Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Thursday 12 December 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 16*

Attendees

Participant Members

Hemang Rathod, Acting Chair
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
John Harrison, Mastercard
Macklin Hartley, WeMoney
Ben Kolera, Biza
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID (arrived 10:40)
Mark Wallis, Skript

Observers

Nils Berge, DSB
Kyle Jaculli, ACCC
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Rob Sorrentino, DSB
Mark Verstege, DSB
Fiona Walker, TSY
Christine Williams, DSB

Apologies

Elizabeth Arnold, DSB
Chrisa Chan, TSY
Olaf Grewe, NAB
Bikram Khadka, DSB
Aditya Kumar, ANZ
Elaine Loh, OAIC
Abhishek Venkataraman, ACCC

Australian Government
The Treasury

DATA STANDARDS BODY

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 elders past, present and emerging.

The Chair noted that members Olaf Grewe (NAB), Aditya Kumar (ANZ) and Tony Thrassis (Frollo) were apologies for this meeting. A number of observers also sent their apologies.

Minutes

The Chair thanked members for their comments on the Minutes from the 27 November 2024 meeting. The Minutes will be formally adopted and published on the Consumer Data Standards (CDS) website after further review.

Action Items

The Chair noted that feedback on defining measurable outcomes and metrics is ongoing and will be revisited at the next meeting. All other action items were completed.

TDIF Role requirements update

Hemang Rathod from the DSB provided an overview of the three-step process for determining the appropriate Credential Levels (CL) and authentication methods for TDIF role requirements. This involved identifying the CL based on the industry, choosing the appropriate authentication method, and meeting the TDIF role requirements.

The DSB noted that feedback from previous sessions and other participants highlighted some requirements that were not met or partially met. Specific requirements, such as the ability for individuals to request the pausing or termination of credentials, were highlighted as challenging for some data holders. It was proposed making these requirements optional (SHOULD) rather than mandatory (MUST).

There was a discussion on the requirement for out-of-band devices to be authenticated using specific methods, such as cryptographic keys or other secure mechanisms. Some data holders indicated that they do not currently meet this requirement, and it was emphasised that these requirements must be met to address security risks associated with OTP-based authentication flows.

One member expressed frustration over the absence of many banks in the discussion about authentication. They suggested that their absence might cause issues later on.

Another member highlighted that the purpose of the consultative group was to gather input and reach a consensus before moving to a formal decision proposal. They were concerned that the lack of participation from banks could lead to prolonged debates and opposition on public forums like GitHub.

One member expressed concerns about adopting TDIF standards, stating that they are not suitable for private sector as they were developed for government departments. Adopting TDIF would impose constraints on how banks authenticate their customers, which they believe is not the right approach and would require significant changes to be implemented effectively.

The DSB mentioned that there have been independent reviews and reports provided to the Data Standards Chair, which recommend requiring multi-factor authentication (MFA) across the board. They stressed the importance of applying these recommendations practically to ensure they are workable for data holders while providing necessary protection for consumers.

They noted the challenges of balancing the need for appropriate security controls with the potential cost implications for data holders, especially for smaller entities like mutuals and non-major banks and acknowledged that enforcing MFA across the board could be cost-prohibitive for some sectors, such as energy retailers.

One member suggested focusing on standards-based integration and outcome-based requirements rather than prescriptive measures, to allow flexibility for data holders.

They suggested that the standards should focus on standards-based integration between the registry, data holders, and data recipients, such as using OIDC (OpenID Connect) and FAPI (Financial-grade API). They proposed that banks should be allowed to implement controls commensurate with the risk, as guided by regulators like Australian Prudential Regulation Authority (APRA), rather than being prescriptive about how to achieve the outcome.

They also raised concerns about the timeline for implementing TDIF, suggesting that it would be a long way off and that a change in the rules would be necessary to address the issues. They acknowledged that a technical standard is needed but emphasised the need for a practical and workable approach.

The DSB challenged the member to think about how to create principled and workable standards that ensure necessary protection for consumers and data holders, emphasising the need for standards that are enforceable by the regulator and provide consumers with confidence in the security of their data, noting that the standards need to be from a cross-sector perspective.

One member emphasised the importance of considering the ecosystem as a whole when defining standards. They pointed out that members of the consultative group should not focus solely on their individual benefits but should aim to set a long-term direction for the entire ecosystem. They expressed frustration that the discussions often revert to business and political considerations rather than focusing on technical definitions and solutions.

The DSB suggested that the member works with Australian Banking Association (ABA) to come up with a practical and workable approach to implementing security standards across the economy.

The DSB noted that the intent is to rely on TDIF or another framework, noting that they are not prescribing the use of TDIF and how a data holder should authenticate every single customer on every channel, it is purely CDR.

One member highlighted that data holders, particularly banks, often rely on a combination of controls, including fraud monitoring and real-time risk assessments, to balance customer experience and security. They pointed out that some TDIF requirements might not be necessary if other effective controls are in place. They emphasised that TDIF might fall short in acknowledging the specific risk-based approaches used by banks. They suggested that the framework should consider these additional controls and not impose unnecessary requirements that could disrupt the balance between security and customer experience.

The DSB noted that they had recently published an Authentication Frameworks Report from PwC Indigenous Consulting. They invited thoughts on the report, noting that the recommendations suggest implementing MFA across the board.

The DSB noted that next steps include further discussions with ABA and banks to propose a workable approach.

Redirect to App Decision Proposal walkthrough

Michael Palmyre from the DSB presented the Redirect to App Decision Proposal, which aims to support redirect to app authentication while making necessary adjustments to existing standards.

The proposal includes:

- Requirements for data holders and ADRs to support this flow, with a future standards obligation of 24 months after the standards are made binding, with the option of voluntary implementation before that period.
- A fallback to the existing method of redirect to web with OTP if the redirect to app is not available or feasible.
- A new concept of an authentication schedule in the standards, which maps out the relevant sections for different authentication flows, such as redirect to app and redirect to web with OTP which helps avoid confusion and streamline the implementation process.
- Changes to the security profile and CX standards to remove constraints that complicate redirect to app. This includes principle-based requirements for friction and consistency, and the ability to invite consumers to install the app during the web flow.
- Clarifies the ability to switch profiles during the CDR authorization process, addressing scenarios where a pre-selected profile is automatically logged into.
- An analysis and assessment section that incorporates feedback from previous discussions and public minutes, listing organisations that have supported redirect to app.

One member emphasised the importance of using consistent terminology, suggesting that the fallback mechanism should be referred to as “redirect to web” rather than “redirect with OTP” to align with international norms and avoid confusion for developers. Another member suggested “redirect to web with OTP” which is more specific.

The DSB agreed that “redirect to web with OTP” was more appropriate.

The member also raised a question about scenarios where a consumer might have multiple devices, such as a personal phone and a corporate phone. They emphasised that just because the app is not installed on the device initiating the flow, it does not mean the consumer should be forced to use OTP. Instead, the app on the registered device should be used for authentication.

Further discussion followed with general consensus that the app should be accessible on the device being used, and if not, the fallback mechanism should be clearly defined to ensure a smooth user experience. The discussion also touched on the technical aspects of how the operating system handles app redirection and fallback to web flow.

One member pointed out that the term “browser to app” is not commonly used and suggested “web to app” instead. They empathised the importance of aligning with international nomenclature to avoid confusion.

One member noted that we need to separate the authorisation flow from the credential level stating that dealing with the authorisation flow first allows the acceptance of existing authentication methods supported by banks simplifying the rollout across the industry. They also agreed with the terminology of “redirect to web with OTP”.

The DSB asked for feedback on the proposed standards changes on the “Authentication Schedule” of the standards explaining that that the “Security Profile” section includes requirements for redirect to app and the separation of OTP credential requirements to ensure clarity and consistency. The draft standards focus on redirect to app, ensuring that the authentication flows are clearly articulated for both data holders and recipients. This includes ensuring that recipients have separate redirect URIs for web and app-initiated flows and the inclusion of LOA 4.

Feedback was requested via the Miro board.

The DSB highlighted the proposed changes to the CX standards, including the ability to invite consumers to install the app, clarifications on password usage, and principles-based requirements for friction and consistency.

They noted that the standards clarify that consumer should be able to switch profiles within the app if they are automatically logged into a specific profile which ensures that they can share data from the intended profile, whether it is a business or individual profile. If not possible, the flow should fall back to the web to allow the consumer to complete the authorisation process, which ensures the consumer is not restricted to a pre-selected profile and can still complete the data sharing process.

The DSB requested feedback on the CX Standards via the Miro board.

One member noted that exception handling was necessary for security purposes which ensures that the request ends up on a specific form of browser, adhering to security protocols. The app involved in the redirect must be CDR enabled, meaning it should be specifically registered for the redirect URI and capable of processing CDR requests.

One member expressed scepticism about the 2027 timeline for implementing redirect to app, suggesting that it would likely be delayed to 2028 and the timelines for mutuals extending even further as they have significant challenges as many banks rely on off-the-shelf digital banking solutions provided by core banking vendors, which are often outdated and not easily adaptable to new requirements.

The DSB acknowledged the challenges and agreed that the standards should allow for flexibility in implementation, including the permission to use a separate app for CDR authentication as a transitional measure with a clear timeline for integrating these features into the main digital banking app.

One member raised concerns about the potential unintended consequences of introducing Level of Assurance 4 (LOA 4) as some data recipients might have copied non-normative examples from the standards, which specify LOA as an essential claim, leading to potential inconsistencies.

The DSB noted that introducing LOA 4 was not intended to change the current requirements for data recipients, but an option for data holders to disclose higher levels of authentication if they achieve them.

There was a discussion around whether the data holder's app should verify the calling application during the redirect to app process. The feasibility and technical implementation of this verification was questioned as it may not be practical. It was agreed that the existing guidance and standards related to verifying the calling application and update them as necessary to ensure clarity and practicality.

There was a discussion around introducing a "MAY" for decoupled for authentication. The standards should permit a decoupled authentication mechanism, where a push notification could be sent to a registered app even if the initial flow was started on a different device or through a web interface.

The DSB agreed that the standards should not unintentionally exclude the possibility of decoupled authentication. The standards could include a "MUST at least support" clause for OTP, allowing for other methods of authentication if available. This means that OTP remains a fallback option while permitting more advanced authentication methods.

There was a discussion around the need for data holders to support profile switching within the app and the potential issues with falling back to the web flow. They agreed that the standards should allow for flexibility while ensuring eligible accounts can be accessed.

One member highlighted the issue of inconsistent terminology used by data holders and data recipients, particularly regarding user identifiers and authentication methods.

The DSB acknowledged the concerns but pointed out that as the standards evolve to support various authentication methods, and the challenge is maintaining consistency when data holders have the discretion to choose their own authentication methods.

Meeting Schedule

The next meeting is scheduled for Wednesday 5 February 2025.

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 12:28