriers for FinTech innovation
- Adopt approach in Europe to third party access - which is that they will only need to be registered with an Australian National Competent Authority (NCA)
- All participants in the Australian Open Banking ecosystem (ASPSPs and third parties) to be authorised via an Australian NCA

Our recommendations regarding the Open Data standard are:

- As ATM and branch details are already available via programmatic interfaces - the focus should be on standardising product information via a standard interface
- The product information structure borrow heavily from the UK OBIE product standard - with an iterative and phased approach to deliver key components of the standard earlier
- Keep the Open data standard publically available - with no restriction to access - as this will make it easier for third parties to access, and provide ASPSPs with less work to secure access to data
- Consider also extending Open Data to cover all standard Australian retail banking account types (e.g. lending products, credit cards, etc).

Our recommendations regarding Read/Write API data are:

- Adopt the UK OBIE standard for Read/Write API data access - as significant work has been undertaken to agree and standardise a structure for this data as well as the functional flows for how this data will be accessed.

How should data be shared?

The predominant mechanism for sharing Open Banking data in the UK and Europe has been via RESTful APIs - using JSON request and response payloads. This has certainly been the approach endorsed by the OBIE in the UK, STET in France, and other FinTech players opening access to data (challenger banks such as Starling Bank and Monzo and payment services providers such as GoCardless & Paypal).

International standards also exist to describe the message payloads for financial data exchange, such as the ISO 20022 standard. However, ISO 20022 is currently an XML interface standard, which is considered heavyweight for an RESTful API design. The OBIE, as part of developing the standards for the Open Data and Read/Write APIs, have borrowed from ISO 20022 standards to develop a RESTful JSON API standard. E.g., ISO 20022 message elements have been re-used where applicable, however, the structure of the JSON payloads have been flattened for developers.

The current UK OBIE standards for Open Data and Read/Write Data APIs are publicly available at:

- https://www.openbanking.org.uk/open-data-apis/
- https://www.openbanking.org.uk/read-write-apis/

For Open Banking in the UK, the OBIE have taken the approach that:

- Open Data APIs are publicly available without restriction.
- Account holders have fairly fine-grained control over customer data that is shared with third parties.

However, the OBIE have standardised the functional flows for how data will be shared for the Read/Write APIs. These functional flows including:

- How a customer's consent is structured (in JSON payloads),
- How this payload describing this consent is sent from a third party to ASPSP,
- How a customer authorises the consent with the ASPSP, and
- How a third party subsequently accesses data based on the authorisation granted

Recommendations

Our recommendations regarding how data should be shared are:

- To aid in adoption - we recommend Open Banking in Australia use standards and frameworks that currently exist
- Use RESTful APIs as the mechanism for data transfer
- Adopt standards for Open Data and Read/Write APIs already developed by UK OBIE - which borrow from other existing standards such as ISO 20022 for financial messaging

- Adopt consent management processes standardised by the UK OBIE

How to ensure shared data is kept secure and privacy is respected?

Any access to an ASPSP's resources needs to performed in an environment that has the following characteristics:

1. Clear identification of all parties involved.
2. Secure and non-repudiable communication channels.
3. Prevention of unintended or unauthorized (accidental or malicious) release of data
4. Performed through a process where the customer's consent can be obtained, verified and revoked by both the requesting party and the releasing party.
5. Technically implemented using standard internet technologies to aid adoption and reduce barriers of entry for all parties.

The UK OBIE trust framework has been designed to ensure that an ASPSP's customer remains securely and centrally in control of all data that has the potential to be shared with third parties. However, the UK's implementation has been heavily influenced by technical, security and aggressive delivery requirements from UK Banks and UK regulators and to align with the PSD-2 Regulatory Technical Standards. These may not be relevant to the Australian Regulatory environment or an Australian Open Banking programme.

In designing an Open Banking or indeed any API ecosystem a careful balance has to be struck between the security of customers and institutions vs the barrier to entry that a high level of technical complexity that an overly defensive security posture may impose on new market entrants.

In addition to participant identification and security, authentication mechanisms used by an ASPSP's customers must be carefully evaluated to ensure that they offer appropriate levels of phishing resistance, and that they can be relied upon to adequately assure both ASPSPs and third parties that the individual authorising the release of financial data is indeed the data owner. This is one of the biggest risks to the successful delivery of an Open Banking programme and the most concerning element of both the UK CMA Order and the EU PSD2 programme.

The CMA9 financial institutions are obliged to deliver API services for their customers by early January 2018. The ASPSPs are required to offer these APIs even if they can not identify their customers via means that would meet the EU PSD2 definition of Strong Customer Authentication (e.g., 2FA minimum) or using a authentication mechanism that is resistant to phishing or customer identity spoofing. The risk that an API service offering coupled with poor quality authentication mechanisms poses to customers, ASPSPs and an Open Banking programme can not be overstated.

More than any other recommendation contained in this submission Raidiam recommends that the Australian Open Banking programme requires all ASPSPs to adopt appropriate identity proofing standards, secure credential usage and secure credential management standards that would meet the levels outlined in the Vectors of Trust standard being considered by the Internet Engineering Task Force (IETF).

The UK OBIE security profile contains several elements that Raidiam anticipates could prove undesirable to the Australian Open Banking program.

The aggressive delivery timeline resulted in the trust framework being significantly influenced by what can be realistically implemented by UK ASPSPs. This resulted in the following compromises:

- A need to support less secure mechanisms for participant identification by some ASPSPs.
- A need to offset the compromises introduced by bolstering other layers of the security and trust framework which increased the technical complexity.

The influence by traditionally conservative ASPSPs as well as a regulatory and liability environment (PSD2 and GDPR) forces ASPSPs to:

- Bear the burden of proof should any data loss or breach occur during or after information has been passed on to a third party.
- Potentially be liable for fines of up to 4% of global revenue under the EU's General Data Protection Regulation.
- Be unable to implement any form of contract between third parties and themselves before releasing sensitive financial data on their customer.
- Be unable to perform any other form of due diligence on a third party apart from confirming that the third party is regulated by a National Competent Authority.
- Be accountable and immediately responsible for customer loss restitution.

This has resulted in the following:

- A requirement that ASPSPs applications and security infrastructure never establish channels of communication with third parties.
- A reluctance to rely on information asserted by third parties in any way, despite those third parties being regulated by Financial Regulators across Europe.

The UK OBIE trust framework serves as an excellent point of reference, however, as the Australian Open Banking programme will be implemented under different regulatory, liability or delivery timelines, then the trust framework under which it operates should be tailored to suit. It will also be possible for an Australian Open Banking programme to benefit from being a 'fast follower' in that the software vendor's support of the new standards will have matured and there will be real world experience of operating the end-to-end solution to draw upon.

Recommendations

Our recommendations regarding ensuring shared data is kept secure and privacy respected are:

- Implement standards similar to the UK Open Banking trust framework, redirect model which ensures that the customer and ASPSP are always certain of permissions granted to third parties with no ability to tamper with these permissions.
- Underpin the open ecosystem by ensuring that ASPSPs implement a robust and secure method for customer authentication that reduces the attack surface for phishing attacks (in line with the PSD2 RTS)
- Adopt common secure web communication protocols (HTTPS) to reach the largest possible audience with a low barrier to adoption.
- Adopt the well known and well supported authorization framework OAuth 2.0 but require the full support for the OpenID Connect Financial API Profile. The profile covers current good practice recommendations for the following areas:
    - Communication channel encryption standards.
    - Payload signature algorithms.
    - Appropriate authentication and participant identification standards.
- Adopt the use of message signing based on asymmetric key so that messages exchanged in the ecosystem offer a strong degree of non-repudiation and forensic records management.
- Review and adopt a national Public Key Infrastructure (Financial) or alternatively define a common trust anchor from which to issue certificates which can be used as a means of identification of authorized participants in addition to message signing for verification and non-repudiation.
- Give customers granular control around how consent is managed through the functional APIs - in line with the UK Open Banking standard.
- Establish methods for exchanging fraud indicators within the ecosystem.

- Produce a balanced delivery plan, with realistic implementation timeframes, which will result in:
    - Improved vendor support and ASPSP adoption of more advanced security technologies, standards and products
    - Consolidation on a more secure standard security layer, which could remove the requirement for significant enhancements needed on lower security layers. This will likely lower barriers to entry for new participants.
- Produce a balanced regulatory and liability framework, which will result in:
    - An improved customer experience provided by the ecosystem - enabled through the bi-directional establishment of channels of communication between participants.
    - A reduction of the need of a trusted intermediary to facilitate communication and trust establishment between parties.
    - A reduction in technical and security complexity of the trust framework.

What regulatory framework is needed to give effect to and administer the regime?

A lot of work has been done in Europe and the UK to define regulatory frameworks. The respective roles of the key UK actors can be summarised as follows:

- CMA: The Competition and Markets Authority is the UK government body responsible for creating and governing the CMA Order.
- HMT: Her Majesty's Treasury is a key stakeholder for Open Banking as the government's economic and finance ministry, maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth.
- FCA: The Financial Conduct Authority is responsible for setting the criteria for and maintaining a Register of all Open Banking participants (ASPSPs and third parties) in the UK.
- Trustee: The Open Banking Implementation Trustee, Imran Gulamhuseinwala, has overall responsibility to define and deliver the UK Open Banking standard in accordance with the CMA Order. In particular, he chairs the Implementation Entity Steering Group, which has senior representatives from the CMA, HMT, FCA, each of the CMA9 and representatives from other stakeholder groups (including challenger banks and third parties).
- OBIE: The Open Banking Implementation Entity is the independent body which is defining the UK Open Banking standard, under the guidance of the Trustee.
- ICO: The Information Commissioner's Office is responsible for governance of GDPR in the UK.

And in Europe, other relevant bodies include:

- NCAs: Other National Competent Authorities who perform a similar role to the FCA in each EU member state.
- EBA: The European Banking Authority is responsible for defining the guidelines on authorisation and registration under PSD2, and in particular the Regulatory Technical Standards (RTS).

However, there are still a number of areas either undefined or open to interpretation. For example:

- The FCA have only just announced the process by which ASPSPs and third parties can register to transact in the UK's Open Banking ecosystem, see https://www.fca.org.uk/firms/revised-payment-services-directive-psd2/implementation and it remains to be seen how smooth this process is.
- There are a number of concerns and differences in opinion as to who and how access is revoked (ether globally by the FCA or individually by one or more participants) for participants who 'break the rules'. In particular, how quickly this can/should happen in the case of, say, a security threat or fraud.

- There are concerns amongst some third parties that if ASPSPs revoke access in error, this could cause serious reputational and financial damage to third parties, and it is not clear what steps will be in place to mitigate against this.
- Whilst much of the liability sits with ASPSPs, how can/should this change to reflect the reality of there being multiple parties involved?
- What insurance will be available for participants, when will the be available and how much will this cost?
- The CMA Order is light on details in some areas and PSD2/RTS is very much open to interpretation and/or still being debated (especially on the topic of direct access / screen scraping). So there is quite a large difference of opinion across the UK programme as to what behaviour and use cases can/should be covered by the standards.
- In particular, there are concerns amongst several third parties, that the APIs may be too limiting based on, for example, restricting API functionality to provide information comparable to what is currently available in a bank's existing online platform.
- What is the role of the OBIE moving forward, who will this be migrated to, over what time frame, and who will pay for this?

Recommendations

Our recommendations for the regulatory framework are:

- The programme should work closely with the Office of the Australian Information Commissioner (OAIC) to review impacts of Open Banking in the context of modern data sharing and privacy, in particular taking learnings from GDPR.
- Rather than rely on other existing frameworks, which may not be definitive enough and/or may contradict each other, the Australian Government should create an equivalent of the UK's CMA Order as self contained legislation which sets out the detailed requirements and scope of Open Banking APIs.
- The details of this Order should take learnings from the CMA Order and PSD2/RTS.
- The Order should apply to all ASPSPs and third parties who trade in Australia, so that the playing field is fair and level.
- There should be a clear and speedy process for onboarding and revoking access for all parties.
- This Order should have absolute clarity about the liability model.
- This should include an effective Alternative Dispute Resolution (ADR) process so that issues can be resolved quickly and without recourse to expensive legal action.
- There should be a dedicated and independent central body which defines and governs this, as well as providing ongoing infrastructure and services to iterate the standards and give support to users, potentially including managing the ADR process.
- There must be a long term vision, and critically a funding model for this, so that there is certainty in the future.

Implementation – timelines, roadmap, costs

In Europe, PSD2 came into force in Jan 2016 and will become UK law in Jan 2018. However, the associated RTS is still in final draft, is not finalised, and will take a further 18 months for ASPSPs to implement once finalised.

In the UK, the process has been costly and taken time (over two years from the initial setup of the Open Banking Working Group in 2015 till the planned main live date in Jan 2018). And it is likely that the programme will continue to evolve during 2018 and beyond, not least because of the need to align to the RTS.

Despite this seemingly long time frame, many key decisions were not agreed until well into 2017 (and some are still not). Hence, the deadline of Jan 2018 is in reality a significant challenge for the industry, with very little time to test before the market is live.

Since Open Banking is a new and untested concept, it would be wise to assume that the needs of end users and third parties will evolve (rapidly) as the market develops, and this will also drive further evolutions in the standard.

It is thus clear that this is a lengthy and costly process in Europe and the UK with no defined end date. However, having no defined end date is not necessarily a problem, and could be considered an opportunity for continual ongoing improvement.

The implementation considerations and recommendations will ultimately depend on the scope of the Open Banking programme in Australia.

Recommendations

Although detailed recommendations are dependent on the scope of the programme in Australia, our high level recommendations are:

- Timelines and costs can be significantly reduced if the Australian ‘regime’ reuses as much as possible from the UK OBIE standard.
- This should include not just the standards for the functional API payloads, but also the OBIE security framework, as both have already gone through significant industry review in the UK and are reusable, with minor changes for the Australian context
- Ensure regulatory framework, governance model (including liability model) and long term funding are in place as early as possible, as the absence of these will cause significant delays during design and implementation.
- Once the above has been agreed, it should be possible to complete the setup and design in the first six months, and then for the programme to go live within a further six months.
- However, there is likely to be a further 6-12 months of live proving, as ASPSPs go live and third parties can accelerate their product development.

About Raidiam

Core services

Raidiam provides independent advice, delivering on the potential of IAM to businesses and their customers in an ecosystem of web and API interfaces to improve business outcomes. We provide the following services:

IAM Thought Leadership

Our work on next-generation technology architectures and the business opportunities provided by a modern, flexible, IAM solution will help your organisation improve customer experience and satisfaction. At the same time we provide guidance that will reduce ongoing costs, reduce time-to-market and deliver a consistent model across your web, mobile and API channels.

Raidiam are members of OIDF and actively contribute to the development of OpenID standards, in particular the Financial API (FAPI) profile (see http://openid.net/wg/fapi/) which is closely aligned to the UK Open Banking security profile.

Solution Architecture

Our well developed reference architecture is based on a number of principles including, 'interoperability', 'scalability', 'modularity', and 'agility'. Our solutions are 'secure by design and default' and support 'internet-scale' service. By combining your requirements with our reference architecture, our architects will tailor a solution that will deliver significant improvements to your business and will provide a roadmap for migration of your existing services. This will deliver an identity-focused solution that can improve business outcomes, improve agility, and reduce risk.

Design and Implementation

We have a highly experienced team skilled at integrating with existing systems and developing design documentation that not only delivers a technical solution fits with modern DevOps operational capability. Our specialists integrate IAM components, including Ping Identity and Forgerock, with other systems and provide customisation where it make sense. We will help you deliver a solution that meets your business needs today and into the future.

Contact details

For further details, please contact us:
info@raidiam.com
Raidiam Services Limited, 50 Brook St. London, W1K 5DR, United Kingdom.

Glossary

The following glossary of terms is used throughout this document:

Term	Name	Description
AISP	Account Information Service Provider	Any organisation registered with the FCA (or NCA) as approved to access the Account/Transaction APIs (Read APIs).
API	Application Programming Interface	In general terms, a set of clearly defined methods of communication between various software components.
API Provider	n/a	Any ASPSP or ATM provider who enrols with OBIE to provision Open Data API endpoints.
API User	n/a	Any individual or developer who builds web/mobile apps which connect to Open Data API endpoints. API Users do not need to enrol with OBIE nor be registered with any authority.
ASPSP	Account Servicing Payment Service Provider	Banks and building societies who will provision the API endpoints.
ATM	Automated Teller Machine	An automated teller machine (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access most ATMs.
BCA	Business Current Account	Current account product for business entities.
CCC	Commercial Credit Card	Credit card product for commercial entities.
CMA	Competition and Markets Authority	The UK Government body which has created the legislation (CMA Order) to 'enforce' the largest UK Banks to comply with the UK Open Banking Standard.

CMA9	CMA9	The 9 largest banking groups in the UK which are covered by the order: Allied Irish Bank, Barclays, Bank of Ireland, Danske Bank, HSBC, Lloyds Banking Group, Nationwide Building Society, Royal Bank of Scotland, and Santander.
EBA	European Banking Authority	The European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.
FAPI	Financial API	A profile of the OpenID specification
FCA	Financial Conduct Authority	The official UK organisation who maintains the register of approved ASPSPs, AISPs and PISPs.
GDPR	General Data Protection Regulation	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU)
HMT	Her Majesty's Treasury	HM Treasury is the UK government's economic and finance ministry, maintaining control over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth.
IAM	Identity and Access Management	Identity and access management (IAM) is, in computer security, the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons".
ICO	Information Commissioner's Office	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
IETF	Internet Engineering Task Force	The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet

		architecture and the smooth operation of the Internet.
MVP	Minimum Viable Product	A minimum viable product (MVP) is a development technique in which a new product or website is developed with sufficient features to satisfy early adopters. The final, complete set of features is only designed and developed after considering feedback from the product's initial users.
NCA	National Competent Authority	Any other country’s equivalent to the UK FCA.
OAuth2	n/a	OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean.
OBIE	Open Banking Implementation Entity	The body which creates and maintains the Open Banking Standards in the UK, including these guidelines.
OpenID	n/a	OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords. With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. Other than your provider, no website ever sees your password, so you don’t need to worry about an unscrupulous or insecure website compromising your identity.
Participants	n/a	In this context a collective noun for ASPSPs, TPPs (both AISPs and PISPs), API Providers and API Users.
PCA	Personal Current Account	Current account product for personal entities.
PSU	Payment Service User	A personal or business retail banking customer.
PISP	Payment Initiation Service Provider	Any organisation registered with the FCA (or NCA) as approved to access the Payment Initiation APIs (Write APIs).

PSD2	Payment Services Directive 2	The revised Payment Services Directive (PSD2) is the EU legislation which sets regulatory requirements for firms that provide payment services.
RTS	Regulatory Technical Standard	Regulatory Technical Standards on strong customer authentication and secure communication, which are key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.
SME	Small to Medium Enterprise	A category of micro, small and medium-sized enterprises.
TPP	Third Party Provider	In this context a collective noun for AISPs and PISPs.