Consumer Data Right

Data Standards Advisory Committee

Minutes of the Meeting

Date:	*Wednesday 10 August 2022*
Location:	*Held remotely, via WebEx*
Time:	*10:30 to 11:30*
Meeting:	*Committee Meeting # 45*

Attendees

Committee Members

Andrew Stevens, Data Standards Chair
Luke Barlow, AEMO
Jill Berry, Adatree
Damir Cuca, Basiq
Chris Ellis, Finder
Melinda Green, Energy Australia
Chandni Gupta, CPRC
Jason Hair, Westpac
Rob Hale, TrueLayer
Richard Hough, ANZ
Lisa Schutz, Verifier
Aakash Sembey, Origin Energy
Stuart Stoyan, Fintech Adviser

Observers

Barry Thomas, DSB
James Bligh, DSB
Ruth Boughen, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Mark Verstege, DSB
Paul Franklin, ACCC
Andre Castaldi, OAIC
Sophia Collins, OAIC
Elizabeth Hampton, OAIC
Bart Hoyle, Treasury
Emily Martin, Treasury
Kate O'Rourke, Treasury

Apologies

Peter Giles, CHOICE
Tony Thrassis, Frollo
Glenn Waterson, AGL

Chair Introduction

The Data Standards Chair (**Chair**) opened the meeting and thanked all committee members and observers for attending meeting # 45.

The Chair noted that given the consultations underway regarding Data Standards for the Telecommunications Sector, it is timely to add a Telecommunications company to the DSAC. Telstra have expressed interest and he recommends that we add Telstra to our number from the next meeting. While we have a term completion and "Committee refresh" date approaching in November this year, it is important that we access Telco input in the near term.

The Chair noted that there has been a number of changes to the Data Standards Body (DSB) team over the last month. Sumaya Hasan has joined the team as Engineering Lead and Ivan Hosgood the Solutions Architect has left the DSB. Recruitment to replace Ivan is well underway along with some other engineering capability.

The Chair would like to welcome Elizabeth Hampton and Andre Castaldi from OAIC and Bart Hoyle from Treasury who are attending the meeting today as Observers.

The Chair noted that Peter Giles (CHOICE), Tony Thrassis (Frollo) and Glenn Waterson (AGL) are apologies for this meeting.

Minutes

Minutes

The Chair thanked the Data Standards Advisory Committee (DSAC) Members for their comments, and last-minute feedback on the Minutes from the 13 July 2022 Advisory Committee meeting. The Minutes were formally accepted.

Action Items

The Chair noted that all Action Items are now completed.

TSY noted that they have reached out to Consumer Policy Research Centre (CPRC) about the findings from the Gateway Review and also had a discussion with Energy Australia to talk about the nominated business representative issues in the banking and energy sector.

Working Group Update

A summary of progress since the last DSAC meeting on the Working Groups was provided, and these DSAC Papers were taken as read.

Technical Working Group Update

The update was provided on the Technical Working Group by James Bligh and Mark Verstege as follows:

The DSB noted that they have finalised Maintenance Iteration # 11 (MI11) which was very large and addressed 38 distinct Change Requests as well as a number of minor documentation updates.

Version 1.18.0 is due to be published in the coming days after final reviews are completed. They extend they're thanks to Hemang Rathod and the team who led the work and the community for their extensive feedback.

The DSB noted that the Independent Information Security Review has been completed. The feedback from the community has been excellent and they're working on their response to the recommendations before publishing in the coming weeks.

The DSB noted that they are close to receiving the threat and risk reports from the University of New South Wales (UNSW) which will be helpful in contributing to the response to the security review.

The DSB noted that for the telco industry, they've been given some dates to work towards to get a draft out to give maximum optionality to the government in setting the rules and the implementation dates. They're pushing ahead with consultation but to date have had limited feedback from industry. They've also held a workshop with Communications Alliance to discuss the standard development process and plan to set up regular meetings with Communications Alliance like they did with Australian Banking Association (ABA) for banking and the Australian Energy Council (AEC) for energy.

The DSB noted that are planning to do at least 4 consultations around energy API's working towards "Candidate Standards" by November. They noted that, given the Designation Instrument for telco, from a technical standards perspective this is nowhere as near as big a job as it was for banking or energy as most of the issues have already been resolved.

One member noted in terms of the Independent Security Review, it's all technically correct and sensible and they broadly agree with the direction. They agreed with the move towards a combined release model and clearer roadmap. They noted that collectively we need to get all the moving parts for the next 24-36 months with a clear Treasury (TSY) direction on the desired roadmap and define how it looks to make it as easy as possible for all participants to plan.

One member asked for further clarity in regard to the work that went into resolving the issues surrounding the publishing of the Product Reference Data (PRD) for the energy sector. The DSB noted that the confusion arises from a combination of the rules and the standards. The original intention when they did the consultation back in 2020/21 was to reduce costs particularly for the long tail of retailers, with the government funding the Australian Energy Regulator (AER) to produce the data. That left them a challenge on how to enable this low cost/effort model while also allowing brands flexibility in managing the presentation of their products.

The DSB noted that the position they took was that AER is providing the data but would not engage with the register. That function was left to the energy retailers.

DSB noted that in terms of the recent issues, AER goes live on 1 October and they will present a series of Application Programming Interfaces (APIs) which need to be discoverable. AER will publish all the APIs for different brands on their own website. On 15 November when the 3 major retailers go live, they will have to put their details in the register, one of them being the public based Uniform Resource Identifier (URI) which is a piece of metadata to give direction to people wanting to talk to the data holders (DHs) to find status and outage, which are part of the consumer data request obligation, as well as product data which is a product data request obligation. This was not changed in the register because it is a cross-sectoral.

The DSB noted that they were operating under the belief that this was fine under the rules because the rules allow the registrar to ask for data for anyone that's coming on as a DH. However, the community have raised concerns around being asked to build a product data request service even though they're not obligated to. The DSB have had guidance from the Australian Government Solicitor (AGS) indicating that that is not the correct way to interpret the rules – asking to facilitate a single base path that then routes to different locations doesn't constitute selfhosting, however they've now been given the guidance that the current rules don't allow that as a requirement so it's not something that can be compelled for 15 November.

They noted that the 3 major retailers going live are not required to facilitate PRD endpoints through their base URI but are required to facilitate status and outage. They can facilitate the PRD data if they wish to, if they don't then anyone going to the register and trying to use that to access their product data will fail. TSY have flagged that they will seek to close this gap in the rules in the future. In the meantime, the ask is with the retailers to voluntarily do this facilitation if they are amenable.

TSY noted that with any potential rule change that may come through, there will be plenty of advance notice and a public consultation.

DSB noted that this is not a new problem as we still don't have a discovery point for PRD in banking, and they have been hosting a public repo to facilitate that. The Registry team at the Australian Competition and Consumer Commission (ACCC) are working on a long-term solution.

The DSB noted that they have asked UNSW for reports addressing a framework and a methodology for identifying the threat and risk landscape of the Data Standards and how they move forward in an objective manner to mitigate these. They hope to have these recommendations in the coming month.

Consumer Experience (CX) Working Group Update

A further update was provided on the CX Working Group by Michael Palmyre as follows:

The DSB noted that was a shift in MI11 to treat customer data languages sector agnostically which will support consistency as we get to telco and other sectors.

The DSB noted that they are seeking input from retailers, especially those that have November obligations, to understand the timing via Change Request 529. They noted that the proximity to November is increasing but there are some warranted language changes there for energy data.

The DSB noted that Decision Proposal 267 – CX Standards | Telco Data Language which is for the telco data language standards will be published in the next couple of days. This DP is to support the principle of consistency across sectors. This is a preliminary consultation as they have to wait for the rules and technical standards to progress further and thus there will be a later, final round of consultation.

One member asked, in terms of the accessibility, when you sign up for energy does this mean you have to say that someone is on life support.

The DSB noted that they expect the issue to relate more to the hardware that someone might use, not necessarily the accessibility needs that they have, but there would be publicly available accessibility information on what kind of hardware exists for XYZ accessibility needs etc.

DSB noted that in terms of Decision Proposal 229 – CDR Participant Representation they've had some good discussions across CDR agencies on an appropriate path for this. This is around the complexities of brands, software, products and those kind of relationships in the register and how they appear in DH systems. They hope to publish this soon.

The DSB noted that the accessibility analysis has been going well which they hope to wrap up soon. They have published some coded artefacts which are available in the new Open-Source Assets section of the CX Guidelines.

The DSB advised that a Noting Paper is being developed on authentication which shares their approach with the community as well as the CX metrics they are using to assess a range of authentication approaches which will ultimately inform standards development.

The Chair asked Energy Australia and Origin Energy if they are happy with their involvement in the consultations underway on telco standards and CX, given that they both offer telecommunication services.

One energy company noted that have been working with their provider and they are trying to impress upon them what the CDR is about but they seem to be downplaying the implications of it. They suggest that more could be done to help them get across it fully.

Another energy company also noted they have experienced the same and they are keeping an eye on the consultations. It is early days, and they are providing whatever they can to their telco entities.

The DSB noted that any help that can be provided to communicate that this isn't trivial and that engagement is going to be needed would be really helpful as there are some misperceptions and misunderstandings around what the CDR is and what the implications are going to be.

Stakeholder Engagement

A summary of stakeholder engagement including upcoming workshops, weekly meetings and the maintenance iteration cycle was provided in the DSAC Papers, which were taken as read.

Issues Raised by Members

The Chair thanked all members who had tabled discussion items.

CDR Consent Issues

Tony Thrassis from Frollo was scheduled to present on overview of failed (pending) consents in the follow consumer app but was a late apology for the meeting. This item will be rescheduled to be addressed at the September DSAC meeting.

Consumer Friction in a Compliant Representative Consent Flow

Jill Berry from Adatree presented on consumer friction in a compliant representative consent flow.

Berry supports the Representative model with currently 13 Representatives and as an intermediary offers a compliant CDR Representative consent flow.

Berry noted that one of the Representatives that is going live is confused about what the consumer is presented with and how it relates to the services provided, not necessarily on the ADR side but on the DH side. The CX is a barrier to going into production as it introduces unnecessary cognitive friction.

Berry noted that some ideas of how this can be consumer friendly while realising its compliance requirements. This could also be replicated for Trusted Advisors (TA) as well as Representatives.

Berry noted that ADR's offering intermediary services should only be a backend implementation detail, not a consumer facing entity. Adatree are regulated and CDR accredited, but as a consumer you care about giving consent to the representative and it's a balance between informing the consumer and delivering a service.

Berry noted that DH obligations result in ADR intermediaries using the new access models being made the sole focus of the authorisation flow and DH's consent dashboard.

Berry noted that in the context of Representative consent, the consumer consents to share data with the CDR representative. In their sandbox they show under "General Information" Adatree's CDR Policy and under "Supporting Parties" the accredited entity. This works as it informs the customer and does not need to be changed.

Berry noted that following consultation with their clients, they have added a disclosure to connect the dots clearly between the accredited entity and the Representative as an interim step. This is necessary given the confusion on the DH side.

Berry noted that as a legal entity they have to include specific fields. They provide the Legal Entity, Brand, Representative and the Product etc but these fields are inconsistently referenced by the DHs and are confusing. Supporting parties have ADR background but DH authorisation has no mention of the Representative and only has the ADR in the foreground.

Berry suggests adding new fields in the CDR Portal for Representative, TA and their respective products. There are currently only two fields "Primary" and "White Label".

In summary, Berry would like to see a fast turnaround for DHs to link to new Representative information; DHs must display consistent information in authorisation flow; DHs must refer to CDR Representative Brand Names (under UADR); DHs must refer to CDR TAs Brand Names (under UADR); DHs must refer to CDR Products consistently; New CDR Portal fields to link information accordingly; and Future proof fields for other access models.

One member asked if anyone has any evidence on dropout impacts?

Another member noted that there are so few Representatives live, but the ones that are, are on the edge of going live as is such a bad consumer experience.

One member noted that in their research, consumers related really well to logos so if we could also capture in the register appropriately sized and formatted logos it would be good.

One Observer noted that there has also been some discussion about the use of software product as an indicator of representative arrangements. There were different views from participants about whether they intended to use a separate software product for representative but this also needs to be considered as part of the solution.

One member noted that as they are going live soon, they are mindful that we don't want to make too many changes for energy.

The DSB noted that it was great to get real world evidence on this issue and that their early analysis on this front was really speculative because it was before there were sponsorship and representative arrangements in the ecosystem. This however validates a lot of that work and gives them insight into some domains that they don't see firsthand. It is appropriate for the CX standards to deal with this immediate issue around the brand being presented in the authorisation flow and the big question is around the timeline for DHs to actually implement it.

The DSB noted that in terms of the onboarding process, appropriate guidance and CX Guidelines could really help tackle some of the ambiguity that exists around the relationships between brands, software, product and legal entity. They did note that without a requirement it won't happen as it's not possible for that to actually flow in the authorisation flow as there needs to be a standard or rule made to actually provide that provision.

One Time Password (OTP) Authentication Method Scam

Aakash Sembey from Origin Energy presented on OTP Authentication Method scams. He has prepared an Issue Paper which he is happy to share with the committee.

Sembey noted the Origin security team identified the OTP scam issue and that approximately 1500 energy customer accounts were compromised, accessed and taken over. Scammers were able to access the OTP from customers to access their energy accounts including invoices, energy usage and historical data.

Sembey noted that the scammers started the password reset flow, which generated an OTP which was sent to the customer which they then provided back to the scammer. The scammers then instantly changed the account password and login etc.

Sembey noted that to resolve this they are implementing alternative authentication models to address the gaps by introducing 'magic links' instead of OTP. They are also providing some additional text and educational materials to their customers to try and make it more difficult for the scammers.

Sembey advised that they have noticed that the CDR authentication flow works on the same OTP principal which is strictly prescribed and it does not allow them to implement alternative authentication methods.

Sembey has raised this issue in GitHub but they are mindful not to provide too much detail because its publicly available information and they do not want to promote the issue. With the approaching November deadlines they would like a renewed focus on the issue and to mitigate the risks by perhaps amending the authentication, adding additional authentication standards and considering one of the success metrics of CDRs which is the reduction in fraudulent activity.

The DSB noted that they have been looking at this issue, which is not a new one. In 2018/2019 how they authenticate was the matter of a great deal of debate but saying that there's always room for improvement. The DSB noted that the Independent Review did highlight various aspects related to OTP.

The DSB noted that following discussion with Origin's security people, the forgot password link that caused the issue with people was in an "open page". Whereas our OTPs are only reachable after they go through a process (they've engaged an ADR who has successfully engaged with the consumer and then a DH and then gone through client authentication and verification with the Register).

The DSB's initial observation to the feedback is that it's nowhere near a serious risk or vector as it was for Origin's 1500 customers. The DSB would love to get feedback from the banking sector on whether they've experienced something similar because obviously the banks have been live for a long time, particularly the four majors.

The DSB noted that they are looking into other authentication methods and how they can improve the flow and looking at things like RSA keys, OTPs in the app, or app to app particularly as they consider how we can progress to write action which will have a much higher risk profile.

One member noted that his predecessor presented on this topic to the DSAC back in November 2020 and their view was that app-to-app works for consumers as it's much more secure and has the benefit of experience from the overseas markets to actually improve the conversion rate. They wondered if app-to-app still an option and whether this could the solution?

The DSB noted that the issue with app-to-app is that you have to have an app. In banking this was not a problem because just about everybody has an internet banking app already. For energy and telco there isn't a highly digital enablement of consumers and it's not necessarily an obvious solution for all customers.

The DSB noted that they think the issue is social engineering so it's actually broader than just OTPs and even in the OTP space, it's not just SMS OTP or email OTP. Any social engineering attack where it is about gaining an honest user's trust to then maliciously obtain information, it's about establishing that trust such that disclosure of sensitive information seemed like less of a risky thing. They have been looking at what's been implemented in the UK - a decoupled authentication where it separates the consent flow for data sharing from the authentication which could be on a mobile app. They think they will need to look at a combination of controls and there is an international movement about sharing fraud signals, security events that occur both on a trusted third-party side and also on a DH side. There are other controls that they could put in place that may look at limiting or sharing information about the frequency of these sort of attempts. It is more than just a single factor or control and they will need to look at the engineering space more broadly and beyond OTP.

One member noted that the digital landscape is constantly changing and they currently have more digitally active users who use internet banking rather than the app. One of the challenges they have when they do an upgrade is supportability for the long tail of iPhone models for example. Planning in the context of the law and the rules upfront around what's acceptable is critical so we don't have a security standard that then disseminates so new additional participants who from COVID got familiar with internet banking but not an app. They think planning for action initiation is the right time to have a critical look at OTP versus now. They noted that there's a level of cumulative change where if we combine the small requests with the bigger chunks, it becomes cumulative and we need to consider the non-major banks who have the same obligations and whether they have the right resources.

One member noted that they have seen SMS, WhatsApp and email-based fraud scams on the rise and they're getting very sophisticated. In the last week their OTP provider was hacked but luckily, they weren't exposed. They support app-to-app or in app authentication and they are moving more broadly to that.

The DSB noted that banking has a digital maturity around authentication and customers are more commonly engaged on a day-to-day basis than perhaps other industries that we're moving into with the CDR. We need to consider how we support other industries and what role does the CDR have to play in uplift of digital services like authentication or whether it has to abide by current digital practices within different industries. Technical controls are one aspect but equally important is the role CDR has to play around education.

The DSB noted that perhaps there is a benefit to wargaming and/or looking at ways that we can say if a breach happens, how do we respond as a CDR community because it's equally important to regain trust with consumers as it is to protect them in the first place.

One member noted that the bank fraud teams meet regularly to combat this and share cross border information. They will reach out to see if this is a formal process and enquire whether the DSB can participate to get some insights and learnings.

ACTION: The member to investigate whether the DSB can participate in regularly meetings with the bank fraud teams

The Chair noted that it doesn't appear that unless an ADR is severely comprised, that this is a material risk at present but recognises the recommendations of the independent security review and the ambient risk that is going up all the time and this is very important and is on their agenda.

Treasury Update

Kate O'Rourke, First Assistant Secretary CDR Division, TSY provided an update as follows:

TSY provided an update on the work Treasury is doing on rules development and action initiation. In response to a query from the Committee, she noted the difficulty in predicting likely implementation and compliance dates for action initiation, given the uncertainty of how long the passage of legislation will take.

TSY and the DSB are undertaking work in relation to consent rules and standards. In addition to internal analysis, the DSB is undertaking consumer research. We propose to hold a workshop with the CDR community in November to work through some of the implications of what that research might be.

TSY thanked the members who provided feedback to the management consultants on benefits following the last meeting. The input has been productive and they have received excellent feedback.

One member asked if there was any update on what's after the telco sector, are there any go live dates and when will they be required to start sharing consumer data?

TSY noted that in open banking, the planned sequencing is non-bank lending, superannuation and then insurance. The other possible component of Open Finance is merchant acquiring services but they're not sure whether that will proceed.

ACCC Update

Paul Franklin, Executive General Manager ACCC CDR Division provided an update as follows:

ACCC noted that in preparation for the launch of data sharing for the Energy sector, they released the latest version of the Register on 15 July and the Sandbox for multilateral testing on 22 July. They're on track to release a new Conformance Test Suite (CTS) instance for Energy DHs by 15 August, which will allow initial Energy DHs three full months to test their solutions.

ACCC noted that all planned technology releases by the ACCC are either complete or on track for the commencement of Energy data sharing.

ACCC noted that they will be ready to undertake onboarding of energy DHs in advance of the commencement of data sharing obligations on 15 November, to permit 'production verification' to occur before the obligation takes effect. They're continuing to meet regularly with Energy DHs in preparation for onboarding.

ACCC have established an Incident Management Focus Group, which addresses a range of related issues including incident management, data quality and ecosystem performance. The group has met twice and have identified a range of issues including:

- Potential improvements to the incident management process, including categorisation of incidents, workflow states, visibility of tickets within an organisation, and the need for more comprehensive information in some incidents;
- Time-frames for resolution of incidents, including potential Service Level Obligations or Agreements (SLOs/SLAs), early acknowledgement of incidents raised, opportunity to review the use of severity ratings; and
- The process for government agencies including ACCC, DSB, OAIC and Treasury to comment on incidents, especially where participants have conflicting views about obligations, and to publish non-confidential information about incidents.

They noted that a range of specific issues have also been identified, including issues related to:

- limited visibility of the consent flow;
- provision of 'optional' data fields in a data payload;
- balance information being potentially inconsistent with the Internet Banking balance;
- the process for connecting to business accounts, and
- description data in response to the 'GetTransaction' data request.

ACCC noted that some participants have indicated that they would like to provide input to the ACCC separately from scheduled meetings. Further work is required on methods to comprehensively capture data quality issues as they arise. They'll continue to work with participating members to develop solutions to these issues and ensuring there are appropriate methods to comprehensively capture new data quality issues as they arise.

Meeting Schedule

The Chair advised that the next meeting will be held remotely on Wednesday 14 September 2022 from 10am to 12pm.

Other Business

No other business was raised.

Closing and Next Steps

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

Meeting closed at 12:00