Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Thursday 21 August 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 9*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
Ben Kolera, Biza
Aditya Kumar, ANZ
Julian Luton, CBA
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Christine Williams, DSB
Kyle Jaculli, ACCC
Abhishek Venkataraman, ACCC
Elaine Loh, OAIC
Chrisa Chan, TSY

Apologies

Sameer Bedi, NAB
John Harrison, Mastercard
Macklin Hartley, WeMoney
Stuart Low, Biza
Michael Palmyre, DSB

Australian Government
The Treasury

DATA STANDARDS BODY

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 Sameer Bedi (NAB), John Harrison (Mastercard), Macklin Hartley (WeMoney), Stuart Low (Biza) and Michael Palmyre (DSB) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 8 August 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted that there were a number of Action Items that would be addressed at the meeting along with some items which would be addressed over the coming weeks.

Terms of Reference

The Chair noted that the Terms of Reference had been updated to include transitioning from a trial period to a time-boxed period of six months. This change allowed for a checkpoint to assess if the outcomes sought were being achieved and if any changes to the format were necessary moving forward.

The updated Terms of Reference was formally adopted and will be published on the Consumer Data Standards (CDS) website.

Update on Threat Modelling

Hemang Rathod and Christine Williams from the DSB provided an update on the threat modelling work for the InfoSec Group. They have completed information gathering and classifying threat vectors using the STRIDE model and www.cyber.gov.au and moving towards threat normalisation phase. This involves reviewing, consolidating, and refining threats to better understand the landscape and deduce controls for a risk assessment.

The DSB mentioned they are exploring tools like Threat Dragon for better visualisation and encouraged members to review and contribute to the CDR Threat Model Catalogue spreadsheet which is shared in the InfoSec GovTEAMS channel.

The DSB also intends to move towards something like Threat Dragon and put the threat modelling work on GitHub to allow the CDR community to raise issues. This provides a longer-term benefit of providing a sustainable way to collaborate as the Threat Dragon solution can source all the threats and vectors and mitigants from the GitHub repository.

Australian Government
The Treasury

DATA STANDARDS BODY

Review of Redirect to App Flows

Bikram Khadka & Holly McKee from the DSB provided an update on the redirect to app flow, focusing on converting the previous meeting's discussions into Figma assets for better visualisation and feedback.

They also introduced an authentication schedule to guide the redirect process across different authentication methods, aiming to future-proof the approach for various authentication mechanisms like decoupled or passkeys. The intent was to ensure that the design aligns with existing digital channel experiences and accommodate various profile selection mechanisms without imposing significant new requirements.

The DSB encouraged the group to review and comment on the Figma assets, emphasising the importance of capturing all potential unhappy paths and determining appropriate error responses within the OAuth framework. This included feedback on the proposed standards, guidelines, and any additional considerations for the redirect to app flow.

This activity aimed to refine the redirect to app flow by incorporating feedback and ensuring that the design accommodates various scenarios and considerations for brand profile selection and authentication methods.

Following the activity, the conversation focused on clarifying the authentication schedule, discussing the support for decoupled authentication, and addressing concerns about the obligations placed on data holders. Key points included:

- Discussion about the use of decoupled authentication and questioning its necessity and application across different use cases. It highlighted the need for clarity on when and why decoupled authentication should be supported, emphasising that its implementation might vary depending on the specific use case.
- Concerns were raised about the accuracy of language regarding the data holder's role in launching the app if it's installed. It was clarified that the data holder's responsibility is to support app-to-app redirection, but the actual invocation of the app depends on the operating system and the relying party.
- The selection of brand profiles or channels at the beginning of the authentication process. It was clarified that the data recipient does not need to know the brand profile upfront; the selection occurs after redirection, based on the data holder's implementation. Also touched on the existing framework for brand selection on the register and how it might accommodate brand channels or profiles.

One member provided an update on the authentication schedule, emphasising the importance of accurately describing the data holder's obligations. They clarified that the data holder's role was to support app-to-app redirection when the app is installed, highlighting that the actual invocation of the app involves the operating system and the relying party, not the data holder directly. This distinction is crucial for understanding the responsibilities in the app-to-app redirection process.

One member wanted further clarification around decoupled, why we are doing it and for what use case. With more context we'll be able to work out whether it's a "must" or "optional" etc and what it's will cost the ecosystem.

The DSB proposed focusing on decoupled authentication at the next meeting, indicating that it is a significant topic that needs further discussion.

ACTION: DSB to add "decoupled" as an agenda item for the next meeting

The group discussed the feedback provided on "Scenario 1: Data Holder Brand Profiles" which focused on data holder brand profiles, where it was highlighted that data recipients may present consumers with options to select from different brand profiles offered by a data holder, such as business or retail banking. This scenario allows consumers to choose the appropriate app for their needs, ensuring the redirection to the correct app based on the selected brand profile. The discussion emphasised the importance of aligning the consumer's choice with the data holder's offered channels to facilitate a seamless app-to-app redirection experience.

One member raised a concern about small mutuals undergoing mergers or acquisitions, leading to multiple brands and apps. They questioned if it would be acceptable for such entities to create a new app specifically for CDR authentication and authorisation to serve all brands, aiming to simplify the process during transitional phases. The discussion highlighted the principle of aligning with existing digital channels and the potential friction for consumers needing to download a new app just for CDR purposes. The consensus leaned towards maintaining existing channel alignment and considering regulatory discussions for exemptions in edge cases.

Due to the time left in the meeting, the remaining comments would be taken on notice. The DSB will review and bring back any feedback to the group.

Mapping Error Scenarios to Redirect to App Flows

Bikram Khadka from the DSB sought feedback from the group around error scenarios relating to redirect to app flows focussing on identifying potential points in the interaction where errors might occur and how they could be addressed. They asked the group to provide feedback via the activity on Figma.

Following the activity on error scenarios, the conversation focused on clarifying and addressing concerns regarding error handling and the implications for user experience and technical implementation. Key points included:

- **Clarification on Error Scenarios**: Discussion on the need for clear error handling, especially in situations where a user might encounter unexpected account selections or the absence of nominated representatives. The conversation aimed to ensure that error scenarios are well-understood and appropriately managed within the CDR framework.
- **Technical Considerations**: Touched on the technical aspects of handling errors, including the use of standard OAuth error responses and the importance of providing sufficient information to data recipients to manage errors effectively. The conversation highlighted the challenge of balancing detailed error information with the constraints of OAuth standards.
- **User Experience:** Concerns were raised about the potential user experience implications of error handling, particularly in scenarios where users might be redirected unexpectedly or required to download new applications. The discussion underscored the importance of aligning error handling with existing digital channel experiences to minimise user friction.

The conversation underscored the complexity of error handling in the context of redirect to app flows and the need for clear guidelines and technical solutions to support a seamless user experience.

Meeting Schedule

The next meeting is scheduled for Wednesday 4 September 2024.

Any Other Business

The Chair provided a summary of next steps as follows:

- Focus on decoupled authentication flows and use cases at the next meeting
- Review the energy authentication practices, including offline customers
- Review the redirect to web approach
- Continue to discuss error scenarios and what gets played back to the ADR
- Consider the impact of Digital ID on CDR in future discussions
- Data Holders to review detailed requirements for TDIF (against their existing systems), for achieving different authentication assurance levels and ensure comfort with adopting

Closing and Next Steps

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

Meeting closed at 11:55