Australian Government
The Treasury

DATA STANDARDS BODY

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Thursday 8 August 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 8*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Sameer Bedi, NAB
Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
John Harrison, Mastercard
Macklin Hartley, WeMoney
Ben Kolera, Biza
Stuart Low, Biza (from 10:30 tbc)
Julian Luton, CBA
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

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

Apologies

Harish Krishnamurthy, ANZ
Aditya Kumar, ANZ
Holly McKee, DSB
Christine Williams, DSB

Australian Government
The Treasury

DATA STANDARDS BODY

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 Harish Krishnamurthy (ANZ), Aditya Kumar (ANZ) and Christine Williams (DSB) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 24 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 a draft spec on new sharing arrangements – open action item.
- Member to share a summary of the gaps between KYC and TDIF – ongoing
- Refine the consumer profile for redirect to app – See Agenda Item 3
- Member to present app2app at an upcoming meeting – open action item
- Group to review the draft standards and issues backlog – ongoing

Terms of Reference

The Chair noted that the Terms of Reference have been updated to include transitioning from a trial period to a time-boxed period of six months. This change allows for a checkpoint to assess if the outcomes sought are being achieved and if any changes to the format are necessary moving forward.

It was noted that some members had not reviewed the ToR so this item will be tabled again at the next meeting for discussion and adoption.

ACTION: Terms of Reference to be added as Agenda Item for next meeting for adoption

Update on Threat Modelling

Hemang Rathod from the DSB provided an update on threat modelling focusing on the transition from information gathering to classification of threat vectors using the STRIDE model and cyber.gov.au categories. They are also reviewing the Threat Dragon tool by OWASP for further classification and they are planning to publish threats in a consumable format on GitHub for community contribution.

The DSB noted this work would be presented to the Data Standards Advisory Committee (DSAC) once the group had reviewed it, emphasising the ecosystem-wide perspective of threat identification.

Update on Consumer Profile design for RedirectToApp

The Chair provided an update on consumer profile design for RedirecttoApp and the importance of data holders having discretion over how they represent their brands and customer profiles, ensuring a seamless and familiar user experience.

The DSB highlighted the importance of differentiating how brands represent themselves and how customer profiles are managed. This distinction is crucial for ensuring seamless redirection to the appropriate app, considering the brand's representation in the market and the customer's interaction with the brand.

The DSB noted for Brand Profiles, the redirection to different apps based on the brand's lines of business needs to be at the discretion of the data holder. This involves how the brands presented via the CDR register and surfaced during the brand selection step in the consent flow.

The DSB noted for Customer Profiles several scenarios were discussed regarding customer profile selection, including pre-authentication profile selection, post-authentication profile selection, user managed virtual profiles, and profile switching. These scenarios aim to accommodate various data holder practices and ensure consumers have access to all eligible accounts.

The DSB noted the need for updates or additions to technical and CX standards to support these scenarios effectively. This includes considerations for how data holder brands present themselves and how user profiles are managed within the app flows.

These discussions aimed to ensure that the consumer profile design for redirect to app is flexible, familiar to users, and supports seamless integration with existing brand representations and customer interactions.

The DSB noted that app launching process involves data holders and data recipients working to claim URLs based on the operating system of the app installed. This is crucial for seamless redirection to the appropriate app from the data recipient to the data holder.

The DSB noted that for deep linking, it's essential that after authentication, users are directed into the CDR authorisation flow rather than the standard view of their accounts. This ensures the continuation of the CDR process within the app.

The discussion highlighted the need for technical standards to support deep linking and the claiming of redirection URLs, ensuring that the redirection back to the data recipient's app is seamless.

The DSB presented a sequence diagram to illustrate the process of app launching for redirect to app, focusing on the interaction between data recipients and data holders. The key points were:

- Brand Selection: The user selects a brand in the data recipient's app, initiating the authorisation flow.
- Authorisation Request: The data recipient sends an authorisation request to the data holder's pushed authorisation request endpoint, receives a request URI, and then sends it to the authorisation endpoint.
- App Launching: The data recipient checks if the data holder's app is installed and claims the authorisation URL to launch the app.

- Authentication and Authorisation: The user authenticates within the data holder's app, selects accounts, and approves the authorization.
- Redirect Back to Data Recipient's App: The data holder's app redirects the user back to the data recipient's app using a claimed redirect URL, completing the authorisation code exchange for tokens.
- Data Retrieval: The data recipient uses the access token to retrieve data from the data holder.

This process ensures a seamless user experience during the redirect to app flow, leveraging claimed URLs for app launching and redirection.

The DSB provided several recommendations regarding the implementation of the RedirecttoApp functionality:

- Data Recipients and Data Holders Implementation: Both need to implement changes to support redirect to app, including claiming URLs for seamless redirection.
- Limitations Consideration: It's important to consider the limitations of redirect to app based on different operating systems and app versions.
- Redirect URIs Usage: Data recipients should use different redirect URIs for app and mobile web flows to ensure proper redirection.
- Future Dated Obligations: There may be future obligations for data recipients to support redirection back to their app.
- Issuer and Discovery Document: Data holders should use a single issuer and discovery document per channel or app to facilitate redirection.
- Integrity Checks: Data holders should verify the integrity of the data recipient app from which the user is redirected, especially on Android platforms.
- Migration Considerations: There's a need for guidance on migration for data holders who may need to move from a single issuer to multiple issuers for different channels or apps.

These recommendations aim to ensure a seamless user experience and address technical and operational considerations for redirect to app functionality.

One member raised concerns about the implications of redirecting back to ADR apps, especially regarding web views within apps and the potential for losing context post-app opening.

The group further discussed app2app redirection and the need to set a higher baseline of operating system version to ensure security and functionality. The conversation highlighted that implementing app2app redirection might necessitate newer versions of operating systems due to security features and the technical capabilities required for seamless deep linking and app redirection.

There was concern about potentially excluding consumers with older devices from utilising app2app features, emphasising the need to balance security requirements with broad accessibility. The discussion also considered fallback mechanisms for users unable to use app2app due to their device's OS limitations, ensuring they can still participate in the CDR ecosystem through alternative methods like web flows.

The DSB asked the group for feedback on the various scenarios and considerations regarding the implementation of redirect to app functionality. A summary follows:

- Multiple URLs Claiming: It was assumed that data holders can claim multiple URLs for their app to facilitate different redirection scenarios.
- Context Loss Post-App Opening: Concerns were raised about potential issues with losing context after the app opens, especially when multiple URLs are claimed for a single app.
- Optional Claiming of URLs by ADRs: There was a suggestion that claiming URLs by ADRs for deep linking should be marked as optional, considering scenarios where ADRs might use web views within their apps for the consent collection and redirect process.
- Deep Linking and Web Views: The discussion also touched on the feasibility and implications of redirecting back to a web view within an ADR's app after completing the data holder's flow in an external browser or another app.

This reflects the discussions and considerations for enhancing the user experience and technical implementation of the redirect to app functionality in the CDR ecosystem.

Design Discussion on New Issues from the Backlog

The DSB reviewed the backlog on GitHub and based on discussions reordered the items accordingly.

Meeting Schedule

The next meeting is scheduled for Wednesday 21 August 2024.

Any Other Business

The Chair provided a summary of next steps as follows:

- Further investigate and model out different flows for app2app redirection, especially focusing on redirecting back to a web view within an app. This aims to clarify the technical feasibility and user experience implications (DSB).
- Error Handling: Review and prioritise error handling scenarios for redirect to app to ensure seamless user experiences during redirection failures or errors (DSB)
- Discuss and decide on retiring the hybrid flow to streamline the authentication process.
- Deep Linking: Clarify and document the best practices for deep linking and redirection back to the ADR app, ensuring both data holder and data recipients support deep linking for a consistent app2app experience (DSB)
- Memorised Secrets: Evaluate the use of memorised secrets in the context of energy sector authentication. (BIZA - Stuart)
- Migration Considerations: Formulate guidance on migration for data holders moving from one issuer to multiple issuers. (DSB - Mark)
- Minimum Security Standards: Define minimum security standards for redirect to app to ensure broad consumer access. (DSB - Mark)

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