Data Standards Body

Information Security (InfoSec) Consultative Group
Minutes of the Meeting

Date: Wednesday 5 February 2025

Location: Held remotely, via MS Teams

Time: 10:00 to 12:00

Meeting: Committee Meeting # 17

Attendees

Committee Members

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

Observers

Nils Berge, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Matt Shaw, DSB
Fiona Walker, TSY
Christine Williams, DSB

Apologies

Elizabeth Arnold, DSB
Aditya Kumar, ANZ

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 member Aditya Kumar (ANZ) was an apology for this meeting. A number of observers also sent their apologies.

Minutes

The Chair thanked members for their comments on the Minutes from the 12 December 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 a future meeting.

Extension of the InfoSec Consultative Group

Mark Verstege noted that the consultative group commenced back in early 2024 with an initial trial period and extended for a further period of six months until December 2024. He sought feedback from members on whether the group should be extended for a further period, noting that any continuation would involve a review of membership and additional accredited data recipients (ADRs) as requested by the Data Standards Chair.

Members expressed support for continuation of the group, highlighting the group's role in understanding ADR challenges and achieving balanced outcomes.

The DSB acknowledged that there was consensus to continue the group for a further six months with meetings on a fortnightly basis, and the possibility of shifting to monthly meetings later on. The DSB would put forward views around membership and continuation to the Data Standards Chair for approval and come back to the group ahead of the next meeting.

ACTION: DSB to provide advice to the Data Standards Chair around membership changes and extending the group for a further six months

Update on planned consultations

Mark Verstege from the DSB provided an update on the planned consultations including the redirect to app decision proposal and lifting the floor for authentication standards.

The redirect to app decision proposal was initially planned for the end of last year but did not get published. It is now intended to be published this quarter, coinciding with the noting paper on best practice security.

The consultation around lifting the floor for authentication will focus on setting an appropriate minimum baseline for authentication, including frameworks around risk-based decision making and hygiene improvements for controls such as OTP.

A potential consultation on decoupled authentication is planned for later this year and consultations on FAPI 2.0, Digital ID Alignment and Success Metrics are planned for Q3.

The Data Standards Chair has asked us to also consider ADR authentication standards, and this consultation is likely to be brought forward into Q2.

Noting Paper discussion

The DSB noted that the Data Standards Chair indicated that he wanted to develop a noting paper explicitly around the Chairs obligations around Authentication Standards that adhere to best practice security.

The DSB invited feedback on the noting paper, which covers the current state of data standards, industry practices, and the Data Standards Chair's hypothesis on best practice security. The group discussed the importance of accurately representing these aspects.

Members raised concerns about the feasibility of implementing ADR authentication standards without changes to the rules. The DSB acknowledged the complexity and emphasised the need for further consultation.

The DSB in invited further feedback from the group on authentication standards and best practice via the Miro board.

Comments included:

One member suggested editorial changes to the current state analysis section of the noting paper. They recommended being more explicit about the shortcomings of the current authentication standards and removing qualifiers like "potentially" to strengthen the message about vulnerable channels.

One member provided feedback on the current state analysis section of the noting paper, specifically suggesting that the term "phishable" should refer to the OTP rather than the channel itself.

One member highlighted the importance of considering consumer awareness and education regarding the authentication mechanisms employed by different entities. They suggested that a lack of understanding could lead to consumer drop-offs when sharing their financial data with ADRs. They also mentioned that consumers might not be familiar with technical terms like "app to app" and might rely more on widely known methods like OTP.

One member pointed out that data holders have choices over how OTPs are delivered and emphasised that while there is a lot of discussion about the insecurity of delivery channels, many banks and a majority of energy holders have apps. They suggested that one way to address the issue of insecure OTP delivery mechanisms is to insist that OTPs be delivered over secure mechanisms, such as through the app.

One member commented on the standards that APRA-regulated entities must adhere to, specifically mentioning CPS 234. They highlighted that even in the absence of a specific CDR standard, APRA-regulated entities are still required to implement best practice security controls commensurate with their threat landscape. This means that these entities are not operating without standards; they are still bound by CPS 234 to maintain robust security practices.

One member noted that not all energy providers have mandated digital access. Some energy retailers turned off their digital access rather than build for the CDR. This indicates that while many energy providers may have digital access, it is not universal, and some have opted out of digital solutions in response to CDR requirements.

One member commented on the use of SMS OTPs by banking brands, noting a significant difference between the practices of the big four banks and the majority of other banking brands. They pointed out that many smaller banking brands still use SMS OTPs exclusively for secondary authentication purposes, such as sending payments. This indicated that for these smaller brands, the use of SMS OTPs is an additional requirement and a new thing they need to manage.

One member emphasised the distinction between capturing consent and achieving authorisation in the context of CDR. They pointed out that from a consumer's perspective, the process involves capturing a consent and then requesting it to be authorised, not authenticated. This distinction is crucial because consumers are often asked to authorise their consent, which can lead to confusion when they encounter authentication patterns and mechanisms that they may not expect. They highlighted that

the current authentication standards in CDR are very specific and are designed for the purpose of authorisation.

The DSB introduced the next activity, which involved reviewing the current practices within the designated sectors outside of the CDR. Feeback was sought via the Miro board and will be reviewed out of session.

The DSB further agreed to schedule a follow-up call with members to gather further feedback on this session.

ACTION: DSB to call members for additional feedback after the meeting

The DSB introduced the next activity, which involved reviewing the working hypothesis. This is based on the context set by the current state analysis, the practices within designated sectors, and the threat landscape and aims to test whether the proposed criteria for best practice security are correct. The Data Standards Chair wants to ensure that the hypothesis is validated through consultation before forming a definitive opinion. The criteria include outcomes that should be achieved to satisfy best practice security, considering security risks, consumer experience, and other relevant factors. Feedback was sought via the Miro board.

Comments included:

One member agreed with the risk-based approach and emphasised the need for some type of minimum or floor to be set, even with a risk-based approach. They also mentioned that any outcomes-based approach should have associated metrics to ensure its effectiveness. They also suggested that there should be some standards or guidelines around customer experience to maintain uniformity across the ecosystem.

One member commented that the current wording of the hypothesis avoids providing a clear opinion and lacks prescription of guardrails or minimum standards, which could lead to varied interpretations and implementations. They emphasised the need for minimum standards and metrics to measure outcomes effectively. They also noted that delegating the choice to data holders makes sense but requires validated metrics to ensure it improves drop-offs and other outcomes.

The member highlighted that it would be very difficult for the ACCC to validate compliance with the current bullet points due to their lack of technical capability and resources. They mentioned that despite existing prescriptions, organisations often engage in extensive legal arguments with the regulator, complicating enforcement.

The member also highlighted that the opening statement mentions providing minimum standards, but none of the outcomes listed specify any minimum standards. They emphasized that without defining minimum standards, the outcomes could be interpreted in various ways, making it difficult to ensure consistent implementation and enforcement.

One member emphasized the importance of distinguishing between an authentication protocol standard, such as OIDC (OpenID Connect), and the security controls applied to that standard. They noted that while adopting a global standard for implementing consent flows is useful for interoperability, the security controls that data holders choose to implement based on their risk assessments should be discussed separately.

One member expressed concerns that the current hypothesis allows data holders too much flexibility, potentially leading to inconsistent security standards across different sectors. They suggested that while the current sectors (banking and energy) might have strong existing standards, future sectors may not. Therefore, they advocated for establishing some base minimum standards to ensure consistency. Additionally, they pointed out that while the hypothesis addresses friction in authentication steps, it does not consider the significant friction consumers face before reaching this point. They also noted that the existing approach, despite its flaws, at least provides consistency.

One member acknowledged the concerns raised by others regarding the measurability of the proposed outcomes and the need for consistency. They expressed disappointment that there wasn't a consensus on the importance of consistency for consumers when interacting with banks. They emphasised that consumers look for consistency in their interactions with banks, not just for specific use cases. They suggested that this should be considered in the noting paper and that the issue of consistency should be addressed.

The DSB noted that they will incorporate feedback from the meeting into the noting paper and prepare it for circulation to the Data Standards Advisory Committee (DSAC).

Meeting Schedule

The Chair advised that the next meeting would be held remotely on Thursday 20 February 2025 from 10am to 12pm.

Any Other Business

No other business was raised.

Closing and Next Steps

Meeting closed at 11:58