Skript

Feedback on CDR Decision Proposal 327 - Authentication Uplift Phase 1

15 Nov 2023

Generally speaking, Skript is very supportive of the authentication uplift proposals. We consider the benefits to Australian consumers will be improved security controls and more intuitive and reliable user experiences while authenticating with a Data Holder (DH). As noted in the decision proposal paper, the UK's experience showed that the x2App interaction flow produced the best conversion rates, and we agree that this would be a significant improvement to the CDR authentication flows. We also acknowledge that allowing, and to some level requiring that DHs use stronger levels of assurance when authenticating consumers aligns with specific recommendations into the CDR as well as industry best practices.

That being said, we see two risks of introducing more flexibility and stronger authentication requirements to the CDR, each explored below.

1. **Additional friction to the consumer experience**

Our strong recommendation is that any authentication methods a DH chooses to implement and require of its customers **cannot introduce more friction** to the overall consent process. It has become widely acknowledged in the industry that the consent process is already too cumbersome, and introducing additional friction could be detrimental to the mass adoption of CDR in Australia. Specifically, we caution against the use of:

- Separate authenticator apps that a consumer must download or register with, just so they can grant a CDR consent
- Requiring a consumer to establish a CDR-specific pin or password that is separate to their general dealings with a DH
- Significantly deviating from or stepping up authentication requirements for CDR compared to other digital channels for each DH

Authentication should ideally align with models used by a DH already, to increase familiarity and trust when a consumer is attempting to grant a CDR consent. This should also theoretically minimise implementation and maintenance efforts for DHs, as there will be alignment with existing solutions.

2. **More things can go wrong, with no visibility for ADRs**

We are also conscious that introducing more flexibility into how each DH may choose to implement authentication will result in more ways things can go wrong during this stage of

the consent process. At the moment, Accredited Data Recipients (ADRs) have no visibility during the authentication process, so can't help consumers when they experience errors. While ADRs can currently apply blanket support statements relating to the existing OTP flow, variance in the authentication flows across DHs will mean ADRs will simply be able to tell a consumer to call their DH for assistance. Calling a help centre is a tedious experience at the best of times but is also not suited to complex issues like identifying where an authentication request went wrong in a particular consent.

As such, we recommend the standards are extended to support enhanced alerting / monitoring / reporting to give ADRs insights during the consent process. This could look something like the Introspection Endpoint, which allows ADRs to determine the status and expiry of Refresh Tokens. Ideally this would provide insights into the status of consumer consent, which may include states like "authentication pending", "authentication unsuccessful", "authentication timeout", etc.

This will help ADRs ensure the consumer receives the best support possible when things go wrong, and ultimately increase the conversion rates of successfully granted consents.

Responses to specific consultation questions

7. Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?

Before SMS-based OTP delivery is restricted, there must be confidence that all DHs can support alternative authentication models that do not impose unreasonable friction to the consumer. Our view is that this is currently not possible, particularly where alternative authenticators are not broadly used by a DH, and therefore requires further consultation.

9. Should the Redirect with OTP flow require a second factor of authentication, including for offline customers?
An example may be introducing an additional PIN code secret that is established for CDR data sharing purposes.

Skript strongly advises against requiring additional PIN code secrets to be established specifically for CDR data sharing purposes. Granting a CDR consent is not a regular enough occurrence for a consumer to reasonably remember the context and value of a PIN they set up. We foresee that this would become a significant blocker to mass adoption of CDR in Australia.

10. Should OTPs be only delivered to a channel the customer has already established to receive authentication secrets?

This would be ideal, however may not always be practical depending on the nature of a consumer's relationship with a DH.

11. Is it reasonable to require Data Holders to support preferred interaction flows, such as x2App, where the Data Holder is dealing with an online customer who has the DH app installed?

Yes, Skript sees a lot of value in the DSB determining the preferred interaction flow based on CX research and learnings from other regions who have undergone similar open banking or open data regimes. The more consistent the experience for consumers across the board, the more reliable and trustworthy the CDR becomes.

The banking sector has also demonstrated through industry-driven initiatives involving somewhat comparable consent flows that the x2App flow is both preferred for UX purposes and feasible to implement.

There may be scenarios where a DH deems a consumer is not well suited for the x2App flow, even if they do have the DH app installed on their device, although we view this more as an exception scenario than the majority.

16. Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?

Yes, and this would require more detailed discussion, potentially as part of the NFR working group proposed under NP 335.