Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 18 September 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 11*

Attendees

Participant Members

Mark Verstege, Chair
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
John Harrison, Mastercard
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Mark Wallis, Skript

Observers

Nils Berge, DSB
Bikram Khadka, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Christine Williams, DSB
Alicia Stewart, OAIC

Apologies

Elizabeth Arnold, DSB
Jim Basey, Basiq
Chrisa Chan, TSY
Macklin Hartley, WeMoney
Elaine Loh, OAIC
Holly McKee, DSB
Michael Palmyre, DSB
Tony Thrassis, Frollo
Abhishek Venkataraman, ACCC

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 members Jim Basey (Basiq), Macklin Hartley (WeMoney) and Tony Thrassis (Frollo) 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 4 September 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted that a number of Action Items were ongoing including:

- Biza to present at future meeting on new sharing arrangements
- DSB to outline details around TDIF documentation for group to review

Update on Threat Modelling

Hemang Rathod from the DSB provided an update on the threat modelling work noting that the focus had shifted from decoupled flows to redirect web and redirect to app flows. The decision was made to push back the discussion on decoupled flows to a later date, prioritising the work on redirect flows due to their immediate relevance.

The DSB noted that work on the threat model for redirect flows had commenced but was not yet in a state to be shared, with plans to present more details at the next session.

Uplift for Redirection to Web and "Offline" energy consumers

Mark Verstege from the DSB discussed the proposed future state of data standards, highlighting the lifting of restrictions on single-factor authentication and OTP, allowing data holders to choose authentication factors based on credential levels (CLs). The DSB also introduced a data sensitivity framework to determine the minimum credential level required for accessing data, where personal information would require multi-factor authentication (MFA), and personal data could be accessed with a single factor.

The DSB mentioned that passwords (memorised secrets) would not be permissible as a single factor under CL1 but could be used under CL2 and above. This change aimed to provide flexibility in authentication methods while ensuring data security.

Some feedback was provided from the group as follows:

A point was raised around the service point detail, particularly the National Meter Identifier (NMI), and its classification under personal information due to its inclusion of the address and whether the NMI should be accessible under CL1, considering its importance for switching use cases in the energy sector. The discussion highlighted the need to possibly differentiate access levels based on the

sensitivity of the information included in the service point details and pointed towards the potential implications for energy sector use cases and the importance of addressing the classification and accessibility of NMI within the CDR framework.

Concerns were raised around redirect authentication and risks associated with authenticating off the back of a redirect, highlighting the need for additional controls to mitigate phishing risks.

Concerns were raised about the specific definitions of SFLTP devices and SS crypto software within TDIF, suggesting they may be more suited to agency workforce scenarios rather than consumer facing environment. They cautioned against adopting these definitions without considering their appropriateness for the consumer facing space.

The DSB sought input from the group via the Miro board on whether there were any rules considerations, security questions or consumer experience considerations that needed to be captured.

Feedback provided as follows:

1. Limiting Data Clusters by Credential Level

Pros

- Reflective of the diversity in the ecosystem
- Less friction for customers at lower levels
- Aligns to best practice, unwinds conflict in rules vs standards

Cons

- Probably breaks most existing energy use cases
  - Meter ID and address used heavily for solar quotes. Restricting to CL2 might break many existing use cases. This is further an issue for bulk buy use cases in energy
  - Need to consider technical impediment (lack of uplift) preventing disclosure of data because CL2 authentication isn't implemented by the DH
- Might exclude offline energy customers from good CDR use cases
- Customer may be confused by different auth methods based on what they select – not familiar like their normal banking login experience as it changes each time
- Distinction between individual and non-individual uses cases. E.g. an address for a business (non-individual) may be considered as less sensitive to the personal/individual consumer use case.
- Should there be commensurate requirements for ADRs to authenticate end users? Restrictions on disclosure of data from the DH, but not complimentary controls for ADRs.
- We already authenticate our consumers, but we work primarily in the business use-case, so I doubt we are a "typical" ADR in this discussion

Further concerns were raised about the prescriptive nature of TDIF role requirements potentially dictating how banks authenticate their customers, not just for CDR but potentially affecting broader authentication practices. The discussion underscored the need for a detailed review of TDIF role requirements to ensure they are appropriate and do not inadvertently dictate broader authentication practices outside of CDR.

The DSB noted that they'd come back to the group with a list of specific TDIF role requirements as they apply to credential levels for review and comments from the group.

ACTION: DSB to provide a list of TDIF role requirements to group for feedback

Questions

- Not keen to introduce lookup secrets into the ecosystem, this feels like a thoroughly outdated technology with known issues similar to passwords
- Missing the distinction between enduring consent and one-off. While the clusters seem about right with regard to one-off, I'd be hesitant to make e.g. usage information available on an ongoing basis
- Obligation phasing will be important implementation consideration
- Instead of arguing specific credentials and levels, that we leverage the work that has been put into the threat model and would like to see opportunities for the data holders to articulate how the threats are mitigated by existing controls to prevent fraud and how the DH appropriately mitigates the threats.

2. Restriction of Authentication Factors for CL1

Pros

- CL1 seems to align with the current state
- Allowing a known sector for CL2 allows for more energy and lower-tech banking holders to achieve CL2 without tech investment. Restricting known secret for CL1 keeps aligned with current rules and standards, which is good Trademark (TM).

Cons

- If holders can choose in the context of their risk appetite *why* restrict?

Questions

- Are we mixing prescriptive approach with risk-based approach? The way it's described it looks like we will be introducing more friction when it's necessary. Are we mixing two separate objectives? Allow for existing authentication mechanisms, channels and risk-based approach to be used in CDR (banking). Note: energy sector needs separate considerations. Uplift authentication and credential levels across the sectors if required. If we focus on # 1 first we can reduce friction, #2 feels bigger than CDR, otherwise it conflicts with # 1.
- Authentication levels are focusing on point in time, they don't even allow for continuous authentication. Authorisation flows are governed by security profiles like FAPI with appropriate security controls, not TDIF.

3. Allow online registration within the CDDR authorisation flow

Pros

- Drives digital adoption
- Pathway to reducing exposure to offline customers
- Preferred by most energy retailers
- Will improve customer engagement and awareness of CDR ecosystem and make informed decisions reducing risk. May be considered for modifiable PI flow as well.

Cons

- Introduces identity proofing into authorisation flow
- Likely implies the need to permit other sources/flows, unclear if this would be kosher with Rules

Questions

- Does this only cover from offline to online or also from lower CL to higher CL?

4. Any other considerations, opportunities risks or concerns

Cons

- Overarching issue with the alignment to CLs/TDIF/NIST is that it is too prescriptive and unlikely to capture the full scope of protective measures taken by data holders
- Redirect to a data holder's page is inherently a risk for banks that direct customers to enter in the bank website directly.

Meeting Schedule

The next meeting is scheduled for Wednesday 2 October 2024.

Any Other Business

The Chair asked the group for feedback on next steps noting there are still a few items remaining on the backlog including metrics and gap analysis of FAPI 2.0.

Feedback included:

- A strong preference for a discussion around "gap analysis on FAPI 2.0 Security Profile" over "metrics" but noted that metrics might be of interest to other stakeholders, particularly data recipients.
- Agreement is required on what metrics need capturing before we start that discussion

The DSB noted that they will include an item for discussion around TDIF role requirements at the next meeting.

Also discussed were the potential policy implications around different sectors that might require distinct approaches to authentication due to varying risk profiles and maturity levels of digital channels. In addition, how will the Data Standard impact the data holder's ability to pivot the way they authenticate their customers as the threat landscape changes.

The DSB noted that they will need to explore the policy implications of the Data Standards Chair potentially dictating how data holders authenticate their customers outside of the CDR. They agreed to include this as an item for discussion at the next meeting (i.e. how data holders currently authenticate in their channels/what are the implications etc).

Closing

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

Meeting closed at 12:00