Australian Government
The Treasury

DATA STANDARDS BODY

# Data Standards Body

## Information Security (InfoSec) Consultative Group

## Minutes of the Meeting

*Date:* *Wednesday 27 November 2024*

*Location:* *Held remotely, via MS Teams*

*Time:* *10:00 to 12:00*

*Meeting:* *Meeting # 15*

## Attendees

### Participant Members

Mark Verstege, DSB
Sameer Bedi, NAB
Nick Dawson, Frollo
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
Kyle Jaculli, ACCC
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Matthew Shaw, DSB
Fiona Walker, TSY
Christine Williams, DSB

### Apologies

Elizabeth Arnold, DSB
Darren Booth, RSM
Olaf Grewe, NAB
John Harrison, Mastercard
Macklin Hartley, WeMoney
Elaine Loh, OAIC
Abhishek Venkataraman, ACCC

# Chair Introduction

Mark Verstege, the 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 Jim Basey (Basiq) had recently transitioned to a new role and will consequently be stepping down from the group. He thanked him for his valuable contributions and wished him well in his new role.

The Chair noted that members Darren Booth (RSM), Olaf Grewe (NAB), John Harrison (Mastercard) and Macklin Hartley (WeMoney) were apologies for the meeting. A number of observers also sent their apologies.

## Minutes

The Chair noted that the minutes from the 30 October 2024 meeting were revised and distributed for further review by the group.

He thanked members for their comments on the minutes from the 14 November 2024 meeting and noted that both sets of minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

## Action Items

The Chair provided an update as follows:

- Biza to present on draft specifications for sharing arrangements at today's meeting
- Access to the Miro board has been restricted and password protected.
- The group continues to provide feedback on defining measurable outcomes and metrics. To be added as agenda item for review at the next meeting.

The Chair noted that the next meeting on 12 December is the last one for the year, and he sought feedback from the group about when they should reconvene in the New Year, suggesting either late January or early February.

The group agreed that late January was preferred, and the Chair agreed to circulate some potential dates for consideration.

**ACTION:** DSB to provide dates of when the group should reconvene in 2025 for consideration.

# Update on Threat Modelling

Hemang Rathod from the DSB noted that they were working on the threat model in the background, focusing on the immediate need of having a threat model view for the Redirect to app and other pipeline changes.

They were also working on building an ecosystem-wide threat model and mapping it to a risk framework. They hoped to have something to demonstrate at an upcoming meeting.

## Future planning roadmap

Mark Verstege from the DSB led a discussion on future priorities and focus areas for the group, emphasising the need to identify key thematic areas for uplift and improvement.

Key areas discussed by the group were:

- The importance of establishing a sustainable pattern for rich authorisation to go beyond current capabilities and prepare for future needs like action initiation, with a focus on improving privacy and fine-grained control.
- Concerns about the current register and trust brokering approach, particularly in the context of non-banking lenders (NBL) and brand representation. It was highlighted that a clear definition of principles to manage brand representation and usability for consumers was needed.
- The need for a standard event-based approach for notifications was discussed, aligning with international standards for better alignment with global practices.
- Consider what capabilities the ecosystem is missing and what security improvements are necessary. This includes looking at hygiene or improvement and uplifting required from a security perspective.
- The importance of addressing the privacy problem, highlighting the potential for over sharing and the lack of control of what is being shared. It was noted that other ecosystems have implemented fine-grained privacy control, which was missing in the CDR.
- Fine-grained authorisation is a key building block for enabling privacy and support future functionalities like action initiation.
- The need for purposed based consent, emphasising the importance of defining the problem it aims to solve and understanding its implications for the ecosystem.
- Need for metrics to understand where consent authorisations are up to and where they are failing.
- The importance of threat intelligence sharing to allow data holders to protect themselves and take proactive security measures against evolving threat actors.
- The integration of fraud controls which could help data holders enhance their capabilities in response to potential threats, especially as the ecosystem moves towards action initiation.
- Completing the migration to FAPI 2 as a priority to simplify the security profile and align with international standards.
- Need for certification to ensure conformance and reduce issues in the ecosystem which would provide a pathway for independent verification and help maintain a high standard of security and functionality.

The Chair noted that following the discussion, the top priorities were:

- Completion of FAPI 2
- Privacy and fine-grained control

He also noted that the next level of priorities were:

- Fraud monitoring and sharing of event-based notification
- Register and brand presentation

## Analysis of TDIF role requirements survey

Hemang Rathod from the DSB provided an overview of the TDIF role requirement, noting the goal was to discuss the adoption and leverage credential level requirements to define TDIF (Trusted Digital Identity Framework) and expand authentication methods available for data holders.

The feedback received from members indicated that some requirements might be too specific or difficult to meet. The DSB categorised the feedback into sections, with a visual representation using a RAG (red, amber, green) status to indicate compliance levels. They asked for members to provide further feedback to address gaps and concerns via the Miro board.

Further feedback from the group was captured on the Miro board.

The group discussion further:

- General consensus on the importance of adopting the TDIF role requirements but highlighted the need for industry-specific overlays to ensure relevance and feasibility.
- For the energy sector, there were entire sections of the TDIF requirements that would be marked a “red” (non-compliant) which indicates significant gaps or challenges in meeting the requirements for this industry. The DSB clarified that the requirements would be applied conditionally based on the industry and the identity proofing level already in place which means that each industry would only need to meet the relevant requirements that align with their existing standards and practices.
- The practicality of requiring a separate memorised secret for CDR, suggesting it could be problematic for users. There was support that if a memorised secret was used, it should be the same as the one used for the data holder’s digital channel.
- The current algorithms approved by the Australian Signals Directorate (ASD) go beyond those supported by FAPI and they need to align with international standards like BCP 195 for cryptographic algorithms.

The DSB noted that this item will be added to the agenda for the next meeting for further discussion.

## Biza presentation on Arrangements V2 design

Stuart Low from Biza presented on sharing agreement V2 (SAV2), discussing its alignment with international standards, the separation of authorisation from actions, and the benefits of the new approach. He also provided a live demo to illustrate the new process.

Some key points raised were:

Current issues with sharing arrangements:

- The current approach is internationally unique and involves using overloaded and non-compliant claims with seemingly no tangible benefit.
- Consumers are lost in the process during the authorisation flow, leading to lack of visibility for recipients.
- Arrangements are not referenceable resources, making it difficult to synchronise arrangement states between holders and recipients.
- Limited metadata available.

Proposed Sharing Arrangement V2 (SAV2):

- Inspired by ecosystems like the UK and Brazil, focusing on Occam's razor approach targeting broader vendor support rather than adopting new specifications like RAR (Rich Authorisation Requests).
- SAV2 is designed to operate concurrent with CDR Arrangement.
- Approach is backwardly compatible, ensuring that existing implementations can adopt the new design without breaking compatibility.
- Treats actions and agreements as resources, making them addressable with their own APIs.
- Design includes a discovery document to advertise capabilities and supports versioning of requests and response payloads.
- Client credential grants are used for back-channel communications and access to resource server APIs.
- Process starts by creating a sharing arrangement request action, which includes attributes like sharing duration and scope.

Implementation and Future Potential:

- Asynchronous Authorisation establishment which allows for actions that do not require immediate consumer interaction, such as machine-auth events.
- Provides visibility into the authorisation process, improving metrics and reporting.
- Designed to be extensible for future needs, such as fine-grained consent and additional action types.

Biza demonstrated the process of creating a new arrangement, showing how the status of the action can be tracked throughout the authorisation flow and how metadata on the arrangement can be pulled after completion.

## Meeting Schedule

The next meeting is scheduled for Thursday 12 December 2024.

## Any Other Business

No other business was raised.

## Closing

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

Meeting closed at 12:02