Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 16 October 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 12*

Attendees

Participant Members

Mark Verstege, Chair
Sameer Bedi, NAB
Nick Dawson, Frollo
Olaf Grewe, NAB
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Hemang Rathod, DSB
Christine Williams, DSB

Apologies

Jim Basey, Basiq
Darren Booth, RSM
John Harrison, Mastercard
Macklin Hartley, WeMoney
Chrisa Chan, TSY
Abhishek Venkataraman, ACCC
Elaine Loh, OAIC

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 members Jim Basey (Basiq), Darren Booth (RSM), John Harrison (Mastercard), Macklin Hartley (WeMoney) 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 18 September 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair provided an update on the Action Items as follows:

- Biza to present at future meeting on new sharing arrangements: to present at future meeting
- DSB to provide list of TDIF role requirements for feedback: completed
- DH to review detailed requirements for TDIF: ongoing

One member noted that their feedback on TDIF role requirements should be treated as confidential and not published or circulated. The DSB agreed to synthesize all feedback without attribution, and to look at the thematic issues or areas where alignment to TDIF may be challenging.

One member raised an issue regarding accessing the TDIF Role Requirements document that was shared to the group via GovTEAMS. The DSB agreed to share a copy via email.

ACTION: DSB to provide the TDIF Role Requirements document via email to the member.

One member questioned why data recipient authentication controls are not considered in the same scope in context to action initiation?

The DSB noted that the Chair can't define standards for data recipients and their authentication controls. They asked the group if there was any benefit in data recipients providing a view of the TDIF credential levels which may assist them in the context to data recipients.

One member agreed that it was worth looking at. The DSB suggested that the data recipients review the TDIF Role Requirements and provide input.

ACTION: Group to provide feedback on the TDIF Role requirements ahead of the next meeting

Update on Threat Modelling

Hemang Rathod from the DSB provided an update on the threat modelling work, focusing on the use of the Threat Dragon Tool and the progress made in defining current and future state authentication flows. They highlighted the work in progress on defining the current state OTP based authentication flow and the threat models for redirect to app and redirect to web-based authentication.

One member suggested integrating the threat modelling JSON files into a GitHub repository for easier collaboration. The DSB agreed to consider this approach.

One member suggested sharing the threat modelling diagram in a more accessible format, such as PDF or Figma to allow for easier commenting and collaboration. The DSB agreed to make this available via alternate methods.

One member highlighted the difference between the single concept of identity in the current system and the tiered approach in Digital ID, suggesting the need to consider in future discussions. The DSB acknowledged that the CDR focused on authentication rather than identity proofing and the potential intersection between Digital ID and CDR, recognising the importance of aligning the two in the future.

Another member expressed concerns about the timeline and political complexities of integrating Digital ID with CDR, fearing it could slow down current CDR progress.

Update on TDIF Role Requirements

The DSB noted that the purpose of this activity was to understand the specific role requirements that could cause issues in achieving particular credential levels or how authentication factors were defined with the aim to understand potential issues and alignment.

The DSB sought feedback from the group, asking them to indicate whether they fully met, partially met or did not meet each requirement.

One member raised concerns about the context of the mapping exercise, questioning whether it would address current problems with OTPs and the potential impact on consumers. The DSB acknowledged that while the exercise would address some security issues, it would not solve all problems related to OTP conversion rates.

One member pointed out that TDIF was done for a specific purpose, which was to enable (in the government context), the proper credential levels that are needed to enable identity use cases. This has different incentives and constructs to the needs of a commercial organisation. They suggested using this exercise to provide clarity where there are specific normative asks in TDIF that do not match what others are doing and not reflect remaining control put in place like behavioural analysis etc.

One member noted that there are two choices in the banking industry regarding authentication requirements. They are:

1. Delegate authentication requirements to the banks, allowing them to use their existing authentication methods, which would simplify processes and improve user experience.
2. Prescribe additional requirements, which would likely create implementation challenges, increase user friction, and incur significant costs.

They highlighted that specifying additional requirements would almost guarantee implementation issues and increased user friction. They suggested that relying on existing bank authentication methods would be more efficient and effective.

They also acknowledged that other industries might have different authentication levels and user scenarios, suggesting that a different approach might be needed for them. They also questioned whether there was a mandate or demand to increase authentication requirements in the banking industry, suggesting that the current levels might be sufficient.

Another member noted the importance of using the spreadsheet to gather data, to understand technical divergences, and make informed decisions. They also highlighted the need for a balanced approach between banks' autonomy and the government's liability framework.

One member noted that creating an identity provider (IdP) to meet specific accreditation levels was a very elaborate tasks and often required significant effort and resources. It was difficult to determine compliance with accreditation requirements until the actual accreditation process was undertaken. They emphasised the complexity and uncertainty involved in meeting specific accreditation levels for IdPs, suggesting that it was challenging and a resource-intensive process.

One member noted that there were two key components for the analysis of the TDIF role requirements:

1. Aligning the TDIF role requirements with the threat model noting that if certain requirements do not mitigate threats identified in the threat model, they might not be necessary.
2. Adding a column to the analysis spreadsheet to allow data holders to articulate any mitigating controls they have in place that are outside of the TDIF framework. This provides a more comprehensive view of the security measures in place and helped to identify where existing controls might already address certain requirements.

The member also suggested the need for confidentiality in sharing this information (highly confidential) and aligning the requirements with the threat model to consider mitigating controls outside of the framework.

The DSB noted that they would revise the TDIF role requirements spreadsheet to incorporate feedback and provide an update to the group.

ACTION: DSB to provide an updated TDIF role requirement spreadsheet incorporating the feedback to the group.

One member recommended that this activity gathers to data to make an assessment and informed choice, and it should be done holistically.

The DSB did note that the Data Standards Chair can only make standards in regard to data holders.

One member sought clarification on the TDIF terms and suggested that the group run through them to ensure all members are on the same page. The DSB asked members to review and come back with any queries at the next meeting.

ACTION: Group to come back with any queries or clarification on the TDIF terms at next meeting

Options Support

Michael Palmyre from the DSB noted that the purpose of this activity was to review options related to authentication uplift including Redirect to App, Redirect to Web Uplift, Data Sensitivity Framework and Decoupled Authentication. They asked the group for feedback including whether

they supported them, were there any gaps or clarifications needed. Feedback was being sought via Miro board.

One member supported the Redirect to App option, suggesting a voluntary standard initially, followed by a mandatory standard. They noted that it wouldn't be too difficult for data recipients to implement if apps were already in place.

One member requested a 24-month timeline for the mandate, highlighting challenges with existing digital banking platforms, especially for smaller banks. They suggested that standalone CDR authentication should be permitted to address these challenges.

There was a further discussion on whether the implementation should be phased, considering the dependencies on both data holders and data recipients. It was agreed that a trial or proof of concept (POC) could be beneficial to identify and address any issues.

There was general support for Redirect to Web Uplift, with participants noting the importance of improving the current OTP-based authentication flow.

The DSB noted that that there would be an opportunity to discuss the feedback in further detail at the next session. They agreed to provide a summary of the feedback to the group for a more comprehensive discussion at the next meeting.

ACTION: DSB to summarise the Options Support activity and provide to the group

Meeting Schedule

The next meeting is scheduled for Wednesday 30 October 2024.

Any Other Business

The Chair noted that agenda items for the next meeting include:

1. TDIF Role requirements
2. Review the feedback provided on the Option Support

Closing

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

Meeting closed at 11:58