Decision Proposal 327 - Authentication Uplift Phase 1 · Issue #327 · ConsumerDataStandardsAustralia/standards (github.com)

General Feedback

A note on the process for standards making.

We strongly recommend that the proposed changes to the standards changes are drafted and then presented as a standards candidate for review by all participants for at least 30 days before they are considered ready for presentation to the Data Standards Chair.

A review by participants of the details of the actual changes to the standards provide opportunity to remove ambiguities, and seek clarification on details before delivery commences, to avoid the urgent MI changes, Zendesk clarifications, and implementation issues that have occurred with previous decision proposals.

The introduction of Authentication Rules

We strongly recommend that the DSB does not define any standards that constrain or define authentication mechanisms employed by participants. Instead, we recommend that a principles-based authentication framework is introduced into the Rules, requiring ALL participants employ a best practice authentication capability, that appropriately balances the requirement for good friction with a seamless experience.

Given current levels of CDR usage and the rapid advancement of authentication and cyber security technologies, standardization of authentication within the CDR is unlikely to deliver any additional protection to consumers. The authentication technologies and techniques employed by participants varies greatly and have been developed to meet the needs of their consumers and the nature of the services that they offer. Participants are best placed to identify what is best practice, and what is good and bad friction, and the burden of compliance will likely hold back an organisation’s ability to strengthen their digital channels to best meet their customer’s needs.

The use of TDIF

A broader use of TDIF in the Standards has the potential to bring negative outcomes on data holders either through an increase of the compliance burden of an organisation to comply with it, the potential to complicate a participants ability to satisfy terms of cyber-insurance policies, and given the wording and purpose of TDIF (for the application of accreditation into a digital identity scheme) potentially complicate its ability to effectively regulate participants.

We acknowledge that the standards already refer to LoA within TDIF, however, we recommend that this reference be removed, and if required replaced with a reference to Authenticator Assurance Levels.

Looking to the future.

Whilst we strongly discourage the reference or alignment of standards with TDIF, we do acknowledge the requirement to align CDR authentication rules with future rules created to support participation in the government’s digital identity scheme. We encourage the CDR and DigiID schemes to work closely to align on a principles-based set of rules for authentication, that allows participants to maintain best practice when authenticating their customers, while also enabling the contestability outcomes and success of the scheme.

Reponses to Questions

1. Are there any reasons, or scenarios, when MFA must be required?

We do not recommend that any standards are made for the CDR that requires MFA to meet any specific reason or scenario. We agree that there should be a framework that requires strong authentication and believe that framework be able to defer to non-CDR practices or standards. The framework could be in the form of Rules and could simply provide guardrails to ensure that best practice in the application of authentication controls.

2. Should the Data Standards Retain reference to TDIF credential levels or consider aligning to NIST Authentication Assurance Levels?

If authentication standards are deemed appropriate, they should refer to or align with NIST 800-63B.

TDIF is specifically written to enable the accreditation of an organization within Australia's Trusted Digital Identity scheme. References to a document intended for accreditation of Identity based within the governments Trusted Digital Identity Framework will only introduce complexity and ambiguity into the standards and complicate any compliance and assessment activities needed to be performed by the participant and ACCC. The Authentication Assurance Levels defined in Section 4 of NIST 800-63B are specific to Authentication requirements and do not incorporate the aspect of identity proving, so fit for the purpose of the CDR.

The inclusion of Table 4 in DP327 into the CDR standards would only introduce complexity and ambiguity, as the CDR rules hold no reference to identity proofing or other aspects addressed within TDIF.

3. Where retention of TDIF is supported, are there any clauses in the TDIF role requirements that should not or must not apply to the data standards?

We do not support the retention of any part of TDIF.

4. Are there any specific accessibility requirement that should be considered in addition to the success criteria 3.3.8 and 3.3.9 of the WACG 2.2?

Westpac supports all efforts to make CDR accessible to all and encourage the inclusion of these standards into the CDR and made applicable to all participants of the CDR.

As these standards are new, the technology requirements to fully satisfy a password-less experience are still immature, we strongly recommend that there is no compliance requirement imposed on participants relating to 3.3.8 and 3.3.9.

5. What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why?

If standards are to be made, refer to or align with NIST 800-63B.

6. Should email based OTP be classified as a Restricted Credential list in accordance with NIST guidance for either or both online and offline customers.

If standards are to be made, refer to or align with NIST 800-63B. At this stage the uptake in CDR is low, and the risk related to divergence with standards is less than the risk which might be mitigated with a divergence.

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

YES – divergence from NIST 800-63B may only complicate other the cyber controls of an organization and increase risk to offline customers.

8. How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?

This section should not be applied – this section refers to an *Applicant* of which a CDR participant is not. Any references to standards should be made to NIST 800-63B.

9. Should the Redirect with OTP flow require a second factor of authentication, including for offline customers?

There should not be any specific standard made here. Data Holders required to serve Offline consumers should follow best practice in authorizing customer access for data sharing.

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

YES, this would be considered best practice - If a channel has already been established then this should be the preference for receiving OTPs.

Existing settings-preferences must be observed, and the standards should not change the delivery preferences of the consumer, unless that preference is determined as weak or compromised (e.g. Restricted Credentials).

11. Is it reasonable to require data holders to support App2App when the Data Holder is dealing with online customers that have the DH app installed?

NO – data holders should be allowed to decide the best mechanism for authentication for their channels. Data Holders may have existing Apps but the purpose, lifecycle, technical capability and other aspects of the Data Holder App might not be the best method of authentication nor best investment for the Data Holder, to make in uplifting customer authentication.

We recommend that standards are changed to accommodate App2App, but compliance obligations to support App2App should not be imposed on Data Holders.

12. Are the dates proposed for Phase 1 achievable?

NO – the nature of the changes being proposed are not insignificant, and for many organizations will need to be coordinated with other change activities they have underway. While Westpac supports all uplifts to the security aspects of the CDR, we believe that the low uptake of the scheme, the timeframes for the readiness of legislation, rules and standards for Action Initiation, and current controls we and other organizations have around authentication (such as risk analytics and biometrics) the proposed "uplifts" would deliver less consumer value than other near-term objectives of the organization.

We recommend that any Phase 1 compliance be pushed out to November 2025; however, welcome urgency in changes which enable data holder to improve authentication flows beyond OTP.

13. Do you propose any other enhancements to the uplift of authentication for the CDR?

Changes to Rules and/or Standards should be made to require ADRs to have their authentication match that of Data Holders, to ensure that the data shared is protected by controls considered best practice for participant type and the data the participant receives.

We also recommend that the issues raised within MI 427 are considered from the lens of authentication and addressed in readiness for future decoupled authentication flows.

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

NO – Authentication techniques will very based upon industry, use case and risk. Creating NFRs may introduce negative security and fraud outcomes as participants trade-off compliance and consumer outcomes.

We also recommend Metrics V5 be abandoned as the value obtained from these measures will be significantly diminished through the introduction of either the proposed Authentication Flows or a move to a Rules-based framework.

15. Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?

We are unclear on what "other service level agreements" refers to what service level agreements are already in place.