Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 15 May 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 2*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Sameer Bedi, NAB
Nick Dawson, Frollo
Olaf Grewe, NAB
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Brad McCoy, Basiq
Dima Postnikov, Connect ID
Tony Thrassis, Frollo
Mark Wallis, Skript

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Ruth Boughen, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Hemang Rathod, DSB
John Williamson, ACCC
Elaine Loh, OAIC
Chrisa Chan, Treasury

Apologies

Darren Booth, RSM Australia
Vincent Cheen, Mastercard
Tilen Chetty, Mastercard
Macklin Hartley, WeMoney
Harish Krishnamurthy, ANZ
Michael Palmyre, DSB

Chair Introduction

Mark Verstege, the Chair of the Information Security (Info) Consultative Group welcomed everyone to the meeting, acknowledged the traditional custodians of the land and paid respect to the elder's past, present and emerging.

The Chair welcomed Aditya Kumar from ANZ to the group. He will be replacing Gaurav Rathi as ANZ's nominated representative on this consultative group.

The Chair noted that Harish Krishnamurthy (ANZ), Michael Palmyre (DSB), Darren Booth (RSM Australia), Vincent Cheen (Mastercard), Tilen Chetty (Mastercard) and Macklin Hartley (WeMoney) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 24 April 2024 meeting. The Minutes were formally accepted and will be published on the Data Standards Body website.

Action Items

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

Governance

Terms of Reference

The Chair sought last minute feedback from the group around the Terms of Reference (ToR) prior to adoption.

One member suggested metrics to define what success looks like including metrics around security and consumer experience which are important. They could be included as part of the ToR or as objectives.

There was further discussion around:

- How prescriptive the metrics should be versus taking a principles-based approach
- Need for consistency in the authentication experience for consumers across data holders to ensure good conversion rates
- Whether consistency means consistent across CDR or consistent with consumers' existing authentication methods with banks.

One member noted there was a recommendation in the UNSW Cyber Security report, which was recently published, for TSY to conduct threat modelling on a periodic basis. That could identify the current and potential threats, would be measurable and this group could work to migrate the risks.

The Chair asked the group whether we should add this to the ToR or add it as an Agenda Item for further discussion.

One member noted that they would be comfortable with something that was not particularly specific and have an agenda item that would determine how we measure that. One of the stated aims of this consultative group is to achieve a measurable, positive impact to information security in CDR.

The Chair noted that they will table this for discussion at the next meeting. He also asked the group to provide input on the ToR via GovTEAMS.

ACTION: Group to provide input on the ToR prior to the next meeting

Code of Conduct

No further feedback was provided on the Code of Conduct (CoC).

The Chair formally adopted the CoC and advised that these will be published on the Data Standards Body website.

Problem Definition Statement

CDR Cyber Security and Data Standards InfoSec Uplift

The Chair noted the Data Standards Advisory Committee (DSAC) has requested the InfoSec Consultative Group (InfoSec CG) consider a broader cyber security landscape prior to developing solutions and report back to them.

The following questions have been proposed for consideration by the group:

1. What are the key cyber security problems the CDR needs to consider over the next 3-5 years?
2. What are the biggest threats the CDR needs to solve for over the same horizon?
3. How does the InfoSec uplift in the CDR complement other government cyber security initiates (e.g., scams)?
4. What are the broader elements needed for a sustainable cyber security framework for the CDR?

The group discussed the key problems, threats, and focus areas the CDR needs to address over the next 3-5 years. There was debate around achieving consistency in authentication methods while allowing choice and meeting security baseline. The scope and focus were discussed with agreement that clear problem statements are needed before discussing solutions.

One member suggested building and maintaining a threat model for CDR. This will make it clear what we have to fix and potential future threats. An end-to-end assessment of the ecosystem has been missing.

Another member noted prioritisation should be on a timeline basis i.e., priorities over the next 12 months not over the next 3-5 years.

One member noted we need a method of mapping threats to what exists in InfoSec today and suggested mapping out the CDR architecture to identify the gaps.

The Chair agreed it would be good to map out of the interface points and security controls and see what threats may exist at each point. However, as a group we need to decide what the focus is for the short term.

Data Standards Authentication Uplift

The Chair noted at the last meeting the group agreed the problem definition statement we are solving for with regard to authentication needs to be agreed. The problem definition Statement follows:

> *How can the Standards provide safe and secure verification of consumers in a way that provides consumers a consistent consumer experience whilst allowing Data Holders to offer authentication choice?*

One member suggested adding "maintaining conversion rates" to the problem statement. Another member noted there may be a debate around what consistent means in the context of authentication methods. They support using the term consistent to refer to standards for the consumer experience, which can help CDR be successful.

One member noted a principle that's missing is that consumers should be using existing authentication, and familiar authentication method with the bank. That is the best outcome from a security and user experience perspective.

Another member disagreed. When the rules and standards were made it was for the purpose of the CDR not for internet banking. That is what we have and what we need to improve from.

One member noted if we move to app2app, and the Data Standards dictate the constraints around how the app is authenticated this would dictate how every bank in the country is authenticated because they can't differentiate between a CDR consent flow and a customer logging onto the app.

The Chair suggested the standards could set a minimum-security baseline while allowing flexibility via a data or risk sensitive framework. For example, getting agreement around risks for data sensitivity analysis and map the credential levels to the appropriate risks etc.

The DSB noted when defining the baseline, we should consider weaker security in sectors beyond banking.

One member argued against overprescribing standards and risking unintended consequences. The rules don't prescribe authentication methods, just consistency with existing authorisation methods with a CDR tag.

One member noted we shouldn't get into solution-mode, we are defining the problem statement and descoping. There will be time and space to debate the solutions.

One member noted in terms of authentication, the group should consider whether it's the DSBs job to specify the minimum floor or is it a job for another industry organisation because authentication is bigger than just CDR.

One member suggested first addressing the problem of data holders needing to downgrade security to support the current CDR standard. There is lack of clarity on whether the goal should be consistency within CDR or with existing holder authentication methods.

One member noted one of the biggest mistakes is thinking that CDR is a product when the growth has been problematic. It started off as the consumer should have this choice to share their data and evolve into building CDR.

The Chair summarised the main points of the conversation around alignment with data holder experiences and where CDR fits within national value proposition; is it simply aligning to what data holders do; and whether the word "consistent" and whether it is just about improving consumer experience rather than consistent consumer experience.

A number of members support the use of "consistent" in the problem definition statement.

One member noted this forum has been put together at the bequest of the DSAC and the Data Standards Chair who was asked for an uplift in security to work out what authentication uplifting should look like to solve the security threat problems. This doesn't mean we shouldn't look at other government initiatives, but this request has come from the Data Standards Chair.

Another member noted there are two school of thoughts for the use of "consistency". One being consistency within the CDR ecosystem or consistency and familiarity with customers natural way of authenticating into their banking. They are not sure if this forum is the right place to figure out what the best adoption mechanism is.

The Chair suggested moving the discussion towards reviewing the principles to shape the problem definition statement.

Key set of questions

This item was not addressed at the meeting. It will be tabled at the next meeting.

Design Principles

The Chair noted, as agreed at the last meeting, a set of guiding principles were drafted for discussion as follows:

1. **Data Holders authenticate consumers:** In order to verify the consumer before disclosing data, it is the Data Holder's responsibility to authenticate the customer.
2. **Authentication is commensurate to the risk:** Authentication controls should be aligned to the sensitivity of the action being initiated or the data being disclosed.
3. **Parity of experience:** the experience available to a consumer when authenticating via an ADR-initiated consent flow should involve no more steps, delay or friction in the customer journey, unless otherwise required by the Data Standards, than the equivalent experience they have with their Data Holder when interacting directly.
4. **Enable innovation:** Data Holders should be allowed to modernise authentication controls within the CDR without being constrained by limitations in their existing channels.
5. **Authentication is accessible and inclusive:** Authentication controls need to be accessible and inclusive to all consumers including those that are vulnerable, those with disabilities and those in remote communities or without consistent access to technology.
6. **Authentication choice:** Data Holder and consumers should have choice in the authenticators they use provided they are appropriate to the risk.
7. **Authentication is familiar:** Authentication should provide a consistent and familiar experience to consumers across Data Holders that promotes safety and security.

One member reiterated the need for a principle around not deteriorating the customer experience or increasing drop-off rates. Discussion occurred around whether friction should be allowed during the initial CDR authentication step or later during the authorisation process. It was suggested explicitly separating authentication and authorisation and measuring authentication conversion rates.

Another member noted specific principles around no degradation of existing authentication conversion rate, and a baseline is also needed.

One member asked in terms of Item # 2, for certain “reads” could we have a lesser authentication burden or less friction in the authentication process? It was noted this would depend on the risk and acknowledging there may be higher risk data which may require a higher level of authentication and data that is deemed less risky because it is not sharing personally identifiable information.

One member noted in terms of item # 5, when a consumer wishes to cease their data sharing arrangement with the data holder, and they wish to do so not in the digital channel. They should remove their consent via the digital channel - do we need to add this as a principle? The driver behind this is to provide an alternate method for those that may not have confidence to do it online. Another member suggested a commonsense approach should be reflected in the principle re: this.

The member also noted for item # 6, we need to keep an eye on the no degradation of existing conversion rate for authentication and for item # 7, what do we mean by the word “familiar”? We need to be consistent within the CDR framework and potentially keeping a concise set of authentication mechanisms that a data holder can choose from.

One member noted in terms of item # 4, should this be worded the other way around? If we have constraints within the standard that may constrain data holders innovating how they choose in the future to authenticate their customers it could potentially require a change in the standard.

The member also noted in terms of item # 3, data holders are increasingly deploying methods where they deliberately increase friction depending on their risk scoring for the event. We need to recognise this.

There was discussion around whether solutions should focus narrowly on the initial consent authorisation step or more broadly enable future use cases like action initiation. One member noted the scope should be limited to the consent authorisation flow while another felt it should enable future expansion. The group generally agreed consumer protections in banking apps today are likely adequate for CDR as well.

One member noted in terms of Item # 2, if there’s a malicious actor or in the likelihood of the risk being higher and there’s an additional friction involved in the process, is there a need for a level of guidance in the authentication? Should it be static or more dynamic which is where most of the models are evolving towards, and do we need an additional principle? Or can we revise item # 2 to elaborate what the risk position means?

One member noted in terms of Item # 7, suggested either removing or being more explicit on the “familiarity” aspect.

The Chair asked the group how we would achieve the conversion rate for authentication and what changes would they propose to the principles and if authentication is aligned to data holder channels, are we assessing a conversion rate against the data holder’s current conversion rate in their other channels or are we assessing that against what exists today?

One member suggested it should be baselined off the existing conversion rates for authentication so no degradation of existing authentication conversion rates.

It was agreed that “No degradation of experience: There should be no unreasonable friction that impacts consumer outcomes or creates lower conversion of consumer outcomes compared to CDR’s OTP authentication flow today” be added as an eighth principle.

The Chair noted that further discussion was required to come to an agreement on the Problem-Definition Statement and there is general consensus on the principles. However, he did ask the group to review again with their teams and come back with any further feedback at the next meeting.

ACTION: Group to review problem-definition statement and Principles and provide a further input

Meeting Schedule

The Chair noted the next meeting is scheduled for Wednesday 29 May 2024.

Any Other Business

One member asked if we could establish an architecture that the group could review to identify any gaps.

Closing and Next Steps

The Chair suggested that at the next meeting, we will include agenda items on the Problem Definition Statement and to review the high-level architecture and risks for the groups review.

ACTION: DSB establish an architecture for the group’s review

One member noted they have a specification draft related to a new sharing arrangement they would like to present to the group which is relevant.

The Chair agreed to add this as an agenda item to a future meeting.

ACTION: Member to present on new sharing arrangement specification draft at future meeting

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

Meeting closed at 11:58