Data Standards Body

Information Security (InfoSec) Consultative Group

Minutes of the Meeting

Date: *Wednesday 13 June 2024*

Location: *Held remotely, via MS Teams*

Time: *10:00 to 12:00*

Meeting: *Meeting # 4*

Attendees

Participant Members

Mark Verstege, Chair
Jim Basey, Basiq
Sameer Bedi, NAB
Olaf Grewe, NAB
Macklin Hartley, WeMoney
Ben Kolera, Biza
Aditya Kumar, ANZ
Stuart Low, Biza
Julian Luton, CBA
Brad McCoy, Basiq
Dima Postnikov, Connect ID

Observers

Elizabeth Arnold, DSB
Nils Berge, DSB
Naomi Gilbert, DSB
Bikram Khadka, DSB
Holly McKee, DSB
Terri McLachlan, DSB
Michael Palmyre, DSB
Hemang Rathod, DSB
Christine Wiliams, DSB
Elaine Loh, OAIC
Chrisa Chan, TSY

Apologies

Darren Booth, RSM Australia
Vincent Cheen, Mastercard
Tilen Chetty, Mastercard
Nick Dawson, Frollo
Harish Krishnamurthy, ANZ
Tony Thrassis, Frollo
Mark Wallis, Skript

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 members Darren Booth (RSM Australia), Vincent Cheen (Mastercard), Tilen Chetty (Mastercard), Nick Dawson (Frollo), Harish Krishnamurthy (ANZ), Tony Thrassis (Frollo) and Mark Wallis (Skript) were apologies for the meeting.

Minutes

The Chair thanked members for their comments on the Minutes from the 29 May 2024 meeting. The Minutes were formally adopted and will be published on the Consumer Data Standards (CDS) website.

Action Items

The Chair noted the Action Items were either completed or to be addressed during the meeting.

Update on Threat Modelling

The DSB presented the draft threat model, which catalogued assets involved in the CDR ecosystem, applying their sensitivity, identifying their authority and from which source, and the threats that apply to them. The aim was to systematically start working though known documents, for example the FAPI attacker model and the UNSW Report, to identify additional threat actors and vectors. The intent is to develop a catalogue that can be maintained in public and start to apply to the architecture and work towards the controls we have in place to assess appropriateness etc.

One member asked whether the scope of the threat model was for the whole ecosystem? Previous reviews in this space focussed almost exclusively on OAuth 2.0 and specifically between the ADR and DH and excluded the Register. Adding energy will also fundamentally change this and there are a number of threats related to interaction patterns with the Register.

The DSB advised we are starting from an inside out perspective, with the direct interaction between accredited data recipient (ADR) and data holder (DH) and then the register but with the intent that it's ecosystem wide. However, some threats will sit outside of the ecosystem boundary, remit of Data Standards Chair and the functions of this Group.

One member suggested the need for clear specifications in terms of data separation on the ADR side which implies a threat of data leaking into other ADR infrastructure, questioning whether this falls outside of the scope of this consultative group?

The DSB noted there are some standards the Data Standards Chair can make in regard to ADRs, albeit they are quite limited. This groups' scope is not to define or look at internal infrastructure of a DH for example as that would need to come under their obligations.

The DSB noted the entities will be fleshed out and participants or actors etc under the Rules added to represent at a high-level view in the next version of the threat model for further discussion.

ACTION: DSB to include entities under the Rules in the updated Threat Model for further discussion.

One member noted, in terms of threat scenarios, threat actors and threat scenario related coverage could further enhance the threat modelling and that mapping could play out meaningfully from a security context.

One member noted the focus at this stage is around the data or the information exchange and the data in transit. They suggest this can be extended and improved if the controls for the data at rest and once it is relinquished then how is the protected down in the chain.

The Chair noted this will be a standing agenda item. Moving forward they will look at representing the rest of the participants and entities that sit within the Rules and they will continue to add to the data sets.

Update on Design Principles

The DSB sought feedback on the revised Problem Definition Statements as follows:

1. Problem Definition Statement # 2: How might we determine if there are any discreet wording changes to the baseline security provisions that permit DHs to implement app2app or equivalent authentication methods in lieu of the one-time password requirement?

   Feedback received:

   - Are we declaring A2A the winner off the bat here?
   - X2app flow changes wouldn't be minimum for Energy DHs
   - [DSB] Decoupled authentication flows also need to be considered
   - Really uncomfortable with A2A being prescribed as problem definition. What's wrong with a web redirect flow with a push notification a banks app being in scope?

   A member noted that A2A in the energy sector will require a massive amount of change as no energy company is doing A2A.

   The DSB agrees that A2A will not be enforced on DHs, and they see decoupled as on the priority list which could potentially be another focus problem statement that they are solving for.

   One member suggested that we design the target framework and not prescribe one of the other (A2A / decoupled) but prescribe it in a conditional way.

The DSB sought any additional feedback on the Design Principles:

1. Principle 1: Data Holders authenticate consumers: In order to verify the consumer before disclosing data, it is the DHs responsibility to authenticate the customer in accordance with CDR rules and standards.

   Feedback received

   - Design principles limited to authentication. A bit unsure about the word 'verify' in here.

2. 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 received

- ‘Authentication controls’ seems to almost be a reference to authorisation – I’m not sure how to fix this.
- available authentication controls should cover the identified use cases and relative sensitivity of the action being initiated or the data being disclosed.

3. 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 received

   - At least 1 method?

4. Principle 6: Authentication is familiar: DH should utilise authentication methods that is consistent and already familiar to customers on a channel they interact on.

   Feedback received

   - This really forces the definition of ‘consistent’
   - ‘consistent’ across digital channels’
   - What about offline users? Nothing is familiar in this situation

5. Principle 8: No degradation of experience: There should be no unreasonable friction that impacts consumer outcomes or creates lower conversion of consumer outcomes compared to CDRs OTP authentication flow today.

   Feedback received

   - The conversion rate baseline will be either aspirational or hard to govern unless we do mandate mechanisms such as usability label testing and open result sets
   - Agree. ‘Conversion rate’ is commercially loaded. Disagree with the inclusion of this
   - I think it should stay even if it acknowledges to be aspirational. Please do not simply remove it.

The DSB categorised the feedback received at the last meeting into themes including ‘authentication and consistency’’, ‘conversation rate and degradation of experience’, ‘x2app as option’, ‘Principle vs prescription’, ‘Risk and Security’ and ‘innovation goes both ways’.

The DSB will take the additional feedback into consideration and incorporate into the Problem Definition Statement.

ACTION: DSB to implement the feedback and update the principles and definitions.

Enabling x2App and group activity

Overview of staged approach

The DSB noted that in the meeting held on 29 May, members discussed a two-phase approach to authentication uplift. Firstly, to consider changes that would allow DHs to implement x2App authentication flows by lifting the ceiling. This was the premise behind Problem Definition Statement # 2. And secondly, to consider changes to raise the floor (minimum bar for authentication).

The DSB suggested a staged approach as follows:

- Stage 1: Lift the ceiling and allow x2App with least amount of change
- Stage 2: Access data sensitivity framework and risk-based data disclosure levels
- Stage 3: Support decoupled authentication as an additional authentication flow
- Stage 4: Improve the minimum baseline (floor) for authentication which includes uplift to the Redirect with OTP flow and considerations regarding and email OTP.

The DSB provided a summary of the key stages of uplift and what they are focusing on at each stage. They sought feedback from the group on how they might consult for example, on each individual stage or as a package.

The DSB also sought feedback on the unresolved design considerations:

1. Under what scenarios is x2App required to be supported by DHs? See UK OB requirements (Stage1)
2. What CX guidelines or standards should apply for 2xApp authentication flows? (Stage 1)
3. What CX guidelines or standards should apply for different authenticators (other than OTP)? (Stage 1)
4. What is appropriate framework for mapping data sensitivity to TDIF Credential Level that will help cover authentication requirements (Stage 2).

One member noted on the banking sector DH side, we're already regulated with respect to how we identity customers (AML/CTF etc) but if a DH was forced to reidentify all their customers on the identity side as a result of a regulation change in CDR that would be a concern.

The DSB reiterated there is no suggestion of changing or imposing any sort of requirements around identity proofing levels on sectors. It is important not to create unnecessary conflict with requirements or obligations that DH currently have.

The member noted in the context of ConnectID, they have done analysis to see what the alignment is between the regulations and how they have implemented those and the gap from TDIF identity assurance levels. They volunteered to bring this back to the group at the next meeting.

ACTION: Member to share their analysis of the alignment between the current regulations and TDIF identity assurance levels at next meeting.

Group Activity

The DSB proposed the following to the group to address in a breakout session:

1. Levels of Assurance (LoAs): Current LoAs support TDIF Credential Level 1 (CL1) or above authenticators. Without limitation to SF OTP, DHs have permissibility to support CL1, CL2 and CL3 authentication. Define an LoA4 that maps to CL3.
2. Authentication standards: Changes to the standards are required. Add standards to allow x2App. Caveat that OTP requirements are only applicable where SF or MF OTP are used as authenticators. Password (memorised secrets) are still excluded.

3. Baseline Security Provisions: Changes to the standards are required. Add conditional statement that the OTP requirements ONLY apply where SF/MF OTP is used as an authenticator. Otherwise permit x2App with fallback to authenticator selection within TDIP CLs
4. Metrics: Change to the standards MAY require metrics currently require recording of abandonment as customer ID and OTP. Requires further guidance where other authenticators are used.

Feedback was provided as follows:

CX Changes

- In an x2app scenario is there a space for streamlined approval? At a minimum the number of screens decreases as 'auth' is done implicitly?
- Any considerations/weirdness for x2App where there are multiple consumer profiles in the same app?
- Need to standardise on not excluding web/non mobile users (i.e. have web2app flows required, web fallback if there is no app, etc)
- Permission to introduce an app for CDR purposes?
- Definition of App. Considering many DH CDR solutions will have no current connection to an App. It is acceptable for a DH CDR app to be created as opposed to using their existing App (noting some DHs may already have several apps and some may have none)
- This also raised the question of a centralised CDR App?
- How do we support multiple apps that service different customer profiles?

Security Changes

- Should passwords still be excluded if we are aligning?
- Would enabling memorised secret such as password open door for security attacks e.g. phishing attack
- Why do we need conditional statements on OTP when referencing TDIP?
- Is there a requirement to consider alternate authorise URL support for web vs. mobile
- Is ACR still alive? I have a vague recollection it has been superseded

Non-functional requirements

- Baseline conversion rates with OTP

Additional considerations

- What about CTS updates?
- If we are moving authentication to app, should we also move authorisation?

Meeting Schedule

The Chair noted the next meeting is scheduled for Wednesday 26 June 2024.

Any Other Business

No further business was raised.

Closing and Next Steps

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

Meeting closed at 11:59