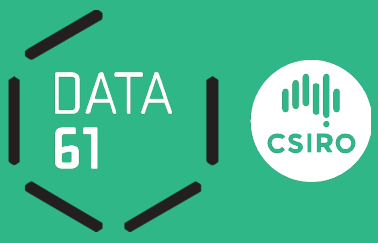


CDR Open Banking Workshop: Defining the UX of Consent

Prepared by: CSIRO Data61

12 November 2018

CDR Open Banking Standards Use Case Workshop

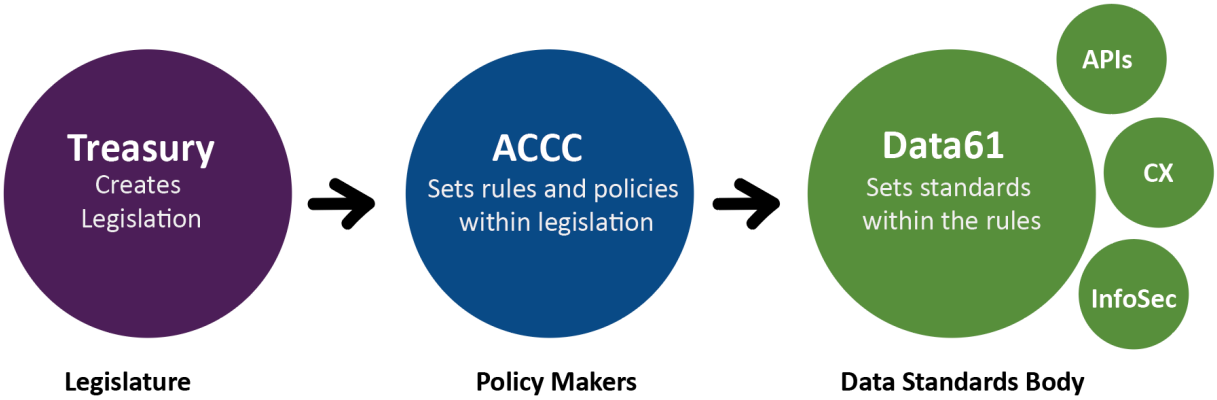
30 October 2018 - ATP, Level 5, 13 Garden Street, Eveleigh

1 November 2018 – Community Hub at the Dock, 912 Collins Street, Melbourne

About the Consumer Experience Work Stream

The Consumer Experience (CX) Work Stream within the Data Standards Body exists to support the technical delivery of open banking, due to commence from 1 July 2019. It must offer practical guidance on:

1. The consent experience for consumers accessing open banking (how consent will be framed by Accredited Data Recipients)
2. The authorisation and authentication experience for consumers (how authorisation and authentication will be sought by Data Holders)
3. Authorisation Management (how consumers can monitor and change authorisations in an ongoing fashion).



The Consumer Experience Work Stream does not have a policy-setting role. While insights that emerge from UX testing in the process of designing a consent experience may inform policy development, the Work Stream does not have a role in:

- Defining consent at a rule-making or legislative level. It will test practical mechanisms for seeking consent in the context of open banking, informed by the emerging rules and legislation
- Identifying/surveying consumers on market opportunities and interests in making better use of banking data. While the need to move to UX testing necessitates choosing some practical use cases to test, use cases are selected purely for the purposes of designing consent and authorisation prototypes.

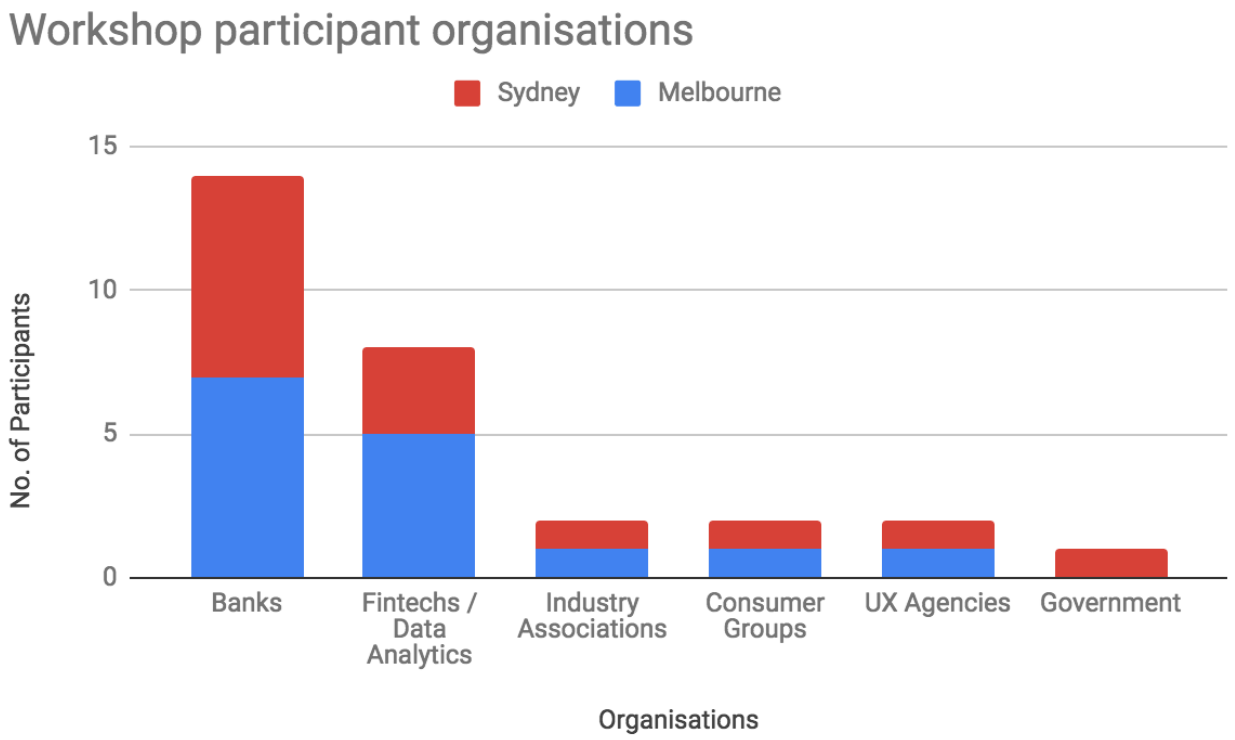
Essential deliverables for the Consumer Experience Work stream between November 2018 – January 2019 include:

- Review and advice on existing payload structures (scopes and claims) for the purposes of describing to consumers what they are consenting to
- Testing of simple consent, authorisation and authentication experiences for consumers, for the purposes of agreeing to initial guidelines on these features for Version 1

Workshop Summary

User Experience and Consumer Research practitioners active in Open Banking were invited to participate in the development of consumer research, written advice, user journeys and wireframes that form the deliverables for the CDR Consumer Experience Work Stream.

The workshops were held in Sydney and Melbourne on 30 October and 1 November 2018 respectively. A total of twenty-eight people were in attendance across both workshops, with seven participants identifying as User Experience practitioners.



There were four activities at the day long workshop:

- *Use Case Review:* Focussed discussion on the use cases to be used to help define and test standards.
- *User Flow and Interface Review:* Discussion on existing user flows, interfaces and wireframes describing consent models for accredited parties to use in seeking consumer consent to access their information, specifically the Open Banking UK Customer Experience Guidelines.
- *Consumer Language and Payloads:* Participants were asked to describe existing payloads, reflect on consumer language to be used, and the logic of data clusters.
- *Research Brief Review:* Discussion regarding the research around consumer comprehension of consent and experiences navigating various authentication, consent and authorisation flows being explored within the information security work stream.

Reflections and Comments

A broad range of reflections and comments on each activity were captured and are detailed in the 'Workshop Activities and Notes' section of this document. Testing will examine issues raised by participants that are within the remit of the Consumer Experience Work Stream for Version 1. Below is a list of key questions to be answered in CX testing:

Questions on the Consent Experience

- What kind of data language, clustering and granularity will give consumers sufficient control of their data, without diluting comprehension?
- What is the best way to clearly explain what an organisation will do with the data a consumer consents to share?
- What extra measures may be used to aid comprehension for vulnerable consumers and those experiencing financial distress?
- What qualitative and quantitative measures may be used to determine the success of a specific consent experience?

Questions on the Authorisation and Authentication Experience

- How distinct do authentication, authorisation and consent stages need to be for consumer comprehension, ease of use and security?
- What language and designs should be used to explain trusted entities and accredited status? *Note: The accreditation process will not be defined by ACCC until March 2019. Testing that occurs before this date will use proxy information and language.*

Questions on Authorisation Management

- What level of friction do consumers expect around reauthorisation and long term consent, specifically redirect and decoupled flows?
- What does a clear experience for the revocation of consent look like? What do consumers expect and understand around deletion, de-identification and derived data? *Note: The ACCC is currently determining the rules around consumers revoking access to their data, including deletion and de-identification.*

Further Participant Questions and Concerns

Important questions raised by participants at the workshops have been answered below.

What is out of scope for July 2019?
- Mortgage applications
- Payments
- Non-digital banking
- Consent for minors and deferred authorities

Will consumers be able to manage their consents outside of data holders? Centralised consent management should be part of CDR.
Consumers will need mechanisms to keep track of organisations they have consented to share their data with, and so revoke consent. At present, information about organisations a consumer has consented to sharing data with are captured as part of the process of authorising a data transfer with a data holder. The DSB will provide guidelines on the consumer experience for data holders making visible to consumers the organisations that consumer has authorised accessing the data they hold, and processes around revocation. A centralised management interface supporting consent management from across multiple data holders and associated consent APIs are out of scope for the CDR in Version 1. As the DSB is only empowered to mandate the standardisation of information in accordance with the ACCC rules, it will feed back to the ACCC interest across the workshops in centralised consent management, for possible inclusion in later versions of the rules supporting the CDR.

Will there be further research? The first round of research is inadequate if it is all that's contemplated.
This is the first round of research and testing to be conducted by the CX Work Stream. It is intended to give initial insights and direction for standards that need to be implemented by July 2019. Further rounds of research are expected with the standards adapting to those further research insights. See CX roadmap below.

How might the risks and rewards associated with Open Banking be communicated to consumers, especially in non-banking scenarios?

It is difficult to predict the full extent of the risks and rewards associated with open banking and the CDR. Version 1 of the standards will only consider banking or financial services use cases that will be deployed or are already in the market for July 2019. However, the perceived *potential* risks and rewards associated with open banking will affect adoption by consumers. We will discuss with stakeholders the contribution further research will provide into better understanding consumer acceptance of the potential risks and rewards associated with open banking, and how these might be communicated in such a way that consumers may make informed decisions on data sharing.

What criteria are being used to select use cases for testing?
It is important to note that the CX work stream deliverables focus on standards and guidelines supporting consent, authentication and authorisation of data sharing only. They do not

standardise use cases that are contemplated under the CDR, or try to prescribe which use cases should be considered. The work stream employs use cases to provide context for behavioural testing. The context within which consent is given needs to be understood to inform what a consent flow will look like, the kind of language to be used as a bare minimum and the consumer expectations about the granularity of access to information that would be contemplated. With that in mind the following criteria have been set for test use cases:

- Current services: use cases will reflect services on offer in market right now including those relying on web scraping (for 1 July 2019, most tangible examples that should move to APIs)
- Consent duration: use cases will cover both point in time purposes for sharing data and ongoing data sharing (to explore re-authorisations and consent duration)
- Payload breadth: use cases will have sufficient coverage of all payloads in scope (to ensure that no payloads are unused)
- Range of needs and behaviours: use cases will apply to/affect/could be used a cross-section of consumers (e.g. low-income, financially savvy, financially illiterate, applying for a loan or credit card; personal budgeting and debt advice)
- Business and individual: use cases will apply to a mix of both SMEs and individuals

Workshop Activities and Notes

Below is a summary of participant comments and questions raised as part of each activity during the workshop. This capturing of feedback does not necessarily reflect endorsement by the Data Standards Body. Comments and questions made by workshop participants have helped to inform the CX workstream's activities and next steps.

Activity 1: Use Case Review

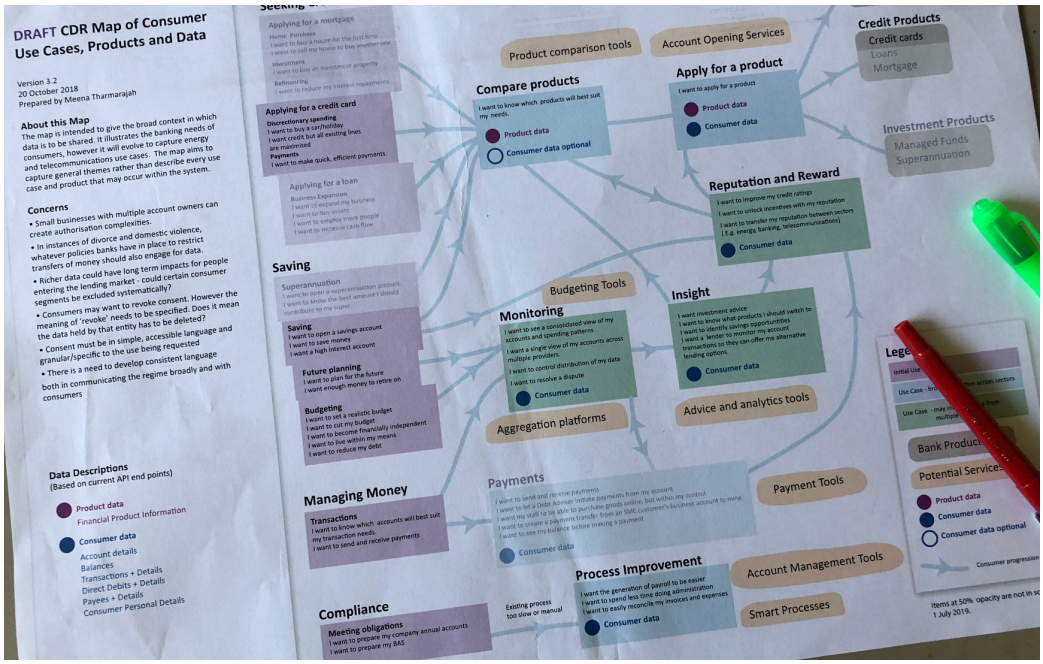
The Activity

Participants were asked to review a use case map that gave an overview of the main use case areas affected by Open Banking. Use cases are a statement of how a user is likely to use a system. Strong use cases help teams to clarify key requirements, come to consensus on an approach quicker, and expose elements that might be outside of the project's scope.

The use case map articulated what was to be in and out of scope for 1 July 2019. Once participants were familiar with the overall map of use cases, they were asked to review a set of primary use cases to be used for testing and research. This set was collected by Open Banking UK, in their research phase. Participants were asked for comments, questions and importantly any additional use cases that should be considered as part of this primary set.

At the end of the discussion, participants were asked to vote on what they thought were the most important use cases, and to then discuss why they had voted on specific use cases.

The Consumer Experience Work Stream will select use cases from those discussed during the workshop to frame user journeys in UX testing and explore consent, authorisation and authentication mechanisms.



Map of use cases (see appendix for full use case map)

Participant Reflections and Comments

There were some general issues that arose in discussion that applied to all use cases:

- **Scope for 1 July 2019 is not clear**
  Several participants were not clear on what is to be in and out of scope for 1 July. There were questions around where phase one intended to cover individuals as well as businesses, also the lack of inclusion of mortgage applications which has been deemed out of scope.
- **Consider time and duration of a use case**
  The duration of a use case and more specifically the duration of a consent was discussed by participants as being an important factor. Consent may be ongoing, but will need re-consent to occur, some consents will expire. Research was expected to uncover consumer expectations around this. In addition, many uses cases are ongoing (e.g. budgeting), these will need consideration on how they may be tested.
- **Create criteria for the selection of use cases**
  The use cases put forward for review were provided by Open banking UK, however the evaluation criteria is not clear. Additional information is needed on whether or not these use cases were the most common ones practiced in the UK

The following are comments and questions from participants that accompanied the specific test use cases presented along with additional use cases deemed important in both workshops. Each participant was given two votes.

Product comparison and account switching

- For appropriate product comparison product features will need to be standardised, across products and institutions – a huge task.
- Consumers will need to transfer their payee lists for useful account switching.
- How do we make sure consumers are given control and choice over the data they share, without overwhelming them? The granularity of the data choices presented to users needs to be tested.
- How might this and other use cases work where consumers are downloading their data?

Compliance

- Explicitly draw out the use case regarding taxation - for example, a real time view of receipts and transactions for the purposes of accounting (not just on 30 June but at all times - helps with deductions)

Online purchases

- Balances that are collected via APIs may not be up to date and accurate
- Purchasing can occur not just from a retailer but from third parties such as AfterPay. Some of these purchases might be facilitated by NPP, with payment innovations replacing peer to peer models.

- Be careful not to assume just retailers are facilitating these payments - it could be an intermediary such as AirBnB or PayPal, facilitating payments on behalf of a retailer.
- For SME purchases the use case concept may vary from authority to pay concept.
- Gumtree is an example where there are risks around payment. Could this be used to understand a user's capacity to pay? Could this help to reduce risks around payments?
- From the consumer's perspective, what changes is the risk associated with a payment. There's a lot of explaining to do for consumers to be comfortable sharing their information with unfamiliar intermediaries and gateways. Could these models be tested with consumers, for example testing the same journey with:
    - Payments with a retailer (potentially simpler option)
    - Payments via gateways and intermediaries (where they would need an explanation of how the ecosystem works)
- Users may want to check their balance before committing to a payment. It may be easier to just check your balance via your account rather than go through the consent and authorisation flow with the retailer.
- Payments covers a range of use cases, and will need dedicated discussion. However they are out of scope for 1 July 2019

Lending

- Consider long term consent, where a user may take out a loan and then want ongoing offers and discounts on better deals
- Consider scenarios in which rewards are given to users for reducing overdrafts
- There are concerns around predatory lending particularly for consumers who regularly overdraft (e.g. a payday loan company peppering vulnerable consumers with loan offers). Notifying consumers that they might be approaching an overdraft situation is viable and positive, but more consideration needs to be given on how to prevent predatory lending in an open banking environment.
- If we design for these special cases - for the vulnerable consumers - then we could design something that is inclusive, that works for the widest range of people.
- Consider looking specifically at loan applications and how long applications may become shorter. Is KYC information to be part of the data to be shared, and can entities truly be aware of their customer if they have merely received that data from a third party?

Debt advice and micro-savings tools

- This use case is useful for everyone, not just financially distressed consumers
- How will consent work when someone else is given the authority to consent for someone else (e.g. children, power of attorney, helping someone manage their money, deceased estates)

- Control is a big issue for people in financial distress. When someone needs to watch their money carefully, they may be more reluctant to give up control to others.
- The growing group of vulnerable customers are those who are used to having some liquidity, used to having income, and have seen the cost of living creep up. They are not prepared for financial distress.

Revoking consent

- Where there's ongoing access there will need to be some means of revocation of consent
- There may need to be information provided at the point of providing consent explaining how data will be stored, deleted, identified.
- Will banks keep records on reputation after I revoke consent?

Consent management

- Consent is such an integral part of the open banking regime – why is consent management not part of the scope? For this to occur there need to be consent management APIs, opening up opportunities for intermediaries to manage consent. This would involve management of who I've given consent to, how that consent is managed, how it can be revoked.
- Consumer data management - consent and authorisation management. Consider business models that allow consumers to manage their consents. (Discussion in the room around difference between consent and authorisations management, authorisations management currently being contemplated with individual data holders.)
- Most of these use cases are about establishing a relationship - not managing those relationships going forward (which is where consent management becomes important).
- Authorisation is a necessary part of consent, the manner in which this is to be handled needs to be defined. Should this be managed as part of a consent management tool?
- Consent management could provide a mechanism to articulate more information about exactly how data will be used and by who and for what purpose, between entities. That way a consumer who begins to feel like they're getting strange deals or interactions they're not comfortable with, can trace back through their detailed consents and understand how that's occurring.
- Should the date on which consent is granted align with the date on which authorisation to receive data is actioned?

Automated Profiles / Non-banking use cases

- Secondary non-banking use cases that will take advantage of the availability of data were considered important to consider. For 'genuine consent' to be given by consumers to share their data, they need to understand where that data might land.

- Direct marketing was considered a likely secondary use case however others such as insurance (health, life, car) were also noted.
- An important consideration is the automatic building of profiles of consumers based on their shared data and without their explicit permission. These could be used by those within and outside the banking industry.

Priority Use Cases

Participants were asked to vote on the use cases they thought should be used as a basis for testing experiences of consent, authentication and authorisation with consumers.

The voting exercise was designed to generate discussion around the reasons why participants held certain use cases to be important. Several of the use cases listed below are out of scope for testing (see page2 for criteria on test use cases), however the reasons participants gave for voting on use case scenarios have and will be given serious consideration throughout CDR discussions.

Votes for both workshops have been combined and use cases with no votes have not been included. See the appendix for a full list of use cases.

Use case	Voting Reason	Votes
Account switching and product comparison	Common challenges and points of friction for lots of consumers	**3**
Account aggregated dashboard	Most/widest use and requires regular access	**9**
Lending - Using transaction data to qualify for a loan	One of the main use cases consumers will take up	**5**
Alternative lending - I want to find alternatives to bank account overdrafts by giving a lender access to my account transactions.	Explores the benefits and the risks for vulnerable consumers	**4**
NEW **Consent management** How do I cancel / revoke and delete data after sharing	Integral to understanding / tracking consent	**14**
NEW **Automated profiling/data used outside banking** (Dating apps, health insurance etc)	Examines risks and rewards that flow on from Open Banking *Note: Sydney participants did not consider this use case, as it was added in the Melbourne workshop.*	**12**

Debt advice tools for the financially distressed	Explores the benefits and the risks for vulnerable consumers	**1**
Micro saving and budgeting tools for the financially distressed	Explores the benefits and the risks for vulnerable consumers	**1**

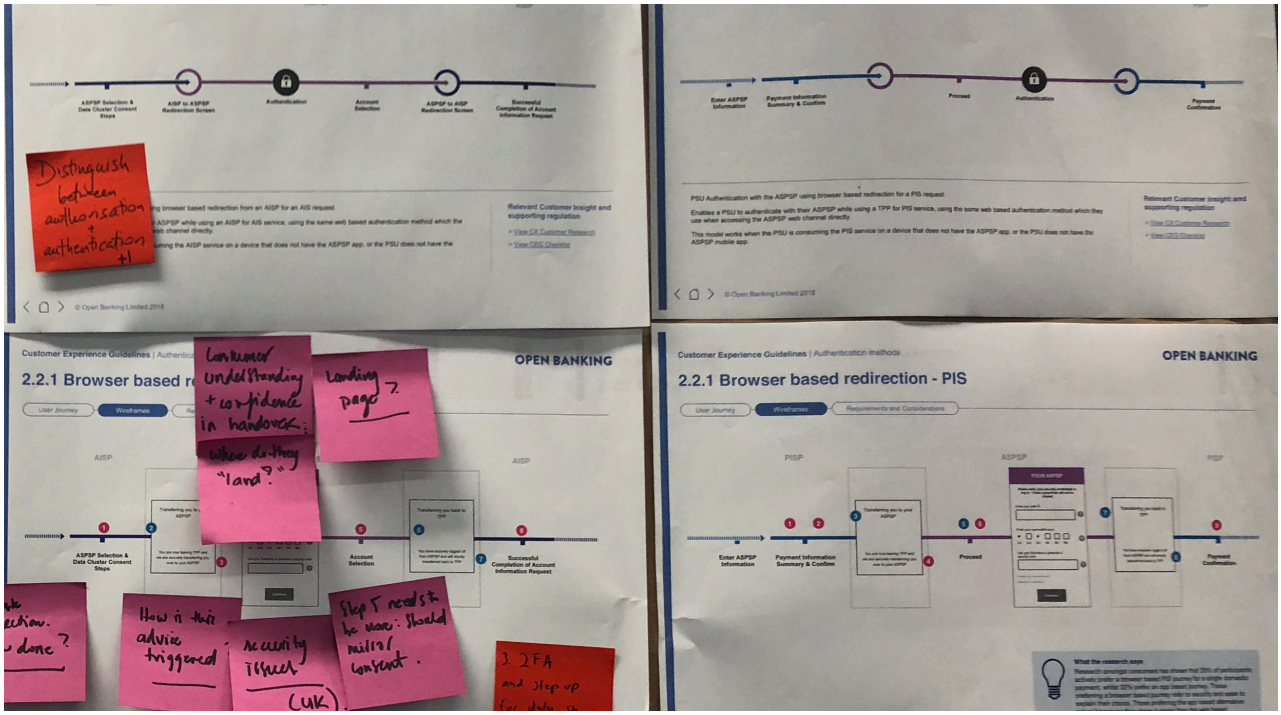
Activity 2: User Flow and Interface Review

The Activity

Participants were asked ahead of time to review the Open Banking UK Customer Experience Guidelines. These detailed wireframes and flows are to be used as a starting point for the CDR Open Banking Consumer Experience standards.

In this session all of the available flows were displayed, and the participants asked to discuss the user journeys and wireframes contained within them. Particular emphasis was placed on changes that should be made to the guidelines based on work participants were already undertaking related to these flows.

Unfortunately participants at the Melbourne workshop did not have time to start this activity.



Participant notes posted on the UK Open Banking Customer Experience Guidelines

Participant Reflections and Comments

Consent, authentication and authorisation

- Need to separate out consent, authentication and authorisation clearly when presenting guidance to the technical implementers

Redirect and decoupled flows

- The UK is moving to support decoupled models as well as redirect approaches.
- Communication about the manner in which redirect occurs is important as you are leaving one environment and being redirected to your banking environment. Is the redirect screen the responsibility of the data holder, or the data recipient?
- One bank participant has tested both redirect and decoupled flows and noted that the redirect flow created unease among participants while the decoupled flow - while creating friction - had greater trust. However no specific scenarios or use cases had been used to setup context for the participants, just a review of how they might want to get their data from one entity to another - testing the suitability of those flows.
- Potentially different use cases will need different levels of friction and security. When is it appropriate to use redirect and decoupled flows?
- Would be interesting to understand who the consumer trusts in these interactions. Who does the consumer want their relationship to be with?
- When users are selecting their bank, How do we order a list of banks for consumers to select from (their data holder), for the purposes of authentication and authorisation? There are obvious benefits to being at the top of the list.
- How does re-direct feel? In one banking model users go straight to the internet banking log in page. Should there be some kind of landing page intermediary?

Authentication and Consent

- Wireframes indicate that authentication happens automatically (push authentication, consumer presented with authentication immediately) - do consumers want that?
- There's an expectation that what is consented to will mirror what is presented to the consumer to authorise. Do we need to make clear from a UX perspective what will be required at each stage (consent, authentication, authorisation) - rather than each of these items merging together?
- One banking participant would like to be able to introduce language as part of authentication and authorisation, alerting consumers to the fact that data may not be held securely by third parties and liability accompanies the sharing of the data. This is important to test to understand how consumers might be disincentivised from sharing data. Language should be explanatory and truthful.
- App based redirection - there are different authentication models (PIN, swipe, log in with customer credentials, faceID). If someone is using faceID, and doesn't move to a specific landing page, how do you get positive affirmation from the consumer? There are sophisticated fraud detection tools for customer logins being used by banks (they monitor regular consumer login patterns and detect fraudulent logins, pass that back to the consumer). There needs to be an expansion of error codes for data holders to pass back to accredited third parties, more descriptive than a 'pass/fail' capturing instances like fraudulent behaviour.

- Multi-banked consumers going through consent and authorisation processes, with every bank, every 90 days will experience some stress. If they set up all their accounts at one time, every 90 days they will need to reauthorise again. This is an area where consent management could be valuable. Rather than a consumer reauthorising, with every different entity, they could designate one entity to manage all of this on their behalf.
- Consumers could be dealing not only with different banks but different re-direct and decoupled approaches to reauthorisation. Varied implementations of authentication and authorisation, coupled with reauthorisations, could reduce consumer trust. Consistency of this implementation is important, so customers learn what they can expect (not five different flavours of redirect). Reauthorisation could be separated from authentication.
- There was some confusion among participants (who are speaking with some level of background knowledge of the UK models and their own implementations) about what 'authentication' is, and who does it in this context (discussion about it being data recipients who are *authenticating* identity).
- The data holder should notify consumers when a change is made to the status of their data (e.g. it has been shared, consent has been reauthorised)

Consent Granularity

- What level of granularity do consumers want to consent to? To be tested.
- The UK consent screen wireframe (3.1) is designed for simplicity, with some information given and options open to consumers to explore what they're consenting to, should they want to. Should this design accommodate more complexity, and should consumers be given more information? Existing services in Australia don't give the level of detail required in the current UK UX guidance (it's just, "you are giving us access" and "we're linking your accounts" – Existing services were cited as examples).

Incentives

- How might incentives be disclosed? For example if a consumer is being offered a service, then they should know if the entity offering that service standards to gain a reward/incentive for directing them through that service.

Data Minimisation

- Data minimisation should be explicit. How do we prevent recipients from asking for more data than they need?

Mobile first

- The UK CEG uses a 'mobile first' approach, is this appropriate?
- Designing for mobile is important because (a) mobiles are widely used (b) because it has the smallest screen real estate – it is easier to enhance a mobile view for desktop, than to to do the reverse.

Revocation, deletion and derived data.

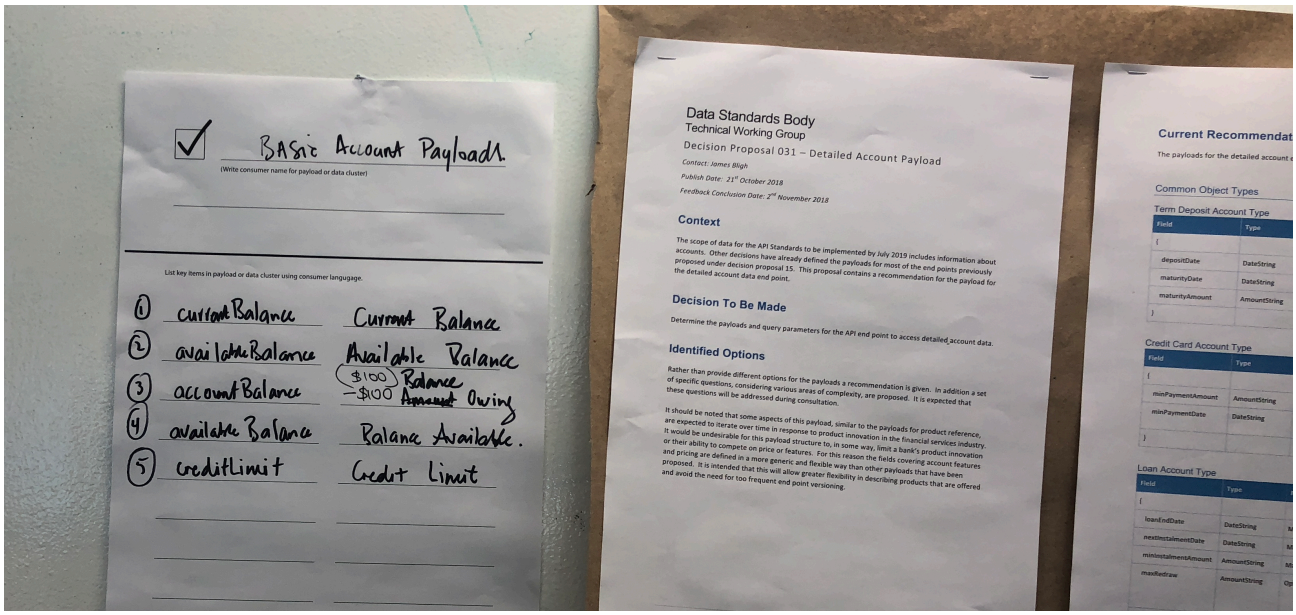
- The reason data is to be shared needs to be given to the consumer at all points so it can be approved or revoked.
- When a user decides to stop sharing their data is the data deleted automatically? Is the data that was shared now deleted? When a user revokes access, do they need to choose to delete the data the data recipient already has? Consumers need to know what has been deleted and what has been kept.
- When will deletion be used and when will de-identification be used? If de-identification is to be used, what form will it take?
- Are there scenarios where data can't be deleted due to legal obligations? Does derived data fit into this category?
- What happens to derived data? Are there different types of derived data that will need to be treated differently?

Activity 3: Consumer Language and Payloads

The Activity

In small groups participants reviewed a set of payloads. A payload is a set of data that is delivered via a specific API end point. Each of these payloads or data clusters needs to receive a consumers consent before it is shared.

Groups were asked to review what was in the payloads and imagine a user needed to give consent to release one of the payloads for a specific use case. Participants needed to define how the payload would be described so that a user could give informed and genuine consent. Participants were asked to note concerns and questions.



Payload proposals reviewed were:

- Decision Proposal 026_Customer.Payloads

- Decision Proposal 027_Basic.Account.Payloads
- Decision Proposal 028_Transaction.Payloads
- Decision Proposal 029_Direct.Debit.Authorisation
- Decision Proposal 031_Detailed Account Payload

Participant Reflections and Comments

Logic of data clusters within payloads

- Participants were concerned that too much detail is being shared in each payload - could consumers provide more granular consent for items within each payload? Consumers may only want to share small amounts of data within each payload. Consumer research shows customers don't like being asked for information that isn't required for the purposes of delivering that service.
- There was a recognition that presenting too many 'buckets' of data could overwhelm users.
- As the payloads have been created at quite a high level, with many different items contained within them, it is likely data recipients will be collecting data they do not need. This is particularly true for the transaction and customer payloads.
- When do you need to share various sets of information and for which use cases? They appear arbitrary at the moment, and we won't know if they'll work until you test them. If we approached these 'buckets' in relation to use cases, then we would probably cluster them differently. These would determine common, logical groupings for consumers. It would then be very evident how to explain these
- Some of the payloads are clustered elegantly from the perspective of communicating to consumers. Two are hard to explain (for the purposes of seeking consent) - perhaps these need re-clustering (work back from use cases/how you would explain them to a consumer and re-sort the fields):
    - Account payload
    - Customer payload

Customer Payloads

- Suggested name was: 'Basic customer information'
- Several items were noted as being problematic or unnecessary:
    - Gender (this has been removed)
    - Prefix – often not captured and reveals marital status, which may change
    - Date of birth, which is a sensitive piece of information used to check identity. The age of user can be useful for segment pricing, but this could be attributed to categories (e.g. under 18, under 65, over 65).

    - Some users will only have a single name
    - Occupation is difficult to define and changes over time. Generally your 'job' is your specific role, whereas 'occupation' is the field you work in. Codes for occupation, are difficult to match up.
- There needs to be clarity on why this payload would be used. Consumers will already have opened accounts with data recipients and will already have entered this data.
- Use cases for this payload could include credit card applications and account switching, where uses can avoid filling out lengthy applications. This needs to be verified in testing.
- Customer matching would be inappropriate for this payload. Checking to see if the "Julian McKay" associated this entity is the same Julian McKay at another entity is hard to verify.
- The fields to change include
    - 'Person' changed to 'Information about me'
    - "Business" - changed to "information about business"
- In the 'detailed customer information' payload, address fields need to be more granular.
- Personal and business account information is contained within one payload. There was confusion about how the customer payload would work in situations where an authority on a business account is involved. Would information about individuals as well as about businesses be shared in this payload? Some participants thought the business and person payloads should be separate payloads.
- What is the "short name" for a business? Is this the same as a trading name? (e.g. Australian Broadcasting Corporation with short name 'ABC')

Detailed account payloads

- At a high level, there are five key pieces of information for consumers to understand:
    - Current balance
    - Available balance
    - Account balance
    - Credit limit
- Should there be so many words for a consumer? What do they understand? Customers have different balances, but do they understand the difference between them all? This is complicated for consumers - the data cluster language might just be "balances".
- "Credit limit" has different connotations. For example, a person signing up for a product comparison might only want to give permission for credit limits but not balance on that credit card.
- Credit limit is currently a mandatory field, but some credit products won't have credit limits (example CityBank charge card).

- Masking - how will masking apply across banks? Account ending in 3859 - if fields are masked differently across banks, comparison will be difficult...is this right?
- What is the difference between a product and an account, and how are they related? When do fields associated with a generic product (in the product reference payload) and fields associated with an account need to correspond?

Direct Debit Authorisation Payload

- Rename this “automatic payments”
- What matters to a consumer is that they are making “automatic payments” - they’re not really thinking about the difference between direct debit and credit card
- What is it we’re trying to convey to a consumer:
    - Who you are paying
    - Your bank (financial institution)
    - Most recent payment choice
    - Most recent amount

Transaction Data payload

- Rename this “transaction history”
- Scopes are too flat, they need to be tailored and appropriate to the use cases. Transaction data is a goldmine for many companies, this is more sensitive than the customer payloads, where a lot of information can be derived about a user. There need to be different payloads in this set that hide details that are not needed, especially information about what the transaction is. At least one payload should just be incoming and outgoing figures.
- The way these products are described (debit and credit) are from a bank’s perspective, not a consumer’s - a consumer doesn’t necessarily understand the difference between debit and credit.
- “Basic transaction” to a bank means one thing; to a customer it might be a much smaller set of information (how much, to whom, when)
- Suggest using the phrase “Details of your transactions coming in and out of your accounts” (not explicit fields).
- This payload seems to be well clustered in terms of consumer language. It is straightforward to explain to a consumer what is being shared without having to go into too many details.
- There should be move levels of granularity for transactions including
    - Setting timeframes
    - Limiting transactions to a particular person (especially for joint accounts, or accounts where there are multiple card holders)

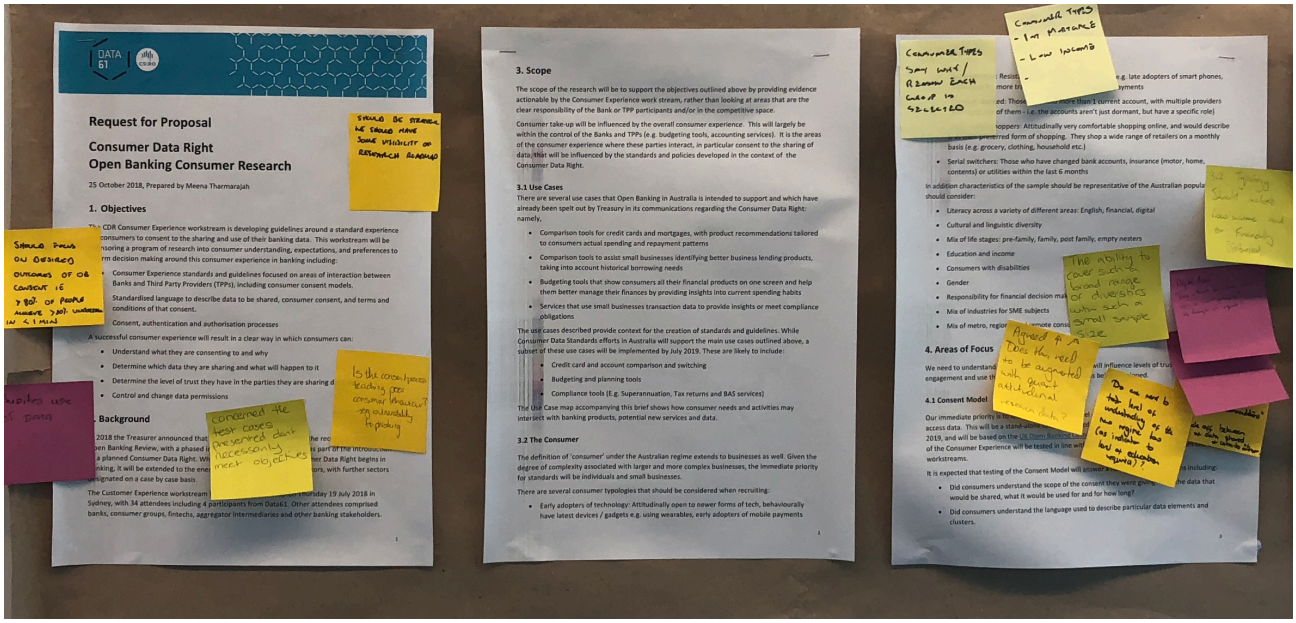
- Nothing allows the customer to scale back transactions on the account that they might not want to share.

- Many participants felt the reference field should be removed as it has the potential to hold sensitive information.
- "Running balance" - should that be in the basic payload
- Need to be clear about the definition of "transaction" - consumers would expect it to correlate with the list of transactions on their online bank account
- Disclosure of consent
- Different language is used to describe the same information being consented to. To what level can we mandate the kind of language that is used on consent screens?
- Feed back to the ACCC the importance of accreditation as part of insulating misuse and curtailing use cases.
- Can there be a payload just for credit summary and debit summary?
- Use case to verify income - can we design a payload just for income?

Activity 4: Consumer Research Review

The Activity

Participants were asked to review a Consumer Research request for proposal covering consumer consent, authorisation and authentication. As in all other activities, comments and questions were captured.



Notes from participants attached to the Consumer Research RFP

Participant Reflections and Comments

Use cases for testing

- Map the use cases for this first round of testing with what reality will look like for day 1 (e.g. budgeting tools - they're already in the market, most likely to be ready for day 1).

Recruitment

- Vulnerable people should be considered an important user group.
- Recruit for level of engagement with digital banking services
- If you think of it as a matrix: low engagement and high engagement, high value and low value: look for high value, high engagement, and test with them.
- Financially distressed consumers should be included for testing (distinct from vulnerable).
- Consider life moments (E.g. people who are applying for credit.)
- Need to consider non-digital people (people who do not have internet access).

Trust, consent and consumer expectations

- The level of trust in the system will be crucial for adoption.
- Consumers need to understand what they are consenting to and why (and understand the consequences).
- There should be consequences for organisations misusing data.
- Data usage should be audited. How can organisations be held to account?
- Is the consent process teaching poor consumer behaviour? E.g. phishing.
- Consumers may be concerned about how their data might be misused.
- Use the research not only to provide consumer views of the consent process, but of what this regime will be.
- There are many factors that contribute to customer trust in the system: who is registered; Are they visibly registered? How are they registered? Is it government regulated; is the regulation to be trusted? How do I trust it? Do I trust it in screen scraping more than government regulation?
- Is data deleted? What are the expectations around revocation of consent?
- Do customers feel in control of their data? Do customers understand where and how their data is being used?

Incentives

- What kind of incentives would customers like to share data? What might the value exchange be? Feedback among participants that this might not be phase 1.

Research activity is too constrained

- Need more people to be included in the study for it to be valid - suggestion that 50 people would be more valid. Another suggestion that 20-30 people is fine, but only if a subset of the criteria for recruitment is addressed.
- There are too many criteria that need to be addressed.
- The test cases don't necessarily meet objectives - the test exercise is being time boxed, resource constrained and poorly funded; feels like we have one shot and we might miss it. Is there more to this than just this one set of research?
- Are we constraining the research too much? It seems bad to go out to organisations prescribing their research.
- Consent is a weighty subject, and we're doing this in a very constrained way.
- Augment this research with other quantitative measures

Strategy

- What is the overall roadmap? There needs to be some visibility of this, and it should cover strategic goals. We need to understand what is on the horizon.

Outcomes and Measurement

- Focus on design outcomes for open banking consent: What does "good consent" look like; what does "bad consent" look like? What outcome are we trying to design for? At the moment, the outcomes are qualitative, not quantitative.
- What does 'successful' mean? And should speed of understanding be a factor or not? How much friction should be present? Terms such as "Appropriately fast and familiar". Or "Friction commensurate to experience". Could be used to determine success measures.

Language

- Ensure alignment around language with the other processes within the CDR, especially the technical.

Appendix A – Defining the user experience for consumer consent Agenda

See PDF File

Appendix B – Open Banking Consumer Research Brief

See PDF File

Appendix C – Use Case Map

See PDF file

Appendix D – Use Cases for testing

See PDF file

Appendix E – Consumer Language and Payloads

See PDF file

Appendix F – Customer Experience Guidelines

See PDF