Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 4 September 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 10*

Attendees

Participant Members

Mark Verstege, Chair
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
John Harrison, Mastercard
Macklin Hartley, WeMoney
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
Michael Palmyre, DSB
Hemang Rathod, DSB
Kyle Jaculli, ACCC

Apologies

Jim Basey, Basiq
Chrisa Chan, TSY
Ben Kolera, Biza
Elaine Loh, OAIC
Stuart Low, Biza
Abhishek Venkataraman, ACCC
Christine Williams, 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 Jim Basey (Basiq), Chrisa Chan (TSY), Ben Kolera (Biza), Elaine Loh (OAIC), Stuart Low (Biza), Abhishek Venkataraman (ACCC) and Christine Williams (DSB) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 21 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.

Update on Threat Modelling

Hemang Rathod from the DSB provided an update on threat modelling process, highlighting the review and consolidation of threat vectors to refine the security measures. This aimed to identify common elements amongst the threats and how they could be condensed while maintaining traceability and resulted in a trimmed down list of threat vectors.

The DSB noted the importance of consulting with the group to ensure the threat model's completeness and relevance to the CDR ecosystem.

One member raised a point about identifying threats that could be mitigated better, emphasising the need to focus on improvements. It was noted that the goal was to identify gaps and areas for improvement once a baseline risk assessment and threat diagram are established.

High level consultation plan for authentication uplift

Mark Verstege from the DSB outlined the consultation roadmap for the meeting, focusing on future steps for authentication uplift in the CDR ecosystem. A summary follows:

- The roadmap includes working through issues identified in previous meetings, such as redirect to app, decoupled authentication, redirect to web, data sensitivity framework, credential levels, energy and offline consumers, authentication metrics, and FAPI 2.0 security profile adoption.
- Presentations to the Data Standards Advisory Committee (DSAC) and the Steering Committee (cross CDR working group) are planned to report on progress and key considerations.
- To focus consultations on redirect to app standards, decoupled authentication, redirect to web uplift, data sensitivity framework, unlocking credential levels, energy & offline customers, metrics and FAPI 2.0 security profile and related changes.

The DSB noted that the roadmap and exercise are part of the ongoing efforts to enhance authentication standards and practices within the CDR ecosystem. They invited participants to provide feedback on the roadmap through sticky notes on a shared Miro board.

A summary of the key points and feedback from the group follows:

- The possibility of integrating digital ID with decoupled authentication flows, suggesting it could be explored in the future.
- The importance of considering implementation time frames and whether initial obligations would be voluntary, impacting the adoption pace.
- The discrete nature of artefacts and events in the roadmap, seeking clarification on their roles.
- Whether the data sensitivity framework should also consider actions (as well as data), to which the response was affirmative.
- Analysing the benefits of introducing FAPI 2 earlier and its impact on existing implementations (app2app and CIBA flows).
- The effort and time required for Decision Proposals, suggesting the potential need to span across two quarters for realistic implementation.
- Expressed difficulty with the concept of step-up authentication and suggested exploring it in more detail.

The discussions reflect the participants' concerns and suggestions regarding the consultation roadmap, emphasising the need for clear implementation timelines, consideration of Digital ID integration, and the potential impact of FAPI 2 adoption.

Review of decoupled authentication and use cases

Mark Verstege from the DSB discussed decoupled authentication and its use cases, focusing on the separation of the consumption device and the authentication device to enhance user experience and security, decoupled authentication and binding.

The DSB outlined various models and considerations for decoupled authentication and how they could enhance user experience and security. Use cases included streamlined loan applications, trusted advisor scenarios and situations where the consumption device is public or untrusted.

Key points included:

- The separation of the device initiating the authorisation request (consumption device) and the device used for authentication (authentication device).
- Various methods to connect the consumption and authentication devices, such as codes or shared identifiers.
- Examples like streamlined loan applications, where a user might start a process on a desktop but prefer to authenticate on a smartphone for convenience.

The DSB discussed various models for decoupled authentication, focusing on the separation between the consumption device and the authentication device. A summary of the models are provided below:

- **Model A (Data Holder Initiated)**: This involves the data holder initiating the decoupling within their domain, allowing for authentication within the data holder's app or website. It's a standard redirect to web flow from a CDR perspective.
- **Model B (Static Data Holder Issued Identifier)**: This involves a pre-shared identifier or token which is used to identify the consumer for subsequent authorisations, enabling the data holder to push authentication challenges to the consumer's device.
- **Model C (Static ADR Shared User Identifier)**: This involves using agreed identifiers like email addresses or phone numbers to initiate the decoupling. It requires the consumer to provide some personal information to the data recipient, which is then passed to the data holder.
- **Model D & E (Dynamic ADR Generated Identifier/Dynamic DH Generated Code Identifier)**: These models involve generating a dynamic code (e.g., a 6-digit code or QR code) that can be scanned or entered to bind the consumption device with the authentication device. Model D focuses on the consumption device displaying the code, while Model E involves the authentication device generating the code.
- **Model F (Stored Data Holder Issued User Identifier)**: This model is about generating and storing an identifier or secret on a device with limited input options, like a smart TV or IoT (Internet of Things) device, to facilitate future authentication challenges.

The DSB sought feedback via an activity from the group about what use cases we are seeking to solve and why, and what are the benefits, negatives and considerations.

One member suggested conducting a poll to understand the primary reasons for pursuing decoupled authentication, aiming to align the motivations and address the models accordingly. A link to the poll was provided to participants. The poll results highlighted different reasons why members would pursue decoupled authentication.

A summary of key points discussed followed:

- **Enabling Use Cases**: Decoupled authentication could support app-only data holders and improve security by allowing authentication to be completed in a more secure channel, such as an app, rather than relying solely on OTPs.
- **Consumer Experience and Security**: Concerns about the complexity and potential confusion for consumers with multiple decoupled authentication options. The need for clear security guidelines for data holder-initiated decoupling was highlighted to ensure secure transitions between web sessions and app sessions.
- **Security**: Apprehension regarding the collection of personal information to initiate decoupled authentication, citing the potential for social engineering attacks and the importance of safeguarding consumer data. Discussion underscored the necessity for a robust binding mechanism between the consumer's identity and the consent flow, to prevent unauthorised access and enhance security of the ecosystem.

- **Implementation Costs and Confusion**: The potential high implementation costs and confusion for both data holders and data recipients were noted, especially for models requiring dynamic codes or personal information collection.
- **Personal Information Collection**: The use of personal information to initiate decoupling raised privacy and security concerns, with some participants opposing it. However, it was acknowledged that in certain contexts, like call centres, using personal information as a hint could be valid.
- **Dynamic Data Holder Generated Code**: This model was seen as potentially useful for various scenarios, such as credit decisioning and direct debit mandate transfers, but concerns were raised about the user experience and the need for foolproof implementation.

The discussion underscored the importance of carefully considering the reasons for adopting decoupled authentication, focusing on specific use cases that would benefit from it, and addressing security and implementation challenges.

Meeting Schedule

The next meeting is scheduled for Wednesday 18 September 2024.

Any Other Business

One member suggested assigning an Action Item to review the threat modelling against the decoupled use case to ensure it serves its purpose and provides a comprehensive view on addressing potential security gaps. The DSB agreed to follow up on this task.

The Chair provided a summary of the follow up tasks as follows:

- Consider the risks and challenges and the “why” of decoupled authentication
- DSB to review the threat model against the decoupled use case to ensure its fit for purpose

Closing and Next Steps

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

Meeting closed at 11:57