Consumer Data Right

Data Standards Body Advisory Committee

Minutes of the Meeting

Date: *Wednesday 10 October 2018*

Location: *Data61, Level 5, 13 Garden Street, Eveleigh*

Time: *14:00 to 16:00*

Meeting: *Committee Meeting No: 4*

Attendees

Committee Members

Andrew Stevens, DSB Chair
Kate Crous, CBA
Martin Granell, AGL (via WebEx)
Mark Perry, Ping Identity
Lauren Solomon, CPRC (via WebEx)
Lisa Schutz, Verifier
Ross Sharrott, Moneytree
Stuart Stoyan, MoneyPlace (via WebEx)
Gary Thursby, Westpac (via WebEx)
Andy White, Australian Payment Network
Patrick Wright, NAB (via WebEx)

Observers

Warren Bradey, Data61
Ellen Broad, Data61
Seyit Camtepe, Data61
Terri McLachlan, Data61
Meena Tharmarajah, Data61
Mark Staples, Data61
Stephen Bordignon, ACCC
Bruce Cooper, ACCC
Anjelica Paul, OAIC
Daniel McAuliffe, Treasury

Apologies

Emma Gray, ANZ
John Stanton, Comms Alliance
Luis Uguina Carrion, Macquarie Bank
Mal Webster, Endeavour Mutual Bank
Viveka Weiley, CHOICE

Chair Introduction

The Chair of the Data Standards Body opened the meeting and thanked all committee members and observers for attending Committee Meeting No 4.

The Chair noted that DSB is making solid progress and there is good communication and interactions with the other related agencies. He also advised that there were discussions being held on the energy sector's inclusion within the CDR and that more will be disclosed on that in the future as options for its inclusion were further contemplated. However, it was noted an accelerated introduction for the energy sector is being considered by the Government.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 6 September 2018 Advisory Committee Meeting. The Minutes were taken as read and formally accepted.

Action Items

The Chair noted that the status of the Action Items were either completed or have been included on the agenda.

It was noted that the discussion held on cadence at the September Advisory Committee Meeting (page 3 of minutes) referred not just to cadence in correspondence with the Advisory Committee but cadence for the working groups. Committee members noted that Decision Proposals to the technical working groups should adjust to a regular schedule as well. The DSB committed to looking at cadence in totality and making changes to the technical working group deadlines for feedback so that they could better fit proposals within their own workloads.

It was advised that the publication of the working draft standards to be published in early November will be the totality of all the decisions so far and that reviewing this from an overview perspective (as distinct from decision by decision) will be the focus for discussion at the November meeting.

ACTION: Working Draft Standards v1 to be added as an agenda item to the November meeting

Technical Working Group Update

API Standards Working Group

A summary of the progress from the last committee meeting on the API Standards Working Group was provided by Ellen Broad.

The team has been extremely busy over the past month with a large number of Decision Proposals posted for general comment. It was noted there has been strong participation from the eco-system participants contributing comments on GitHub. We are grateful for the energy and support from everyone on these discussions.

It was noted that as the next phase of development we are moving into defining the payloads for each of the end points and that the following Decision Proposals were posted on Monday 8 October, which remain open for feedback:

- Decision Proposal 026 – Customer Payloads
- Decision Proposal 027 – Basic Account Payloads

Decision Proposals on Accounts and Balance are due to be posted today (10 October) with more to follow within the week.

A discussion was held on the Designation Instrument that would clarify the specific information to be included for rule-making for the banking sector. Treasury advised that the consultation period for this document closed last Friday. Treasury advised that they would like to settle this as soon as possible but do not need to have it closed off until early next year.

In discussion it was queried whether the Designation Instrument could be versioned and Treasury advised that they prefer the Minister only issue a single Instrument for the sector. It is intended that the Designation Instrument will cover all information the government is contemplating as in scope up to July 2020.

A discussion was held on the working draft standards and it was noted that some of the elements may/will change based on the rules as they are finalised. The ACCC and the DSB are working closely together, as both the rules and standards are being developed, to align them as much as possible.

A discussion was held on impending delivery timelines. Committee members expressed a broader preference to go simple and narrower to ensure the sector can meet the 1 July 2019 deadline.

The Committee discussed the option of holding face to face working group sessions and if the Data Standards Body was open to that option.

It was confirmed that the DSB has already commenced scheduling face to face workshops. It held the first API Working Group Workshop in Melbourne last week which was very successful and the DSB is aiming to do more from November onwards, once the draft working standards are published. It was also advised that the meetings will align to committee meetings where possible.

Information Security Working Group

Seyit Camtepe, who is currently leading the Information Security Working Group (ISWG) provided an update on the progress from the last meeting.

Since the last meeting, a further Decision Proposal has been issued on Use of TLS-MTLS (Decision Proposal 033). This relates to a series of specific technical decisions in relation to the security of communication between participants in the Consumer Data Right Regime. There are four specific decisions contained in the proposal which are:

- The adoption of TLS and MTLS to secure communications between CDR stakeholders;
- Use of cryptographic primitives;
- Support for Certificate Bound Access Tokens; and
- Certificate Extensions

A discussion was held on the cryptographic primitives and the NIST key size guidelines and whether there will be an orderly way to upgrade the bit size. It was agreed the DSB need to document how this will happen in the guidance notes with the standard.

It was agreed that the DSB would streamline and narrow the focus of Decision Proposal 033, issuing a revised version.

A discussion was held again on cadence, the volume of decision proposals coming over the next few weeks in the lead up to the first full draft set of standards, and the difficulty for teams responding when we post at ad hoc times. It was agreed that whilst the DSB needs to continue to post decisions as quickly as possible, we will in future treat decisions published Monday-Thursday in a week as being published on the Friday, and feedback deadlines will be the following Friday.

A discussion was held on some of the core components on content and security protocols and having visibility of the timing. The Committee noted it is important to publish these as soon as possible to provide the banks and other participants sufficient time to build/test and meet the deadline.

It was advised that some of these will be posted next week and will intersect with the ACCC's rules.

The importance was reiterated by the Chair of using GitHub to provide comments and feedback as this will help us greatly in the intense period from now to November when the first working draft of the standards will be published.

The Committee discussed the intersection of the information security standards with the build of the Directory by the ACCC and the importance to understand how these will operate as soon as possible.

ACCC advised that they are using the Digital Marketplace for a two stage procurement process as they saw this as the quickest way to develop the Directory. It was acknowledged that it is an important element in the process. ACCC advised they are evaluating the first round of EOI's and will move forward to shortlisting and issuing RFQ shortly. ACCC noted Data61 have been helpful in providing expert advice on the specification development.

A discussion was held on the Rules Framework and whether it will cater for non-digitally enabled / offline customers and how many people this would affect. It was confirmed that this will not be included in version 1 of the rules. It was noted this will be a larger issue for other sectors of the economy when they become part of the CDR regime as in many sectors the interface with customers is non-digital to a significant extent.

It was noted that the bank branch network will always be available for the non-digitally enabled banking customers who can use branch facilities.

ACTION: ACCC to provide an update on non-digitally enabled customers and the effects for banking and other sectors.

A discussion was held on whether the Information Security Working Group had met face to face and if there are any plans for such meetings. It was noted there is a preference for face to face sessions as well as GitHub. It was confirmed that concurrent face to face meetings across each of the work streams will be held from November onwards. It was also noted that if there are any particular, sensitive points that needed to be discussed offline, the team were happy to arrange suitable time to discuss these issues.

A discussion was held on Open ID's Financial-grade API (FAPI) Read/Write API Security Profile. It was advised that the starting point for the ISWG will be the recently revised UK open banking security profile, which is based on FAPI Read/Write API Security Profile. Working with the FAPI elements will ensure consistency with global protocols including OAuth and OIDC, and reduce reinvention of the wheel whilst still providing us with the opportunity to adjust for any specific Australian context.

It was noted that whilst Australia is similar to the environment in the UK, that we are subject to more cybercrime attacks. It was suggested any unique contextual challenges for Australia should be taken into account in drafting information security standards.

A discussion was held on the adoption of the TLS stack and the trouble with the new TLS version numbers. The new version of the encryption protocol TLS 1.3 may lead to a redesign of the TLS version-negotiation mechanism and we need to be thoughtful of that before adopting it in version 1 of the standards.

Further discussion was held on how the DSB could best operate the Technical Working Groups – closed ecosystem vs GitHub. It was noted that the DSB will have to make public all the technical decision proposals, and is following standard protocols, but that some security issues may not be desirable to discuss in a public setting. Nonetheless, the DSB noted that its final profiles will need to be made public to enable eco-system developers and system integrators to build to a known end point. It was discussed whether we could have a closed GitHub to discuss sensitive security issues to satisfy some concerns raised. It was agreed that the DSB will meet with participants offline to discuss sensitive issues affecting security standards development.

User Experience Working Group

Meena Tharmarajah has commenced at Data61 as a strategic adviser on the user experience work stream. She introduced herself and provided some details on her background and experience.

Ellen Broad provided a summary of the progress of the User Experience (UX) Working Group since the last committee meeting.

It was confirmed that we have two new members of the team. Meena Tharmarajah who will provide strategic support and Michael Palmyre who will provide support for the set up phase of the UX Working Group.

It was noted that the 2 November draft will be at the technical level only and will not include UX guidance and language for seeking consent.

In Nov-Dec, guidance and testing of consent and authorisation with diverse consumers will be undertaken. We know from insights from UX research that insights from user testing may lead to adjustment to some of the API and information security standards on payloads and authorisation flows, which we will do in parallel as part of testing the draft standards over the Nov-Dec period.

A discussion was held in regards to the 90 days reauthorisation limit rule proposed in the rules. It was noted that this may not be appropriate for the energy sector and may cause friction in certain elements of the banking sector where longer reporting periods are the norm. It was noted these issues will need to be considered in the period through to the end of December in conjunction with our UX workshops.

It was flagged to the committee that two UX Workshops are planned at the end of October and early November where the intent is to define the deliverable for November and December and the questions that need to be answered. The workshops will be held in Sydney on Tuesday 30 October and in Melbourne on Thursday 1 November. It was requested that participants bring along any pre-existing research that can be shared and that separate meetings can be organised for those that are unable to attend.

Draft Standards Publication Timetable

It was noted the Data Standards Body is currently still on track to meet the publication timetable as noted in the committee papers.

The timetable is taken as read.

Open Banking approaches in other jurisdictions

The report on open banking initiatives around the world included in the committee papers is taken as read. Committee members were encouraged to reach out to Warren Bradey if they would like additional information.

ACCC Rules Framework Update

Stephen Bordignon from the ACCC provided an update on the Rules Framework.

The ACCC Rules Framework was released publicly on 12 September 2018 and the ACCC has been consulting extensively with stakeholders. It was noted submissions on Rules Framework close on 12 October, 2018 and the ACCC is targeting December for release of the draft rules.

The ACCC noted the following issues had been raised in Rules Framework consultation meetings:

- Balances/interest rates: there had been wide support for inclusion of balances/interest rates in data sets.
- Consent: discussion on joint accounts had raised a range of views from authorisation should follow authority to transact to either account holder can authorise (with or without notification of the other account holder) to allowing ADIs time to create a mechanism for account holders to create specific data sharing permissions. ACCC noted the need to consult further in determining what should be included in version 1 of the rules.
- Minors: allowing minors and other vulnerable customers to authorise data sharing received a lot of commentary. Consideration is being whether to exclude these from version 1 of the rules.
- Time limited consents: a range of comments had been received on 90 day re-authorisation and will be considered further.
- Accreditation: the requirement to meet particular security standards, remains an important issue for the ACCC to specify further. ISO accreditation was likely to be considered as too onerous for new Fintechs.
- Compliance: a lot of queries had been received about what ex poste auditing would look like, and the ACCC confirmed further consideration was being given to this issue.
- Use of data: handling redundant data included a range of views on both deletion and de-identification and will be considered further. Some suggestion that it should be at the election of the customers.
- Reciprocity: the ACCC noted that a reasonable number of comments had expressed a desire to provide for reciprocity from day 1 and that some smaller ADIs had expressed a desire to opt into CDR as data holders earlier than planned.
- Other sectors: the ACCC noted that there had been interest from energy and telecommunications industry participants as to whether all the Rules will carry over to those sectors and noted that there was likely to be a core set of rules of general application and some rules that would be sector specific, or vary the application of the generic rules.
- Tiers of accreditation: different levels of accreditation for data recipients is noted as important for many smaller participants.

Draft Legislation Update

Daniel McAuliffe from Treasury provided the following update on the Consumer Data Right Legislation.

Part of the legislation was re-released for a second round of consultation on 24 September 2018, with new submissions closing on 12 October, 2018. These provisions relate to the scope of the regime, the Privacy safeguards and the sections to support reciprocity.

It was noted that Treasury will need to introduce the Bill in the last week of November as the following week will be the last sitting week of the year.

One thing that has been changed is which derived data may be subject to mandatory access arrangements. Deciding what is to be considered covered will no longer be left to the Rules. Instead, derived data subject to mandatory access will only be included where it is specifically outlined in the Designation Instrument.

- Intellectual Property will have to be considered in deciding what data can be designated in scope;
- The only data not relating to an identifiable person that may be subject to mandatory access will be product data.

The second round of the Bill submission included a range of technical issues including:

- The scope and operation of reciprocity;
- Simplification and clarification of the interactions between the Privacy Safeguards and Privacy Act;
- Pricing of access and use of data not included in the designation Instrument as being free
    - The Minister can specify what is to be provided free of charge – if it is not specified to be free then data holders will be entitled to charge for access. A market based mechanism will apply on what charges are appropriate. The ACCC can only step in when a fee is unreasonable.

Other changes:

- Limitation on CDR consumer definition to persons or their associates who receive supplies of goods or services;
- We have reviewed the Designation Instrument and tried to reasonably restrain it.
    - The description of data included in the Designation Instrument may widen some of the payloads. The Designation Instrument will not specify a highly granular exhaustive list of data sets, they will be specified in the standards and rules.

It was reiterated during the discussion that:

- CDR data is data ‘related’ to a CDR consumer, a broader concept than information ‘about’ an identifiable person;
- Privacy safeguards will apply to data recipients in respect of CDR data they receive through the CDR system.

Other Business

In regards to the open banking in other jurisdictions agenda item committee members were encouraged to reach out to Warren Bradey if they would like additional information.

The Chair thanked everyone for their input and reiterated that we are making good progress. It was noted the next couple of months are going to be very intense as we look at the standards in total and consider the information security issues in face to face meetings.

Meeting Schedule

The Chair advised that the next meeting will be held on Thursday 15 November from 2pm at the Data61 offices in Canberra.

Closing and Next Steps

The Chair thanked the Committee Members and Observers for attending the meeting.

Meeting closed at 4:00