Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Thursday 11 July 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 6*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
Macklin Hartley, WeMoney
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Ruth Boughen, DSB
Bikram Khadka, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Hemang Rathod, DSB
Elaine Loh, OAIC
Chrisa Chan, TSY

Apologies

Vincent Cheen, Mastercard
Tilen Chetty, Mastercard
Olaf Grewe, NAB
John Harrison, Mastercard
Harish Krishnamurthy, ANZ
Holly McKee, DSB
Brad McCoy, Basiq
Tony Thrassis, Frollo
Christine Williams, 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 the consultative group was capped at six meetings and as discussed, he has reached out to the Data Standards Chair seeking approval to extend the trial for a further period. The Data Standards Chair has approved to extension of the trail for a further period of six months.

Minutes

The Chair thanked members for their comments on the Minutes from the 26 June 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted that several Action Item will be carried over until the next meeting including:

- Biza to present on a draft spec on new sharing arrangements at a future meeting
- CBA to share a summary of gaps between KYC standards and identity proofing levels with the DSB meeting after they receive GM approval

Update on Threat Modelling

Hemang Rathod from the DSB shared the progress on the threat modelling catalogue spreadsheet that captures the entities, assets, actors, vectors, scenarios and vulnerabilities in the CDR ecosystem. The attacker model was reviewed, and information extracted on threat actors and vectors, and also extended the entities list to include some of the ones described in the rules.

They noted that more work needs to be done to build up scenarios and identify vulnerabilities and controls, with the end game to come up with a baseline threat risk assessment.

The CDR Threat Model Catalogue was shared in the InfoSec Consultative Group channel on TEAMS, and they welcomed feedback from the group.

Waterfall Authentication Model

Bikram Khadka from the DSB noted that the waterfall authentication model is a proposal for how data recipients (DRs) and data holders (DHs) can support app2app authentication with a fallback option to redirect with OTP.

The DSB presented the conceptual flow of this model, which was based on the Decision Proposal 327 and informed by the CX research last year. The model involved different decision points and scenarios depending on whether the DH app was installed, whether the redirect URL is an app or web URL, whether there is an existing context or arrangement, and whether the DH can use push notification or decoupled authentication.

The model was discussed, and some queries were raised by the participants, such as:

- Concerns about the technical feasibility and user experience of the proposed authentication flow, particularly regarding the ability of data holders to find the app and the use of intermediary web pages for consumer identification.
- How to simplify and consolidate the decision points and avoid potential collisions or conflicts with the protocol or the standards.
- How to handle the case of multiple brands or apps using the same or different redirect URLs.
- How to deal with decoupled authentication, whether it should be part of the scheme or left to the data holder, and what are the use cases and implications for it.
- How to align the authentication methods with the levels of assurance and the TDIF requirements.

Further discussion ensued about the app2app authentication process, with concerns about the user experience when transitioning between apps and web pages. The group considered the need for a seamless flow and the technical challenges associated with implementing such a process.

These issues will be further analysed and discussed at the next meeting.

Standards Review Activity

The DSB went through an activity to review the Authentication Flows, Redirect to App, Levels of Assurance (LoAs), Credential Requirements, Restricted Credentials and the CX Standards.

The activity generated a lot of feedback and questions from the participants, which were captured on sticky notes via the Miro board.

Some further discussion followed around:

Authentication Flows

- Offline consumers and the challenge of identifying users who do not have an online user ID and may need to provide multiple data points, such as email and account number, to authenticate. This is a common scenario in energy and the member offered to share some examples of the different data points that customers are collecting.
- The possibility of removing hybrid flow option from the standards as it may not be used by DRs. Suggestion that either standards should mandate the use of auth code flow for app2app, or explicitly ban hybrid flow for app2app to avoid increasing the testing load for DHs
- X-FAPI customer-IP-address is probably useless, should it be retired?

Redirect to App

- Do we collide with “Except when using a mechanism like Dynamic Client Registration to provision per-instance secrets, native apps are classified as public clients.
- Deep link reference seems confusing
- Intermediary webpage will work but the experience will be nasty. Is there a situation where the redirect URL can be the same?
- Offer the same authentication methods available to the consumer when authenticating via direct channels. Is this maybe too loose, shouldn’t we reference a baseline of acceptable app authentication methods?
- May support x2app is now ok, eventually has to be SHALL support if the app is present on the device
- Intermediary page will not work before the app – the flow is broken
- Maybe we should not use deep link term at all

- DP profile selection in the app is ok
- LoA requirements

The Chair suggested that due to the time remaining the DSB will do some thematic analysis of the feedback provided on the Miro board and raise the issues on the standards experimental repository so we can track and provide commentary against it.

Retrospective

Bikram Khadka from the DSB ran a short retrospective to gather feedback on what the consultative group should stop, start or continue doing. Some of the main pointes were:

- Continue having open discussions and time-boxing the agenda items
- Start using the Gov teams, Miro, and GitHub channels more actively to collaborate and raise issues
- Start experimenting with different authentication flows and use cases
- Start bringing in SMEs or other perspectives when needed
- Start providing more guidance on the security and CX standards

Meeting Schedule

The next meeting is scheduled for Wednesday 24 July 2024.

Any Other Business

The Chair provided a summary and next steps as follows:

- Provide an update on the threat modelling exercise
- Provide analysis around the issues and the themes raised from the feedback on the draft standards.
- Allow sufficient time of the agenda to review the Standards Review Activity feedback not discussed at this meeting
- DSB to synthesis the retrospective feedback and address any suggestions for improvements
- Allow sufficient time to discuss the thematic issues that emerged from the feedback

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