Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: Thursday 20 February 2025

Location: Held remotely, via MS Teams

Time: 10:00 to 12:00

Meeting: Committee Meeting # 18

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
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID

Observers

Nils Berge, DSB
Chrisa Chan, TSY
Kyle Jaculli, ACCC
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Matt Shaw, DSB
Fiona Walker, TSY
Christine Williams, DSB

Apologies

Harish Krishnamurthy, ANZ
Michael Palmyre, DSB
Tony Thrassis, Frollo
Mark Wallis, Skript

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 Mark Wallis (Skript) 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 5 February 2025 meeting. The Minutes would be formally adopted and published on the Consumer Data Standards (CDS) website.

Action items

The Chair noted that feedback on defining measurable outcomes and metrics was ongoing and would be revisited at a future meeting. All other outstanding items were now complete.

Extension of Consultative Group

Mark Verstege from the DSB noted that the InfoSec CG would continue for a further six months (up to 30 June 2025) with meetings being held on a fortnightly basis. They were finalising the list of candidates for approval by the Data Standards Chair.

They noted that the InfoSec CG would continue consultations on authentication and other areas of information security improvement.

Best Practice Security Consultation Update

Mark Verstege from the DSB provided an update on the consultation paper, mentioning that they'd received feedback from the Data Standards Advisory Committee (DSAC) as well as this group. The feedback had been incorporated into a revised draft of the paper and would be published within the next week for the broader community to review.

One member raised a query about the adoption of Payment Service Directive 2 (PSD2) type authentication guidelines in Europe and the UK in Open Banking, which had caused a fragmented consumer experience. They asked whether this statement was anecdotal or if there was a reference?

The DSB noted that the statement was less about PSD2 and more about the original implementation of open banking through the standards and guidelines of the Open Banking Implementation Entity

(OBIE). They explained that there was not much prescription through the authorisation and authentication flow, which led to significant friction within that flow initially. They agreed to add a reference for further clarity.

Meeting Schedule

The Chair advised that the next meeting would be held remotely on Wednesday 5 March 2025 from 10am to 12pm.

Any Other Business

One member discussed the balance between data holders (DHs) risk mitigation measures and the impact on Accredited Data Recipients (ADRs) conversion rates and emphasised the need to address those concerns to ensure ADRs were not adversely affected.

The DSB acknowledged those concerns and clarified that the focus should be on drop-off rates related to risk mitigation measures.

One member emphasised the need for measurable metrics to assess the success or risk management strategies and suggested that without prescription or metrics, the same issues would persist. They also mentioned their frustration with the ACCCs technical capabilities in assessing these issues without clear metrics. They emphasised the importance of having a method to measure and compare success rates to ensure fair practices across the ecosystem.

The member also raised concerns about the potential behaviour of Non-Bank Lending (NBL) participants and the need for some form of oversight or metrics to manage risks.

The DSB acknowledged the members points including consent completion and lack of visibility. They mentioned that other open banking and open data regimes measured authentication completion and suggested that a similar approach could be considered. They indicated that measuring statistics related to authentication methods and channels could help benchmark across the industry.

Another member suggested that the group should consider how other systems handle similar issues and use that knowledge to develop a suitable approach.

The DSB noted that they would craft an agenda item for a future meeting to discuss the balance between prescription and flexibility in authentication methods and metrics for measuring success.

ACTION: DSB to add as an agenda item the balance between prescription and flexibility in authentication methods and metrics for measuring success

One member noted that FAPI 2 is now final and ready for adoption and that some key vendors are already supporting FAPI 2. They are compiling a list of differences between the last implementers' draft published 2 years ago and the final specification, which they plan to publish in the next couple of days.

One member mentioned that they are very close to being FAPI 2 compliant but highlighted limitations due to some CDR controls which are limiting, such as encrypted ID tokens and hybrid flow issues.

The DSB noted that they would follow this up and revert back. They also suggested that the member compiles a list of limitations that prevent out of the box FAPI 2 compliance to facilitate progress towards compliance.

ACTION: Member to compile a list of limitations and differences between the current CDR standards and FAPI 2 compliance for further discussion

The member noted that some DHs, particularly those using vendor-delivered core banking systems, were struggling to support code flow despite it being mandated. Some holders have figured out that the ACCC only check the discovery document, implying that if the discovery document indicates compliance, the ACCC may not verify the actual implementation.

One member asked what the thinking was behind the extension of the consultative group and whether it was meant to complement the public consultation and decision proposal process, or serve as a substitution.

The DSB explained that the group would continue for a further six-months with meetings every fortnight. They emphasised that the group had been instrumental in shaping consultations and will continue to provide feedback on early drafts and advise on enhancement to the security profile.

One member noted the prescriptive nature of the Trusted Digital Identity Framework (TDIF) requirements and suggested it might be worth revisiting at a future meeting.

The DSB acknowledged the importance of this topic and suggested that it might be better addressed with some preparation, particularly when discussing the decision proposal for the minimum baseline security.

ACTION: DSB to add as a future agenda item the prescriptive nature of TDIF

One member raised the issue of failure rates related to the ACCC register's content delivery network (CDN) upgrade which impacts their ability to monitor and alert on the status of data recipients. They mentioned the failure rate is around 1-2%, which is leading to significant operational challenges and their team had to turn off monitoring alerts to avoid constant paging. This means they may not be aware of issues with the register, impacting their ability to ensure data recipient status updates.

The ACCC acknowledged the issues with the CDN and mentioned that they were actively monitoring the CDN performance. They mentioned that they had noticed the CDN responses had dropped to less than 0.1% failure rate internally to Australia. They also requested any additional information from the member/s to help them to continue monitoring and addressing this issue.

The member responded that the 0.1% failure rate still translates to 100 failures a day for them, given the volume of calls they make to the API (they represent 60% of the total holders in the ecosystem). They emphasised the operational impacts of the CDN issues, including the mental health challenges faced by their engineers due to constant alerts. They stressed the need for a reliable solution to ensure the integrity of the data recipient status updates.

The DSB expressed interest in knowing whether this issue was widespread amongst other DHs and if members could discuss with their teams.

The DSB noted that there were ongoing discussions regarding the scale of the number of brands that NBLs provide and the impact on the register. They suggested that once they had some facts and figures to quantify the size of the issue, they would bring it back to the group for discussion.

ACTION: DSB to quantify the size of the issue related to the number of brands in NBL and discuss at a future meeting

Closing and Next Steps

The Chair noted that they hoped to have the consultation paper out and welcomed any feedback.

The Chair also suggested an early look at FAPI 2 might be worthwhile item to discuss at the next meeting.

Meeting closed at 10:58