Consumer Data Right

Data Standards Body Advisory Committee Banking Sector

Minutes of the Meeting

Date:	*Wednesday 13 November 2019*
Location:	*Data61, Level 5, 13 Garden Street, Eveleigh*
Time:	*14:00 to 16:00*
Meeting:	*Committee Meeting No: 16*

Attendees

Committee Members

Andrew Stevens, DSB Chair
Kate Crous, CBA (via WebEx)
Mark Perry, Ping Identity
Lisa Schutz, Verifier (via WebEx)
Ross Sharrott, Moneytree
Lauren Solomon, CPRC (via WebEx)
Stuart Stoyan, MoneyPlace (via WebEx)
Erin Turner, Choice (via WebEx)
Jamie Twiss, Westpac
Mal Webster, Endeavour (via WebEx)
Andy White, AusPayNet
Patrick Wright, NAB (via WebEx)

Observers

Mark Staples, Data61
James Bligh, Data61
Rob Hanson, Data61
Terri McLachlan, Data61
Michael Palmyre, Data61
Louis Taborda, Data61
Bruce Cooper, ACCC
Ying Chin, OAIC (via WebEx)
Angelica Paul, OAIC (via WebEx)
Daniel McAuliffe, Treasury (via WebEx)
Matt Clifford, APRA

Apologies

Emma Gray, ANZ

Chair Introduction

The Chair of the Data Standards (DSB) opened the meeting and thanked all committee members and observers for attending meeting no 16.

The Chair noted that the DSB had the first meeting this morning with the Energy Data Standards Advisory Committee (EDSAC). It was noted that there is increasing interest in the implementation of the Consumer Data Right (CDR) across the media, industry and government and the formation of the EDSAC has pushed that along and is attracting attention.

The Chair noted that Matt Clifford from APRA is joining as an observer and is attending today's meeting.

The Chair noted that he, Louis Taborda and Mark Staples met with Tim Goodwill from the Department of Home Affairs who has a stream of work in relation to API standards. Tim asked that we look into their standards work.

The Chair welcomed Ying Chin as the new representative from the Office of the Australian Information Commissioner (OAIC) and noted that Anjelica Paul is moving onto other opportunities. It was noted that Ying joined the EDSAC Meeting earlier today.

It was noted that Emma Gray from ANZ was an apology for today.

It was noted that Lisa Schutz from Verifier and Lauren Solomon from CPRC also attended the EDSAC meeting and the Chair appreciates their commitment to participate in both Advisory Committees to provide an important link given we are implementing an economy-wide regime, not implementing sector by sector standards.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 9 October 2019 Advisory Committee meeting. The Minutes were taken as read and formally accepted.

Action Items

The Chair noted that the Action Items were either completed or would be covered off in scheduled discussions.

It was noted that the action item in relation to ACCC to provide an update on the accreditation process and AAT review rights will be provided by Treasury later in the meeting.

Technical Working Group Update

A summary of progress since the last committee meeting on the Working Groups was provided in the Committee Papers and was taken as read.

Treasury Update

Daniel McAuliffe from Treasury provided an update as follows:

It was noted that the Grant Thornton review had been actively gathering input from participants and agencies and are in the process of preparing their advice.

Treasury noted that in the last meeting there was a question about whether accreditation decisions are reviewable by the AAT and whether a third-party can challenge decisions. It was noted that the AAT Act states that a person must have an "interest" in the decision. It was noted that Treasury's view is that other competing businesses do not have sufficient interest in the outcome of other persons' accreditation decision outcomes to support them seeking an AAT review. It was noted that Treasury are examining whether the current regime provides enough certainty about this. It was noted that the AAT Act contemplates other regimes specifying more detail about reviews by the AAT.

The Chair noted that if someone's own application is denied, they can challenge that but if someone else wishes to challenge a decision about your application, they may not have sufficient interest.

One member asked if they don't have any confidence in the security or privacy established by an accredited party, can they seek a review. Treasury noted that it depends on how much interest in the outcome you have. It was noted that it may depend on whether you were being harmed yourself. Treasury also noted that parties can go to ACCC or the Registrar with these concerns.

ACCC noted that there are provisions to report concerns to them. Treasury noted that the ACCC have powers to suspend or place conditions or even strike off an ADR.

Treasury noted that a draft of the Privacy Impact Assessment (PIA) report from Maddocks is with the agencies for final comments. It was noted that there have been few changes, but some things have been added such as recommendations relating to a warning for consumers. It was noted that Treasury will consider how to respond in the next week. In response to a question as to whether agencies are bound by the recommendations of the PIA, Treasury noted that strong consideration must be given to any recommendations but acknowledged that all recommendations to change the rules don't necessarily have to be adopted and, if adopted, not necessarily for February.

One member asked whether the Maddocks report is for Treasury's eyes only or will it be published. Treasury confirmed that the report will be published, together with responses to its recommendations.

ACCC Update

Bruce Cooper from the ACCC provided an update on the rules and the register as follows:

In relation to the request at the last meeting for information why one of the selected ten initial data recipients had dropped out, it was noted that this party realised that they wouldn't be able to satisfy accreditation and testing requirements in time. It was noted that the ACCC did consider a replacement but decided that 9 was sufficient. It was noted that there is one remaining data recipient who is "close to the line" regarding expected readiness.

A member at the previous meeting had also asked for an update on communications. The ACCC noted that there is a Working Group between Treasury, OAIC, DSB and the ACCC on communication for consumers, data holders, and data recipients. It was noted that this is starting to develop some products, and the first will be a series of "Frequently Asked Questions" (FAQs). It was noted that the ACCC is developing a single CDR website, but for the present, each agency had CDR releases on its own website. It was noted that future education videos will cover a number of things from accreditation, consent flows, some of the benefits of use cases. It was noted that ACCC will be looking into info graphics and FAQ information sheets in other languages, after the first lot of FAQs.

It was noted that the ACCC are acutely aware that smaller banks and the wider community of data recipients are seeking more information. The Chair noted that the next tranche of ADIs are starting to ask where they can access material and what they need to do. There was a brief discussion about whether the ACCC's proposed website or the Consumer Data Standards (CDS) website would be an appropriate channel and the importance of consistent messaging. The ACCC is to consult further with the DSB.

In relation to accreditation, it was noted that the ACCC have arrangements and draft accreditation applications for most of the initial nine recipients, and that assessment is currently a manual process. It was noted that in parallel with the testing, the ACCC are working through whether the nine satisfy the draft accreditation criteria. It was noted that the ACCC plan to have an accreditation platform in production in January/February 2020, when accreditation will be open to other data recipients.

One member noted that there were two aspects of the draft application that were a surprise. The first was that it requires an ASAE 3150 (Standards on Assurance Engagements) certification which is less than three months old. It was noted that it is likely that none of the nine would have that ready by 1 February 2020, as Ernst & Young (EY) have advised that this process would take approximately three to five months to complete. It was noted that members have been talking in this meeting about ISO 2701 and SOC 2 for a long time but that this was the first time the member has seen ASAE 3150 (which appears to be close to SOC 2) being required. It was noted this new requirement will be hard to meet for the February deadline. The ACCC advised that if a participant had one of these other certificates, the ASAE assurance would only need to focus on the aspects not included in the other certificates. The ACCC to confirm at the next meeting.

ACTION: ACCC to provide an update on the ASAE assurance report at next meeting.

The same member noted that the second surprise was the requirement to be part of an external disputes body and noted that they will start to look into this and see if any of the external bodies listed will allow them to join, but that is still unclear because they are not in financial services. The ACCC noted that they have been talking to the Australian Financial Complaints Authority (AFCA) and they will accept participants. Another member noted that they succeeded in joining AFCA. The Chair has suggested that it would be helpful if the first member contacts AFCA as they have established a "CDR Stream" for any complaints.

Another member noted that they will also have the same issue providing an ASAE 3150 report.

It was noted that a document in the papers has responses to a number of questions on interpretation of the rules. The ACCC confirmed this has been provided to the DSAC members and would be published widely shortly, likely after the Rules have been made.

The ACCC noted that they are conscious that intermediaries are an important issue, but that the rules don't allow them to the extent they are not outsourced service providers within the meaning of the Rules. The ACCC noted that "passive" intermediaries may be simpler and be able to be dealt with, for example service providers who do not have consumer data disclosed to them. The ACCC noted that they will be sending out a newsletter next week or so with a proposal, and plan to have some draft rules for comment by the end of the year.

One member noted that single vs concurrent consent is still an issue for them. ACCC noted that the rules don't specify this one way or the other. For the DSB decision proposal, ACCC's preference is option three, but noted two concerns. The first is whether this would cause issues for any of the 13 participants in testing and ability to launch in February 2020, and the second is whether adopting that approach now may pre-empt possible changes for consent and consumer experience next year. ACCC noted that they have discussed this with the DSB and have come to the view that it shouldn't have a big impact on the possible future changes but are still unclear about what impact it will have on the 13 participants.

The API & InfoSec Lead summarised the third option in the decision proposal. It is based on standard OAuth 2.0, where going through the full consent flow again results in a new set of tokens. If there was a pre-existing token, you would have two sets and in the dashboard for the holder and the recipient there would be two entries where the intent of the second entry would be to apply to a different purpose. It was noted that if there was a desire to re-establish an existing purpose, then you would go through the full flow, but at the beginning the recipient would supply the previous refresh token as an optional claim in the request object and the holder would provision the new refresh token as per normal and then revoke the previous token identified with the new claim. It was noted that you would end up with only one entry in the dashboard at both ends rather than two, and that this is a way to extend one consent whilst also allowing new concurrent consents for different purposes.

It was noted that the challenge for this proposal is the February milestone and whether the proposal has a low implementation impact. It was noted that the proposal would enjoin data recipients not to seek to create instances of concurrent consents until July. It was noted that from February to July, recipients would act as if single consent was required, but that if creating a re-authorisation, they would supply the refresh token in the request object. The holders would then be able to optionally implement the single consent or the new concurrent consent standard, whichever is easier, with the expectation that all holders would implement the new standard by July.

One member noted that they should be pointing their team back to option 3 and the API Lead confirmed this request.

One member asked whether the security team has looked into this. It was noted that this is still under TLS (transport layer security) and the token is being passed in the request object. The API & InfoSec Lead noted that there has been no feedback so far with these concerns. It was noted that the intent is that the old token is revoked when it is sent through. The API & InfoSec will take this concern on notice for review.

The ACCC noted that while they think that the proposal is good from a consumer perspective, they want to understand the impact to current participants for February. It was noted that the ACCC intend to write to the 13 participants to understand the impact.

One member requested that we reiterate what the 3 options are. The API & Infosec lead did so. The first option would be to move to a full consent flow but stay with single consent and add a consent API to carry the multiple purposes and the additional complexity. The general consensus was that this is not possible for February, and also spoils the field for future approaches to fine-grained consent. The second option was to remove the requirement for a single consent. That leaves data recipients in a scenario where they can't do a reauthorisation to maintain a single entry in the dashboard. They would have to proactively revoke the previous consent, or otherwise there would be multiple consents laying around. It was also noted that treating reauthorisation as revoking and reissuing a sharing arrangement might confuse matters for the rule's requirements for deidentification and deletion.

It was noted that option three is perceived to best meet the needs of recipients and holders, and that is why it is the preferred option. It was noted that a key point for February is the proposal which maximises flexibility for the holders in that they can implement the single or concurrent approach under the standard until July 2020, while ADRs would need to supply a new field for February only if they are doing reauthorisation. One observer noted that the ADR's main constraint would be not having a single consent, but this is what they would be faced with anyway under the current standards. The change and additional effort for an ADR would only be in relation to re-establishing a consent.

It was noted that if a husband and wife share an account they are considered by the holder as one consumer, so they could not each establish separate sharing arrangements for the same account under a single consent constraint.

It was noted that originally the standards adopted single consent because earlier versions of the rules framework implied that was required. The ambiguity arose because the standards didn't seek to reiterate the rules, and the rules shifted to not imply a constraint, but the standards stayed the same in that regard.

One member noted that for February, single consent requirement is probably a significant constraint on the full CDR regime. It was noted that an easy way to resolve it would be to allow the regular OAuth and take the constraints out of the system later. It was noted by an observer that this is exactly option two, which leaves the ADRs in a scenario where if they are re-authorising, they are left in a difficult situation being able to demonstrate that a reauthorisation has occurred.

One member noted that this is why the accreditation process is in place, to ensure that participants behave correctly. The ACCC responded that the accreditation process determines whether you are a fit and proper person, rather than operate as an on-going behavioural norm.

ACCC repeated that they are proposing to satisfy themselves that every one of the 13, is okay with the preferred option. It was noted that ACCC will write to the 13 within the next day or so for feedback.

One member noted, that in principle the further you get from OAuth standards the more bespoke development it requires. However, it was noted in response that for February, delaying the holder implementation requires no extension of the OAuth standard.

One member noted that consent traceability is one of the most important things, and they think there is a need to see the history, and so they like option three.

One member noted on intermediaries, the assumption is that ACCC will initially address the intermediaries that are structure-related, such as Telstra, IBM, cloud service providers and other carriers of information as opposed to more complicated data sharing. The ACCC confirmed that this is correct.

One member noted in regards to accreditation they have joined AFCA and that AFCA is ready for CDR participants. The member supported the previous point on accreditation but agreed that there is a tight timeline and noted that they are struggling to find the right auditor for February.

ACCC noted that the Testing Working Group is meeting weekly and the pairs have started working with each other and that the ACCC is getting a view on how those pairs are travelling. It was noted that the ACCC will share some deidentified status reporting at the next Advisory Committee Meeting.

ACTION: ACCC to circulate a de-identified document showing the status of the pairings and other testings at the December Advisory Committee meeting.

One member noted an area of concern was that until we are testing with the registry in place, we are not doing complete end-to-end testing. Testing is necessary to confirm whether the registry works the way we all think it will.

ACCC noted that their impression was that people have certificates, enabling manual testing of the registry for the next two weeks. One member noted that they have no concerns that mutual TLS will work, the concern is whether they can get the keys from the registry and use them. ACCC noted that this is two weeks away.

One member noted that following the Monday call, they are concerned about authentication and the nuances and details of how the registry works, that there continue to be changes and those changes require engineering on how they interact with the registry.

ACCC noted that it is their understanding that it will be ready in 2 weeks' time. It was noted that all the changes that are being made, are being discussed and agreed in the Testing Working Group meeting and they are only being made unless there is complete agreement. It was noted that the changes are being made for good reason and with participants' agreement.

One member noted that historically, the only way to get the data in a digital way is by screen scraping and whilst the CDR will look slightly different, how do we make sure we are using it the right way and comparing the data like for like when we go live.

One member noted that so far in the Testing Working Group they are only willing to use synthetic data so there will be no testing to see if the data is real until production. It was noted that at that point, the member will do a screen scraping and a CDR comparison but would prefer to do that before "go live" if possible.

A discussion was held on whether the regime could have a sandbox environment where it could provide a safe haven for testing by volunteers. One member asked where the liability would sit. It was noted that as a sandbox, there would be an additional paper consent.

One member noted a risk that the data might not be what it says it is, and they don't want to provide the customer with wrong information.

One member noted that as part of the controlled "go live" testing, they don't trust any system that is working if any part of it is mocked.

Other Business

One member asked in relation to the desktop sandbox QuickStart environment. It was noted that this currently requires a username and password to get access to GitHub and they were wondering if that was the standards credentials that are required.

The Head of Technical Delivery will take that on notice and get back to the member out of session.

ACTION: Head of Technical Delivery will provide an update of the standards credentials.

One member asked how the maintenance backlog is prioritised. The API & InfoSec Lead noted that the Chair committed to prioritising and endorsing the prioritisation and the DSB indicated that there would be a call for the prioritisation of the backlog before it went to the Chair. It was noted that this call occurred (23 October 2019) and the backlog was submitted to the Chair and approved. It was noted the main principle was through community consultation and that phone call, bearing in mind the importance for February and for resolving immediate term issues and the capacity of the standards team and again bearing in mind that we are all busy with testing.

The API & InfoSec Lead noted that most issues were included, and only three issues were not prioritised. It was noted that since then, another urgent change was included which was raised after the prioritisation period finished. The issue came out of the testing regime and has been published in v.1.0.1 earlier this week. It was noted that of the remaining backlog, nine issues have been dealt with which were the urgent change and other queries, and eleven are in the awaiting approval stage. It was noted that these issues will be rounded up after the four-week consultation phase and will be discussed at the next phone call as advised via the mailing lists and which is scheduled for 20 November. It was noted that there are five issues with questions for the committee to respond to and two that do not yet have a recommendation. It was noted that the DSB has worked through about 90% of backlog and is on track for completing the iteration including the extras by the end of next week.

One member noted that at a previous meeting we advised that we circulate the operating model policy to the committee for review. It was noted that this has been previously sent to the committee members, but it would be resent.

ACTION: To resend the policy on the Operating Model to Advisory Committee Members and Observers.

The Chair noted that it would be useful to provide a list of backlog items and the treatment, status, priority and the prioritisation criteria that we use in the committee papers for each meeting.

ACTION: DSB to provide a list of backlog items at each committee meeting

One member wanted to clarify that the prioritisation of the backlog was being conducted and approved by the Chair. It was noted that the Chair approves the prioritisation of the backlog.

One observer noted that the Maintenance Operating Model is in trial mode and that we would welcome feedback on the process.

One member noted with interest the Senate Committee on FinTech and RegTech includes the issue of payment initiation and wanted Treasury's thoughts on that and how the community will be consulted on that issue.

Treasury noted that there is expected to be a long reporting time before the Senate Committee makes a recommendation. It was noted that in parallel, Treasury is doing some thinking internally about enhancing CDR functionality in general. It was noted that the focus is on getting banking sorted. Notwithstanding that there may be some Treasury discussions with stakeholders regarding future functionality, there is no government commitment to write access or payment initiation at this time.

One member asked, relating to intermediaries, what kind of underlying infrastructure would be allowed as a services provider. It was noted that it was understood that resharing data is not allowed yet, but there are grey areas, and will ACCC clarify soon. ACCC noted that they will soon make a statement about use of cloud infrastructure for people to comment on, and that next year they will work on more complex situations. It was noted that the rules currently allow for third party service providers where there is a contact with the data recipient, provided that the service is maintained by a contract and made clear to the consumers.

One member noted that they have had a number of calls and meetings with people saying they want to become an accredited recipient, but they don't understand about building consent dashboards. It was noted that there is interest in the market. ACCC noted that they will explore this with the 13 but initially as said it is not for version 1. ACCC realise that it is important.

One member noted that July will come quickly, that there are a number of outstanding items, and if we wait to February to fall over the line, we will not make July.

James Bligh, the API & InfoSec Lead thanked everybody for the journey and advised that this might be his last committee meeting as he is moving on. The Chair also noted that Mark Staples' interim role of Acting Director of the DSB is coming to an end and the incoming Director, Barry Thomas will commence on 18 November 2019. It was noted that Barry comes to the role from the Australian Banking Association (ABA). The Chair thanked James Bligh for everything he has done and noted that we wouldn't be where we are today without him, and thanked Mark Staples for stepping in on top of his own workload.

Meeting Schedule

The Chair advised that the next meeting will be held on Wednesday 11 December 2019 from 2pm to 4pm at the CBA's office in Melbourne.

Closing and Next Steps

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

Meeting closed at 3:55