Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date:	*Wednesday 30 October 2024*
Location:	*Held remotely, via MS Teams*
Time:	*10:00 to 12:00*
Meeting:	*Meeting # 13*

Attendees

Participant Members

Hemang Rathod, Chair
Mark Verstege, DSB
Sameer Bedi, NAB
Nick Dawson, Frollo
John Harrison, Mastercard
Macklin Hartley, WeMoney
Ben Kolera, Biza
Stuart Low, Biza
Julian Luton, CBA
Tony Thrassis, Frollo

Observers

Nils Berge, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Christine Williams, DSB

Apologies

Elizabeth Arnold, DSB
Jim Basey, Basiq
Darren Booth, RSM
Chrisa Chan, TSY
Aditya Kumar, ANZ
Elaine Loh, OAIC
Olaf Grewe, NAB
Dima Postnikov, Connect ID
Mark Wallis, Skript
Abhishek Venkataraman, ACCC

Chair Introduction

Hemang Rathod, the acting Chair of the Information Security (InfoSec) Consultative Group welcomed everyone to the meeting, acknowledged the traditional custodians of the land and paid respect to elder's past, present and emerging.

The Chair noted that members Jim Basey (Basiq), Darren Booth (RSM), Aditya Kumar (ANZ), Olaf Grewe (NAB), Dima Postnikov (connect ID) and Mark Wallis (Skript) were apologies for the meeting. A number of observers also sent their apologies.

Minutes

The Chair thanked members for their comments on the Minutes from the 16 October 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted that the action item around Biza presenting at future meeting on new sharing arrangements was still outstanding. All other actions were either completed or covered off in the meeting.

One member requested an extension on the Action Item around providing feedback on the TDIF role requirements due to the complexity and lack of internal stakeholder awareness. The DSB agreed to an extension.

Options Feedback Review

Michael Palmyre from the DSB summarised the feedback on the Redirect to App option, noting that members supported the Redirect to App in principle, concerns around the technical complexity of change, and a suggested 24-month timeframe for mandatory implementation.

There was a discussion around the need for data recipients to provide redirection back to their app and the articulation of web flows.

Further discussion was held around the impact on new sectors, particularly NBL, agreeing that a 24-month lead time would be appropriate for implementation. This approach would ensure consistency across sectors.

The discussion also touched on the need for consistency in credential levels across different channels (web and app) and the importance of ensuring that the chosen authentication factors do not lead to higher drop-off rates.

There was consensus that fallback options such as web flows, should remain available and that the credential levels should be consistent regardless of the channel used.

The discussion also highlighted the challenges of implementing higher credential levels, especially for sectors like NBL with low digital maturity. The need for a balanced approach that considers both security and usability was emphasised.

A discussion was held around security concerns related to OTP and the need for a comprehensive approach to ensure data security within the CDR framework and any changes to authentication methods do not lead to drop-off rates.

The Chair summarised by saying how do we secure consumers data appropriately without undue friction and what types of data should be shareable under a single factor authentication opposed to multiple.

It was suggested that safeguards should be put in place to ensure that any changes to authentication methods do not lead to higher drop off rates. The proposal of collecting metrics and observing success rates to ensure that chosen methods achieve the intended goals without causing undue friction for consumers was suggested.

There were concerns raised about the potential for phishing attacks if passwords were introduced as an authentication method and the need for countermeasures to address phasing risks, such as ensuring that OTP was sent before presenting the password prompt.

The DSB summarised the feedback on the Redirect to Web Uplift option, noting support but also concerns about poor consumer experiences as part of this uplift, impacts to offline customer authentication, and the need for clear guidelines on memorised secrets and secondary authenticators.

A discussion was held around increasing the length of OTPs, noting that the entropy requirements under TDIF was 6 digits or higher. The DSB noted that as proposed in DP327, they would like to set it between 6 to 10 digits.

Concerns were expressed about the TDIF role requirements, particularly how they apply to SMS OTPs, highlighting that many data holders might not meet the requirement to demonstrate ownership of the device to which the SMS is sent.

Further discussion followed around the challenges associated with offline customers, particularly in the energy sector, and supporting offline customers is problematic with suggestions that it might be more practical to eliminate offline customers from the CDR framework.

It was mentioned that some energy retailers have secondary users who were always offline and do not have accounts with the retailer. These secondary users, such as real estate agents managing properties, present a unique challenge as they are eligible to share CDR data but do not have digital accounts.

It was noted that removing offline customers would dramatically simplify the process of achieving higher credential levels (CL2 and above) with the suggestion that offline customers could be limited to CL1 and if they want higher credential levels they must onboard as digital users.

The DSB summarised the limited support for Decoupled Authentication with the main concerns around the consumer experience associated with this approach and it should only be considered if there are clear service level agreements (SLAs) for success in place which would ensure that implementation does not negatively impact the user experience.

The need to be explicit about not defining a protocol-level solution for decoupled authentication and whilst protocol-level solutions like CIBA (Client-Initiated Backchannel Authentication) are out of scope, data holders should still be allowed to implement decoupled flows from the consent flow perspective was emphasised. This would enable them to offer higher credential levels without requiring immediate changes to their digital banking platforms.

The DSB summarised the data sensitivity framework option noting that Option 1 (Data holders may voluntarily provide stronger authentication) and Option 3 (Data standards prescribe CL2 for all data access) had limited support from members, whilst Option 2 (Data Standards define CL based on data sensitivity classification) was generally supported by members. However, impacts to usability and use cases would need to be considered as well as additional research and threat assessments conducted as part of that.

The DSB introduced a new option, Option 4 (combination of Option 1 & 2) which considered the identity proofing level of a sector to determine credential levels. That meant that the minimum credential level would be based on the identity proofing level for customers in different industries.

The group expressed support of Option 4 noting that it would simplify conversations with banking data holders by aligning credential levels with existing identity proofing requirements. However, implementation considerations would be needed to address potential challenges with energy account switching and ensuring consistency across sectors. This option provides a nuanced approach that considers the specific requirements of different sectors, making it easier to achieve compliance.

The DSB asked for further feedback on Option 4 via activity on the Miro board. They would also reach out to the group for additional feedback due to a number of members not in attendance today.

ACTION: DSB to reach out to group for further feedback on Option 4

TDIF Requirements

Hemang Rathod from the DSB noted that several members requested an extension to fill out the TDIF requirements spreadsheet, which was agreed. This item would be carried over to the next meeting. They opened the floor to any specific questions or areas members wanted to raise regarding the TDIF requirements.

It was highlighted that the TDIF requirements are vastly different for an ADR compared to a data holder, emphasising the need to consider these differences in the discussion.

The DSB noted that once feedback is collated, they will walk through a heat map with what implementation support is required for all requirements.

It was noted that implementing TDIF requirements is challenging, especially for mutuals' core banking systems.

Meeting Schedule

The next meeting is scheduled for Thursday 14 November 2024.

Any Other Business

One member proposed that they present the draft specification for sharing arrangements version 2 in an upcoming meeting to address concerns around tracking drop-offs and consumer consent status. The DSB agreed to add this item to the agenda to an upcoming meeting.

ACTION: Add Sharing arrangement presentation to upcoming meeting

One member noted that the group had made good progress and suggested that at the next meeting or the one after, we should develop and share a timeline with specific targets and activities and timelines. The DSB agreed with this approach.

One member also suggested the group figure out what assets the DSB might be able to produce, for example a reference implementation.

The Chair noted that the next steps/action items were as follows:

- Collect and collate feedback on TDIF requirements from members and include as agenda item at the next meeting
- Share and discuss the content of the draft decision proposal for Redirect to App at the next meeting
- DSB to reach out to group for further feedback on Option 4
- Add Sharing arrangement presentation to upcoming meeting

Closing

The Chair thanked everyone for attending the InfoSec meeting and being part of the consultative group.

Meeting closed at 11:56