Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 24 July 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 7*

Attendees

Participant Members

Hemang Rathod, 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
Tony Thrassis, Frollo

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Ruth Boughen, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Christine Williams, DSB
Elaine Loh, OAIC
Chrisa Chan, TSY

Apologies

Mark Verstege, DSB
Jim Basey, Basiq
Harish Krishnamurthy, ANZ
Brad McCoy, Basiq
Michael Palmyre, DSB
Mark Wallis, Skript

Chair Introduction

Hemang Rathod, the Acting Chair of the Information Security (InfoSec) Consultative Group welcomed everyone to the meeting, acknowledged the traditional custodians of the land and paid respect to elders past, present and emerging.

The Chair noted that Mark Verstege (the Chair of the InfoSec CG), Jim Basey (Basiq), Harish Krishnamurthy (ANZ), Brad McCoy (Basiq), Michael Palmyre (DSB) and Mark Wallis (Skript) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 11 July 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair provided an update on the Action Item as follows:

- Biza to present on draft spec on new sharing arrangements at future meeting
- CBA to share (out of session) the summary of gaps between KYC standards and identity proofing levels with the DSB. CBA confirmed internal approvals are in place that they will reach out to DSB to lock in a meeting.

Update on Threat Modelling

Hemang Rathod from the DSB noted that the threat modelling work is in progress and aims to identify and assess the potential threats and vulnerabilities of the data sharing arrangements. It is based on reviewing various sources of information, such as reports, standards, and guidelines, and extracting relevant data in categories such as actors, vectors, scenarios, and recommendations.

The threat modelling spreadsheet has been shared in the GovTEAMS channel and members are encouraged to provide comments and feedback on it. This will help the DSB conduct a threat risk assessment and figure out the appropriate controls and mitigations for the data sharing arrangements.

Review of Retrospective

Bikram Khadka from the DSB presented the themes and action items from the feedback that the participants provided on the last meeting and one-on-one calls.

Key points included:

- Stop Runaway Conversations: It was agreed to limit discussions that deviate from the agenda.
- Equal Participation: Encouragement for all members to contribute equally to discussions.
- Clarity on scope, agenda and goals for the group and the meeting
- Proactive Discussions: Emphasis on moving conversations forward constructively.
- Meeting Preparations: Importance of publishing materials in advance for better engagement.
- Communication and Decision Making: The need for clear decision-making processes and effective communication was highlighted.
- Firm Decision Making: make firm decisions during group meetings to ensure shared understanding.

- Keeping discussions within set time limits to stay on track.

Review of Standards Experimental draft and issues backlog

Hemang Rathod from the DSB noted that the draft standards are maintained in a public repository. The issues backlog had also been created to manage and track design considerations and is publicly accessible. The group were encouraged to review and raise any issues and comments.

The DSB noted that in terms of profile selection scenarios, when it comes to redirect to app there might be gaps in some of the assumptions and they have allocated a session dedicated to gathering information to help paint a clearer picture of profile selection scenarios.

The DSB emphasised the importance of collaborative review and feedback on the draft standards and issues backlog to ensure comprehensive coverage of all necessary considerations for app-to-app flows and other related standards.

Customer Profile Design for Redirect to App

Bikram Khadka from the DSB presented three scenarios of profile selection: Scenario 1: Single Profile, multiple apps; Scenario 2: Single app, multiple profiles; and Scenario 3: Multiple apps multiple profiles. They asked the group to review the scenarios and provide feedback, comments, and questions. They also shared some general and context-specific questions, as well as some assumptions to guide the discussion. They clarified that the scenarios are not proposals, but rather a way to start the conversation and gather information.

Scenario 1: Single profile, multiple apps

The discussion focussed on the feasibility and technical aspects of having a single profile with multiple apps for a data holder. It was highlighted that this scenario, involving a choice between personal and business banking apps, is not technically feasible without specific information from the data recipient to guide the redirection to the correct app.

The discussion also touched on the technical limitations and the importance of adhering to OAuth 2.0 and FAPI standards for app2app redirection, emphasising that the redirection URL must be registered to a single app to avoid conflicts.

While scenario 1 presents challenges, focussing on the existing standards and allowing for flexibility within the ecosystem could address those issues.

Scenario 2: Single app, multiple profile

This scenario is considered feasible and reflects the current practice where a consumer has one app from a data holder but may have multiple profiles (e.g., personal and business) within that app. After consenting on the ADR, the consumer is taken to the data holder's app, authenticates, selects the profile, and then proceeds with authorisation.

The discussion highlighted that this scenario aligns with OAuth 2.0 and FAPI standards, allowing for a straightforward redirection to the app and subsequent profile selection within the app. This approach does not require changes to the standards or the register.

It was noted that data holders have the flexibility to manage profiles within their app, which does not necessitate changes to the CDR standards. The scenario supports the use of existing authentication methods, including biometrics and FIDO, within the app

The scenario allows for two paths of redirection: one at the register level with separate records for different channels (handled by the data recipient) and another post-login within the app for profile selection (handled by the data holder). This approach respects the existing setups of data holders and provides a clear path for consumer redirection and profile selection.

This scenario was widely accepted as the most realistic and feasible, aligning with current practices and technical standards.

Scenario 3: Multiple apps, multiple profiles

This scenario was discussed as a complex situation involving multiple apps and multiple profiles for a single brand. I was considered complex due to the technical and operational challenges of managing multiple apps and profiles under a single brand. The feasibility of implementing such a scenario was questioned, with concerns about the technical limitations and the user experience.

The discussion highlighted the need for clear standards and guidelines to manage the redirection between apps and the selection of profiles within those apps. It was noted that the current standards and OAuth 2.0 and FAPI protocols might not directly support such complex redirection and profile selection mechanisms.

The scenario underscored the importance of allowing flexibility within the ecosystem to accommodate different data holder setups. It was suggested that data holders should have the autonomy to manage their apps and profiles in a way that aligns with their operational models and customer experience goals.

This scenario would require innovative approaches to address the challenges presented by this scenario which might include developing new standards or adapting existing ones to better support complex app and profile management. This requires further exploration and collaboration within the ecosystem to address the challenges of implementing complex app and profile management scenarios.

Outcome

The group evaluated the different scenarios for app redirection and profile selection, with a consensus emerging that scenario two (Single app, multiple profiles) was the most practical and widely adopted model in industry. Concerns were raised about the feasibility and complexity of scenarios involving multiple apps for a single brand. The complexity of such implementations was highlighted with the group agreeing that these scenarios might not be implementable within the current standards framework.

The conversations led to a decision to focus on refining scenario two, as it represents the most realistic and feasible model for app redirection and profile selection. This decision was based on the technical insights shared and the recognition of the need for a practical approach that aligns with existing standards.

The DSB also mentioned that in a previous meeting a member volunteered to present a demo on app2app which would be useful. They proposed that the member present on this at an upcoming meeting.

Meeting Schedule

The next meeting is scheduled for Thursday 8 August 2024.

Any Other Business

The Chair provided a summary of Action Items and next steps as follows:

- Dima Postnikov from Connect ID to present on App2app at an upcoming meeting
- DSB to refine the customer profile for redirect to app and bring back to next meeting
- Group to review the draft standards and issues backlog and raise any issues or comments

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