Australian Government | data standards body

Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: Wednesday 2 April 2025

Location: Held remotely, via MS Teams

Time: 10:00 to 12:00

Meeting: Meeting # 20

Attendees

Committee Members

Mark Verstege, DSB
Sameer Bedi, NAB
John Harrison, Mastercard
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

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

Apologies

Darren Booth, RSM
Nick Dawson, Frollo
Olaf Grewe, NAB
Macklin Hartley, WeMoney
Ben Kolera, 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 provided an update on the status of the Data Standards Chair's obligations around best practice security for authentication standards consultation and the redirect-to-app decision proposal, mentioning that they are still undergoing internal review, and they are slightly behind scheduled. The papers incorporate feedback from the Data Standards Advisory Committee (DSAC) and CDR agencies.

The Chair noted that member Darren Booth (RSM), Nick Dawson (Frollo), Olaf Grewe (NAB) Macklin Hartley (WeMoney) and Ben Kolera (Biza) were apologies for this meeting. A number of observers also sent their apologies.

Minutes

Minutes

The Chair thanked members for their comments on the Minutes from the 19 March 2025 meeting. The Minutes would be formally adopted and published on the Consumer Data Standards (CDS) website.

Action items

The Chair provided an updated on the action item as follows:

- Defining measurable outcomes and metrics for the authentication uplift work will be tabled for a future meeting. This is pending DSB's discussions with CDR agencies
- Membership changes are in progress. The outgoing Chair approved a change of membership, which is currently being reviewed by the new Chair. The current membership will continue for the next six months
- The outstanding action item around the balance between prescription and flexibility in authentication methods and metrics for measuring success will be address at a future meeting
- The outstanding action item regarding the prescriptive nature of TDIF will be addressed in the consultation draft on minimum baseline security and at a future meeting.
- The issue related to the number of brands in NBL. A survey will be sent out to NBL and banks as part of the consultation around the v8 rules. The survey aims to gather information on how brands and products are represented within the NBL sector.

One member emphasised the importance of staying on top of the NBL implementation, as there are many decisions being made by NBL on how to implement the rules.

FAPI 2.0.0 Gap Analysis

The Chair invited Stuart Low from Biza to provide an analysis between FAPI 2.0 and CDR to understand what the delta is and to get our current security profile FAPI 2.0 to final.

The Chair highlighted the importance of FAPI 2.0, not just for baseline security but also for future opportunities to build upon business capabilities, such as fine-grained authorisation and consent. They referenced the Inquiries into the Future Directions Report for the CDR, which significantly touched on fine-grained authorisation.

Biza noted that the current CDR implementation is very close to FAPI 2.0's baseline security profile. The main interest is to achieve FAPI 2.0 certification from OpenID and ensure it works for CDR.

Biza noted that FAPI 2.0 requires both the OIDC Discovery document and the OAuth 2 Discovery document, whereas the current CDR only supports the OIDC Discovery document. This will necessitate the introduction of the OAuth 2 Discovery document.

Biza noted that FAPI 2.0 does not mandate pre-registered redirect URIs, allowing them to be supplied in the PAR. They suggested that CDR could continue to mandate pre-registered redirect URIs without impacting certification.

Biza noted that FAPI 2.0 mandates specific HTTP codes, such as banning HTTP 307 and requiring HTTP 303 for redirecting user agents. The current CDR does not have explicit requirements for these codes, which will need to be addressed for alignment.

Biza noted that FAPI 2.0 requires tokens to have at least 128-bit entropy. The current CDR does not mandate token entropy, and some implementations use shorter tokens, which will need to be updated to meet the FAPI 2.0 requirements.

Biza concluded that the key changes for alignment with FAPI 2.0 include the introduction of the OAuth 2 Discovery document and specific HTTP codes. These changes are not dramatic changes but necessary for certification and improved security.

One member emphasised that FAPI 2.0 does not mandate the use of Rich Authorisation Requests (RAR) but recommends it when the scope parameter is not expressive enough. They highlighted the importance of aligning with global standards to increase vendor support and security benefits.

One member noted that message signing is a significant part of the certification process and that a separate profile for CDR would be necessary. They also referenced an article comparing FAPI 2.0.0 Final specification and the Implementer's draft which highlights relevant changes.

One member highlighted the importance of identifying and understanding the business use cases that can be enabled by FAPI 2.0.0, such as improving lending decisions, energy switching, and accounting services for small businesses.

The DSB noted that adopting FAPI 2.0.0 offers a mechanism to standardise more comprehensive authorisation requests. This would help data recipients (DRs) observe the data minimisation principle better and ensure that only the required data is returned.

The DSB mentioned that fine-grained authorisation could enable more sophisticated use cases, such as specifying product categories or the duration of historical transaction data needed. This would be particularly beneficial for use cases like responsible lending and payments.

One member expressed concerns about the difficulty in justifying the implementation of FAPI 2.0.0 They noted that while the technical improvements are clear, there is a lack of direct consumer benefits or new consumer engagement that can be easily demonstrated. They emphasised the importance of aligning the implementation of FAPI 2.0.0 with the onboarding of NBL.

One member noted that the benefits of going to FAPI 2.0.0 is that FAPI 2.0.0 recommends the use of RAR, which allows for a more detailed and structured authorisation process. This creates a container for metadata directly associated with the authorisation, enabling more expressive and comprehensive authorisation details.

The member mentioned that the current scope parameters are not expressive enough for many use cases. FAPI 2.0.0's RAR provides a mechanism to include additional attributes and constraints, such as time-based elements and varying levels of data access, which supports better data minimisation practices.

They also emphasised that FAPI 2.0.0 sets a foundation for future use cases beyond the current CDR framework. This includes potential actions like account opening, account closing, and modifying payees, which are not possible with the current CDR specifications.

One observer suggested that cost-benefit analysis of the implementation of FAPI 2.0.0 could be evaluated in tranches or incremental steps, as there may be a minimum baseline of requirements, plus extensions for future feature capability.

One member suggested that one of the measurable outcomes should be the alignment with FAPI 2.0.0 standards. They proposed that the goal should be to fully align with the upstream standard and measure any divergence from it negatively.

Fine-grained authorisation Use Cases

The Chair introduced the topic of fine-grained authorisation by highlighting the current limitations and the need for more detailed control over data sharing in the CDR ecosystem. Key points included:

- The current system is coarse-grained, with consent requested through authorisation requests that map to specific data clusters and API endpoints. This often results in DRs having to request entire data clusters to access specific data elements they need.
- Authorisation is conveyed through OAuth scopes, which are limited in granularity. The sharing duration attribute only specifies how long data can be collected, not the historical range of data.
- DRs have no visibility over account selection, which can lead to incomplete data sharing for use cases like responsible lending.
- There have been multiple sources of input identifying the need for fine-grained authorisation, including the Future Directions Report, consent review, and use case realisation work. These sources have highlighted the need for more detailed permissioning language to support various use cases and improve data privacy controls.

The DSB invited the group for their views on the first activity which focused on identifying the outcomes and purposes of implementing fine-grained authorisation in the CDR ecosystem.

One member emphasised the importance of not just solving specific use cases but ensuring that the designed schema for fine-grained authorisation can be used by the market at large for various purposes and required attributes can be incrementally added to.

One member emphasised the importance of identifying the challenges associated with implementing fine-grained authorisation early in the consultation process. They noted that this is a significant change and there will be challenges to address. Whilst technical challenges are important, understanding the challenges from the customer's perspective is crucial.

One member emphasised that the primary value of fine-grained authorisation lies in providing more granularity and control over the data that gets shared. This approach allows for better data minimisation, ensuring that only the necessary data is shared.

One member expressed concern that without a clear mandate from the Minister or specific rules, it would be challenging to justify the implementation of fine-grained authorisation. He noted that while the Minister has expressed a desire to eliminate screen scraping and see more use cases, there hasn't been detailed guidance on what those use cases should be.

One member suggested the need for a mandated standard to drive market adoption and innovation, and the importance of experimentation and risk-taking to demonstrate the value of new capabilities within the CDR framework.

One member emphasised the need for clear communication regarding response times to improve the quality of service, suggesting the use of indicators to differentiate between immediate and asynchronous responses.

One member emphasised the need to streamline consent flows to avoid repetition and address customer concerns with the "Get Customer" API to enhance user experience and trust.

One member suggested that a metadata construct could be used to specify which attributes are disclosed in a response. This would allow for partial or dynamic disclosure of customer details, addressing concerns about sharing too much information.

The member also mentioned that all business holders support status polling, which allows DRs to actively poll the status of an arrangement and understand where it is in the consent flow. This functionality is already available but not widely adopted by recipients.

One member proposed using RAR with OpenID (OID) to issue verifiable credentials. This could allow DHs to issue credentials that customers can use to prove their income or other attributes without disclosing personal information.

The DSB provided an overview of activity two which focuses on categorising use cases, providing practical examples, and identifying the necessary functionality to support fine-grained authorisation. They invited the group to provide feedback.

One member highlighted a problem where authorisations are established for multiple accounts, but if a consumer loses access to one of those accounts, the ADR is not notified. This results in errors and accounts disappearing from the get accounts listing without proper notification. They emphasised the need for improved notification mechanisms to inform ADRs about changes affecting authorisations, ensuring better handling of such scenarios.

The DSB acknowledged that the current system only notifies ADRs of CDR arrangement revocations, which is a limited solution. They suggested a shared signals profile which could provide a more comprehensive notification solution.

A summary of feedback around what other uses cases we should consider follow.

One member mentioned that subscriptions, along with other use cases like loan origination and real estate applications, have been requested by their customers. These requests come from both the organisations they work with and the customers of those organisations.

One member emphasised the need for fine-grained authorisation to support multi-party authorisation use cases, improve status understanding, and handle asynchronous authorisation flows.

One member highlighted the importance of account switching for better financial terms, the need for a complete financial picture in lending scenarios, and the challenges in the current consent flow.

One member emphasised the potential for agentic authorisation and delegated authority to enhance the CDR framework, particularly for complex scenarios like energy switching and cross-sector action initiation.

One member emphasised the need for improved notifications and shared signals to handle changes that affect data sharing arrangements, particularly when accounts become inaccessible or nominated representatives leave an organisation.

One member mentioned that in their implementation, if a nominated rep leaves the business but there is still another nominated rep attached to the business and account, the data sharing arrangement should not be affected. This ensures continuity of the arrangement despite changes in personnel.

One member pointed out that if a data sharing arrangement is terminated due to the departure of a nominated rep, that is a compliance issue. The arrangement should remain valid as long as there are other nominated reps, or the business entity itself holds the arrangement.

A summary of feedback on how the use cases could be achieved follows:

One member mentioned that relying solely on RAR might not fully achieve the desired objectives. They explained that in their research for developing arrangement V2, they realised the need for a more comprehensive approach to managing sharing arrangements.

The member also questioned the need of whether it is necessary to continue supporting both scopes and RAR which could add unnecessary cost and complexity. They suggested a streamlined approach with broad scopes and detailed metadata.

One member empathised the importance of aligning with global standards rather than creating an Australia-specific solution. They suggested that this approach would increase vendor support and provide additional security benefits.

The DSB suggested continuing the discussion at the next meeting, focusing on impacts, complexities, and cost considerations.

One member suggested revisiting common problems that have been discussed previously, indicating that many of these issues are still relevant. They proposed experimenting with potential solutions to these problems, rather than waiting for standard changes, which could take years. They emphasised the importance of taking proactive steps to solve these issues.

Meeting Schedule

The Chair advised that the next meeting would be held remotely on Wednesday 16 April 2025 from 10am to 12pm.

Any Other Business

No other business was raised.

Closing and Next Steps

The Chair thanked members for attending the meeting.

Meeting closed at 11:57