Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 26 June 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 5*

Attendees

Participant Members

Mark Verstege, Chair
Sameer Bedi, NAB
Nick Dawson, Frollo
Olaf Grewe, NAB
Macklin Hartley, WeMoney
John Harrison, Mastercard
Ben Kolera, Biza
Aditya Kumar, ANZ
Julian Luton, CBA
Brad McCoy, Basiq
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Ruth Boughen, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
Christine Wiliams, DSB
Jon Dart, CBA
Chrisa Chan, TSY

Apologies

Jim Basey, Basiq
Nils Berge, DSB
Darren Booth, RSM
Vincent Cheen, Mastercard
Tilen Chetty, Mastercard
Harish Krishnamurthy, ANZ
Elaine Loh, OAIC
Stuart Low, Biza
Michael Palmyre, DSB

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 the initial trial period for this group is coming to an end at the next meeting. Whilst this trial has demonstrated that the approach is effective there is still a lot of progress to be made. He proposed to extend the trial for a further six meetings with periodic reviews of its usefulness and outcomes. The group agreed with this proposal.

ACTION: The Chair will seek the Data Standards Chair approval to extend the trial for a further six meetings.

One member commented that we are light on outcomes and suggested that we set aside some time at the next meeting to reflect on the outcomes to date. The group agreed with this suggestion.

ACTION: DSB to include an agenda item on "Retrospective" at the next meeting

The Chair noted that members Jim Basey (Basiq), Darren Booth (RSM Australia), Vincent Cheen (Mastercard), Tilen Chetty (Mastercard), Harish Krishnamurthy (ANZ), Stuart Low (Biza) and observers Nils Berge (DSB), Michael Palmyre (DSB) and Elaine Loh (OAIC) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 29 May 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted that the Action Items were either completed or addressed at the meeting.

Update on alignment between current regulations and TDIF

Julian Luton and Jon Dart from CBA explained the differences and gaps between the two regimes, and the challenges of mapping KYC standards to TDIF levels. They also highlighted the prescriptive and specific nature of TDIF authentication standards and suggested a more flexible and scorecard-based approach.

The Chair noted that one of the key discussion points in the group is around the principle-based approach with the Anti-money Laundering and Counter-Terrorism Financing Act (AML CTF) regulations and how we move towards a more principle-base that creates a framework without high levels of prescription and ensures there is a baseline of security across data holders.

One member asked how easy was it to adhere to the credential levels in TDIF for banks and how do they get the accreditation happening beyond banking.

CBA noted that the accreditation process is an expensive exercise as it's on a cost recovery basis and you need to get external assessors to measure your fraud and cyber controls etc.

One member asked how the credential levels relate to the IP levels (basic, standard or strong) as the government allows different services to have different requirements about the level they require.

For example, Connect ID is an exchange service between the bank and the other party. We need to decide what type of reliant party we need for the CDR.

CBA agreed there are two credential levels under consideration, and depending on the IP level you choose, that will determine what authentication security is required.

The Chair noted that they leave the proofing of identities to the data holders, and that we are talking about transactional risks and sharing certain data sets and disclosing to a third party rather than looking to introduce additional identity proofing requirements on data holders.

CBA suggested that, outside of this forum, we need to go into details about where the specific gaps are between the bank authenticators and TDIF CL123. As much as the DSB don't want to be prescriptive and tell banks how to authenticate their customers, by adopting TDIF they are. They are trying to avoid the situation where all banks in Australia as a result of moving to app2app, and therefore not having a discrete mechanism for authentication into CDR or have to change the way they authenticate their customers. They suggest most banks would rather not be regulated through CDR with regards to how they choose to authenticate their customers.

The Chair suggested that CBA share the specific gaps between the authenticators that they currently deploy in their existing digital channels against CL123.

ACTION: CBA to share (out of session) the summary of gaps between KYC standards and identity proofing levels with the DSB

Update on Threat Modelling

Hemang Rathod from the DSB shared a landscape assessment of the CDR architecture which extends beyond the boundaries of the Data Standards Chair's authority to make standards for the purposes of identifying key threats and vulnerabilities to the CDR infrastructure.

The spreadsheet (shared in the GovTEAMS channel) catalogued the entities, assets, threat actors, vectors, scenarios, vulnerabilities and risks in the CDR ecosystem. The next step was to conduct a threat risk assessment of the CDR ecosystem which included identifying threat actors, vectors and scenarios to ultimately assess residual risk. He invited feedback from the group.

One member noted that the Data Standards Chair had recently stated that there will be a formal threat modelling assessment conducted. Was that piece of work running in parallel to this assessment? They noted that the level of cyber security knowledge needed to do this piece of work justice is beyond them and they would like to bring in a cyber security expert from their organisation to work on this.

The DSB suggested that the Data Standards Chair was more than likely referring to the current Independent Health Check around threats and vulnerabilities. That work was high level, and they would certainly welcome bringing in any cyber expertise from data holders or data recipients.

The DSB noted that the next steps are to continue to evolve this information with the ultimate goal of coming up with an initial view of what controls are in place for any risks or threats identified, what the residual risk assessment is and work with the group to come up with a list of recommendations moving forward.

Update on Design Principles

Bikram Khadka from the DSB recapped the group activity from the last session on the least changes needed to enable app to app flow. He also clarified some points on the problem definition and design principles, such as the scope of authentication and authorisation, the accessible and inclusive authentication, and the multiple apps and profiles.

One member noted that multiple apps are not as straight forward and that app2app will only work if the registry has a separate data holder record or brand for each app. For example, the current setup and register will not work for all data holders because some have multiple apps for different customer bases, but they're registered only one brand because at the moment they're dealing with it in a web experience. This is the where the profile selection comes in.

The DSB asked if this could be solved by having the data holder allow some profile selection within their domain and then launch app2app from their web domain as opposed to being redirected from the accredited data recipient.

One member noted that it is probably a mix, but it depends on the existing data holder set up. If you have two apps you have to have two different redirect URLs. In the future, if you migrate to one app then the profile selection you'll have one redirect URL and one brand registered.

One member noted that pushing that onto the data holder app will be too prescriptive. The data holder may choose to have one or two apps, technically what is required is claiming the URL to which the app and redirect happens. There needs to be a provision wherein if you have two, you can define two separate redirects and switch between direct profiles.

One member asked if the DSB had given consideration to password managers in the context of data holder experiences needing to support password managers?

The DSB noted that they have not considered any requirements in the standards around that as they only have currently one-time passwords (OTP). They have also not received any feedback from the community around this (when consulting on auth uplift).

One member noted that by adhering to WCAG standards it should ensure that the accessibility features properly pick up a password field.

Draft Stage 1 & Stage 2 Authentication Uplift Standards

The Chair walked through the draft standards that incorporate the changes based on the feedback to date, such as allowing app-to-app flows, introducing a lightweight data sensitivity framework, and removing the OTP constraints. He then facilitated a group activity to critique the CX standards, authentication flows and the credential levels and authentication factors.

The group provided feedback via the Miro board.

The Chair noted the Miro board will be kept open and invites the group to provide additional feedback out of session. They will also review the feedback on the draft standards and update them accordingly and provide a GitHub repository link for further comments.

ACTION: The DSB to synthesise the feedback, update the draft standards

ACTION: DSB to provide the GitHub repository link to the group

Meeting Schedule

The Chair noted the next meeting is scheduled for Thursday 11 July 2024.

Any Other Business

No further business was raised.

Closing and Next Steps

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

Meeting closed at 11:55