Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 29 May 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 3*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Darren Booth, RSM Australia
Vincent Cheen, Mastercard
Ben Kolera, Biza
Aditya Kumar, ANZ
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
Michael Palmyre, DSB
Hemang Rathod, DSB
Christine Wiliams, DSB (joined at 11am)
Elaine Loh, OAIC

Apologies

Sameer Bedi, NAB
Tilen Chetty, Mastercard
Nick Dawson, Frollo
Olaf Grewe, NAB
Macklin Hartley, WeMoney
Harish Krishnamurthy, ANZ
Stuart Low, Biza
John Williamson, ACCC
Chrisa Chan, Treasury

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 members Sameer Bedi (NAB), Tilen Chetty (Mastercard), Nick Dawson (Frollo), Olaf Grewe (NAB), Macklin Hartley (WeMoney) and observer John Williamson (ACCC) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 15 May 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) 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. The ToR were adopted and will be published on the CDS website.

Problem Definition Statement

The Chair noted that the Problem Definition Statement had been revised based on feedback received at the last meeting to ensure that a clear and concise statement captures the core problem to be solved.

The Chair sought feedback on the following revised statement:

Problem Definition # 1: 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 (DH) to offer authenticator choice?

Feedback provided:

- Need to be clear there can be no degradation of existing conversion rates by implementing a new authentication interaction
- Need conversion rate in the problem statement
- Meaning of "consistent" needs to be clear
- There are two schools of thoughts for the use of "consistency". One being consistency within the Consumer Data Right (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.
- How can the Standards provide safe and secure verification of consumers in a way that provides consumer a consistent consumer experience (CX) across CDR whilst allowing data holders to offer authenticator choice?
- Can't have both. Either consistent within the DH exp or across DH in CDR

- Where does the current authentication standard fall down? Is it only against other standards or do we have a proven gap or failure in the current redirect with one time password (OTP)?
- By aligning the consumer's experience with their existing DH login experience
- We need to aim for a low cognitive load on consumers, balanced with a clear awareness they are sharing their data
- Could we say a successful consumer experience?
- What is the issue with current OTP, where is the gap?
- Language to state prepare for future initiatives
- Should authentication be aligned more to minimum credential level (CL) to be met, instead of being specific on the authenticator type (OTP, app2app or otherwise)

Problem Definition # 2: Prior to a more comprehensive change to the Standard, is there a discreet wording change to the baseline security provisions that allows data holders to implement app2app or equivalent authentication methods in lieu of the one-time password requirement?

Feedback provided:

- Problem of data holders needing to downgrade security to support the current CDR standard. There is a lack of clarity on whether the goal should be consistency within CDR or with existing DH authentication methods.
- If we move to app2app, and the Data Standards dictate the constrains around how the app is authenticated, this will dictate how every bank in the country in authenticated because they can't differentiate between a CDR consent flow and a customer logging onto the app.
- Whether it's the Data Standards Body's (DSB) job to specify the minimum floor or is it a job for another industry organisation because authentication is bigger than just CDR
- Suggested "as well as" rather than "in lieu of"
- Agree with statement #2

Problem Definition # 2b: What is the minimum amount of change to enable app2app?

Feedback provided:

- Agree with statement #2b
- If app2app was introduced as an optional inclusion by DHs for an initial phase the minimum effort for this phase could be none for DHs who chose to opt out
- This phase could also be used to prove out app2app before mandating every DH implements this authentication method
- I think the wording will be relatively easy. The obligations will be harder. Can a DH drop OTP for app2app etc
- Probably make it optional, however doing so may not be enough to drive broad adoption

The group discussed the Problem Definition Statements and refining the language around 'consistency', risk levels, security, and consumer experience. There is agreement that rather than being prescriptive on authentication methods, the standards should refer back to credential levels and minimum requirements to provide more flexibility.

Design Principles

The DSB noted that the Design Principles have been revised based on feedback received at the last meeting and provided below for further discussion.

Principle 1: Data holders authenticate consumers

In order to verify the consumer before disclosing data, it is the data holder's responsibility to authenticate the consumer.

Feedback provided:

- In a world where consumers may use third party identity services to authenticate to (more than one) data holder(s), does this principle still stand?
- Consistent with standards today

The group accepted principle # 1.

Principle 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.

Feedback provided:

- Similar to purpose-based consents, can we have a purpose-based authentication process?
- Yes, but who controls the controls? DHs already have robust controls in place to protect their customers when authenticating to channels
- At time of consent this is not known other than consent
- Commensurate to the risk of the action
- For certain read actions 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 (PII)
- 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?
- Support step-up authentication when risk is assessed

Principle 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 consumer journey, unless otherwise required by the Data Standards, than the equivalent experience they have with their DH when interacting directly.

Feedback provided:

- This principle places too much emphasis on data standards. If customer authentication is as per existing channels, not sure this is needed
- Business customers who are unlikely to have the DH app shouldn't be forced to install it just to consent
- Proposed adding "parity" to principle #2Data holders are increasingly deploying methods were they deliberately increase friction depending on their risk scoring for the event. We need to recognise this.

Principle 4: Enable innovation

Data Holders should be allowed to modernise authentication controls within the CDR without being constrained by limitations in the existing channels.

Feedback provided:

- Agree with other comment here, noting that it should not result in a less secure method, there are likely to be modern authentication methods that appear faster than the Standards can be updated to include them.
- If the Data Standards defer to DHs for authentication, then this principle isn't needed
- Add above the baseline standard
- Should this be worded the other way around? If we have constraints within the standard that may constraint data holders innovating how they choose in the future to authenticate their customers, it could potentially require a change in the standard

Principle 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.

Feedback provided:

- There is a 'greater good' moral dilemma here. By forcing a lowest common denominator to support a tiny minority we may weaken security for everyone (for example)
- 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.

Principle 6: Authentication choice

Data Holder and consumers should have choice in the authenticators they use provided they are appropriate to the risk.

Feedback provided:

- This is very open to interpretation
- If the data standards defer to DHs for authentication then this principle isn't needed
- The choice should factor in the customer demographic – i.e. we should enforce the same choice across retail and business customers
- Do we need this at all?

Principle 7: Authentication is familiar

Authentication should provide a consistent and familiar experience to consumer across data holders that promotes safety and security

Feedback provided:

- We need to keep an eye on the no degradation of existing conversion rate for authentication
- 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
- Suggested either removing or being more explicit on the "familiarity" aspect
- Authentication is simple to understand and use
- If the data standards defer to DHs for authentication then this principle isn't needed
- Yes, but is this CDR to prescriber?

Principle 8: No degradation of experience (new principle: added after meeting #2)

There should be no unreasonable friction that impacts consumer outcomes or creates lower conversion of **consumer** outcomes compared to CDRs OTP authentication flow today.

- Should it be baselined off the existing conversion rates for authentication so no degradation of existing authentication conversion rates

The DSB agreed to review the feedback provided and come back with an update at the next meeting.

ACTION: DSB to provide update on Design Principles at next meeting

The DSB shared the "Double Diamond approach to design" and pointed out we are currently in the "defining" step of the design process. This approach involves gathering information to understand key issues before considering solutions and notes that it is important not to rush into solution-mode while exploring and considering different options.

High Level Security Architecture

The Chair noted that at the last meeting we discussed modelling the key threats to the CDR and it was agreed that the DSB would create a high-level architecture.

The DSB presented a model with the different interaction points between the data holder and data recipient for group discussion.

They also noted that taking into account the Problem Definition Statement and Design Principles we need to consider the following key design questions:

Baseline security

1. What is minimum or baseline security
2. When is a required control necessary, and what are the determining criteria?
3. When should implementation choice be preferred (e.g. map data sensitivity to credential levels and allow DHs to decide what authenticators are used)?

Threat identification

1. What are the primary threats to protect against?
2. What are the risks being mitigated?
3. What are the appropriate controls to mitigate the risk?

Solution Evaluation

1. What are the costs and implementation considerations?
2. 2. Does the solution increase consumer safety or security?
3. 3. Does the solution improve the consumer experience?
4. 4. Does the solution improve consumer outcomes (including conversion rates)?
5. 5. Should the solution be tested via an experimental or voluntary standards?
6. 6. Should the solution be mandated or voluntary?

The Chair suggested focusing on threat modelling for authentication uplift and allowing participants to start identifying key threats across the different system interfaces shown in the high-level architecture diagram, including overlaying threats already identified by the FAPI security profile.

The Chair noted he will break the security architecture diagram into functional areas of interaction and highlight what is within the control of the CDR and what's outside. The collaborative Miro board will remain editable and available for input from participants after the meeting.

ACTION: The DSB will provide an updated diagram to the group for input prior to the next meeting

Meeting Schedule

The Chair noted the next meeting is scheduled for Thursday 13 June 2024.

Any Other Business

No further business was raised.

Closing and Next Steps

The Chair noted that the focus for next meeting will be to review the threat model and prioritisation.

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

Meeting closed at 11:59