Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Thursday 14 November 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 14*

Attendees

Participant Members

Mark Verstege, DSB
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
John Harrison, Mastercard
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Nils Berge, DSB
Chrisa Chan, TSY
Bikram Khadka, DSB
Elaine Loh, OAIC
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Matthew Shaw, DSB
Fiona Walker, TSY

Apologies

Elizabeth Arnold, DSB
Jim Basey, Basiq
Macklin Hartley, WeMoney
Abhishek Venkataraman, ACCC
Christine Williams, DSB

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) & Macklin Hartley (WeMoney) were apologies for the meeting. A number of observers also sent their apologies.

One member raised a concern about the Miro board that is used by the group being accessible to anyone with the link. The DSB agreed to restrict access to the Miro board via a password.

ACTION: DSB to restrict Miro board access to the group

Minutes

The Chair thanked members for their comments on the Minutes from the 30 November 2024 meeting.

One member requested a review of the minutes regarding the requirement in TDIF that mandates demonstrating ownership of the device to which an OTP was sent as it sounded like data holders were doing what was required, yet it could lead to non-compliance. The DSB agreed to revisit the minutes and provide an amended version to the group for review.

ACTION: DSB to review the 30 November 2024 minutes and provide an updated version to the group.

The Minutes will be formally adopted and published on the Consumer Data Standards (CDS) website after further review.

Another member inquired about the broad agreement around the implementation timelines for app to app for new sectors and the 24-month maximum lead time that was discussed as the last meeting.

The DSB confirmed that the feedback at the last session supported a 24-month timeline, with flexibility for data holders to implement sooner if desired.

Further discussion highlighted the need to consider NBL sector's go-live dates when setting the timelines for app-to-app implementation, and sector specific considerations, similar to the energy sector, to ensure that new sector's timelines are taken into account for any standard changes.

Action Items

The Chair provided an update as follows:

- Presentation on new sharing arrangements from Biza will be scheduled for a future meeting
- Discussions around TDIF are ongoing and feedback from participants is still being collected.
- Decision Proposal for redirect to app is going through internal review and will be presented at a subsequent meeting for feedback
- DSB reached out to the group seeking feedback on Option 4 of the Data Sensitivity Framework. This was completed.

One member suggested that the item on Biza presenting on new sharing arrangements be scheduled for the next meeting or after the Christmas break as they would be out of the office during the intervening period.

ACTION: The DSB agreed to revisit the timing for Biza's presentation and schedule accordingly.

Progress Update on Thread Modelling

Hemang Rathod from the DSB provided a brief update on the progress of threat modelling, noting that they are building out an ecosystem-wide view that covers CDR and beyond.

This work leverages the information captured in the threat catalogue previously shared with participants. The focus is on building out the threat model for authentication options, specifically redirect to web and redirect to app.

The DSB introduced new team member Matthew Shaw who will be helping to advance the threat modelling piece of work.

Update on TDIF Role Requirements

Hemang Rathod from the DSB provided an update on the TDIF requirements, noting that feedback from all data holders had not yet been received. They suggested an alternative approach where the DSB could conduct an assessment and propose recommendations for the requirements categorising them into must, may, and not required from a CDR perspective. This approach aimed to progress the discussion while still expecting responses from data holders to ensure a comprehensive view.

There was consensus with proceeding with this alternative approach in parallel with responses from data holders. This combined approach would help informing an informed view at the next session.

Defining measurable Outcomes and Metrics

Mark Verstege from the DSB led a discussion on defining measurable outcomes and metrics for the authentication process and emphasised the importance of understanding what should be measured and why. This included looking at the purpose of measuring certain metrics and how they can be practically measured.

The DSB noted that the current metrics capture abandonment by stage, but with the introduction of alternative authentication flows and factors and grading of credential levels, there is an opportunity to look at what additional metrics should be measured.

The DSB referenced the UK, where they measure various quality factors around authentication, including credential levels, authorisation flows, and channels. This serves as a potential model for what could be measured in the CDR context.

The group discussed the purpose of measurement, including improving customer service, reducing dropouts, and monitoring the ecosystem. They emphasised the need for a clear purpose to avoid unnecessary data collection and highlighted technical considerations, such as the need for status indicators, aggregate metrics, and the potential complexity of implementing detailed metrics across the ecosystem.

Detailed comments from the group were captured on the Miro board.

Future Agenda and Priorities

Mark Verstege from the DSB outlined some potential priorities for the group to consider moving forward including:

- Modernising authorisation flows to share additional data around the purpose of the authorisation to allow data recipients to direct some of the data holder experience.
- Considerations around lodge intent
- Shared signals with data holders to advance the security profile
- Final approval for FAPI 2 followed by an impact analysis
- Threat modelling and attacker model
- Digital ID interoperability
- Consideration around moving to an RFC format
- CDR authorisation receipt which came out of the 2022 IHC

Further feedback included looking into the following components of FAPI 2:

- Assessing Depop (Demonstration of Proof of Possession) as an alternative to MTLS (Mutual TLS) for trust brokering and potentially for non-repudiation purposes.
- Looking at the FAPI 2 as it mandates a discovery document via RCA 414 which is the OAuth 2 Discovery document instead of the OpenID Connect Discovery document.
- FAPI 2 mandates DNS SEC (Domain Name System Security Extensions) on endpoints and most data holders do not currently use DNS SEC on their domain

The group expressed support for purpose- based consent but sought clarification on its implications for the group and what specific actions or discussions would be required to address this topic?

The DSB mentioned that purpose-based consent would involve looking at the security profile components. This included understanding the needs and drivers for changing anything beyond the current considerations for authentication uplift.

A query was raised on whether Rich Authorisation Requests (RAR) was part and parcel of the scope for authentication uplift, and should it be discussed in the context of purpose-based consents?

The DSB acknowledged that RAR is outside the scope of authentication uplift but is relevant to the discussion on purpose-based consents. They mentioned that RAR, along with rich authorisation and lodged intent patterns, are different approaches to establishing a richer authorisation that provides more information to data holders and allows data recipients to make more expressive and complete authorisation request.

There was need for a timeline to understand when the group's objectives could be met, and it was emphasised the importance of knowing whether the topics listed (such as purpose-based consents) were necessary to address in order to establish a clear timeline for completion.

The importance of metrics was again highlighted, particularly in understanding how many consent requests are made and how many consumers are lost due to issues with consent. It was suggested that having this measurement would validate the extent of the problem and help address it effectively.

Meeting Schedule

The next meeting is scheduled for Wednesday 27 November 2024.

Any Other Business

The Chair asked the group to continue adding their feedback to the activity on the Miro board around "Defining measurable outcomes and metrics" out of session.

ACTION: Group to continue to provide feedback on "Defining measurable outcomes and metrics" out of session.

The Chair noted that the Agenda Items at the next meeting will include:

- Biza presenting on sharing arrangements
- Revisiting the Future Agenda and Priorities

One member emphasised the need to measure how many consent requests are made to understand the number of consumers being lost due to issues with consent. They believe that having this measurement would prove the extent of the problem. They suggested that it would be beneficial if the measurement of consent requests came from data holders to validate the number of requests received.

Closing

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

Meeting closed at 12:05