Australian Banking Association

Decision Proposal 327 consultation

15 November 2023

Australian Banking Association

Key recommendations

The ABA welcomes the opportunity to provide input on the authentication uplift approach.

Banks, as the custodians of highly sensitive customer data, have significant experience in managing authentication control environments. As CDR specific control environments are considered, the ABA strongly advocates for authentication controls that are both commensurate to risk, and aligned to existing industry regulatory models, practices, and customer experiences.

1. Requirement setting should prioritise alignment with principles-based standards to limit conflict between regulatory requirements and compliance complexity.

Banks already operate within a tightly regulated environment with respect to customer on-boarding and ongoing authentication. Generally, regulation emphasises an outcome driven, principles-based approach, which enables banks to manage customer safety and security in a way that they determine is appropriate and congruent to their customers, business model, and digital channels.

The ABA recognises the importance of robust authentication under CDR, ensuring customers have confidence to share their data. We are concerned however the proposed changes to the CDR Data Standards represents a pivot from the current regulatory model to a prescriptive approach. This approach establishes bespoke authentication requirements, introducing significant additional complexity from overlap between existing standards and authentication standards.

Of particular concern is the risk that establishing situational and prescriptive requirements will lead to parallel authentication standards – one for CDR and another for banking. In a practical sense, as banks already facilitate high-risk activities, e.g., payments and transfers, separate CDR requirements could lead to a situation where higher standards of compliance are applied to relatively lower risk activities.

We therefore believe that the focus of this Decision Proposal should be on authentication credential levels, with specific requirements being guided by common standards and deference given where possible to a data holder's existing controls. We strongly caution against incorporation of standards that go beyond authentication, e.g., identification proofing, as this represents both an encroachment into the scope of the CDR, and a fundamental divergence from its overall intent.

2. We oppose mandating consistent interaction experiences as they will entrench unfamiliar, disjointed journeys into digital experiences that customers are already familiar with.

The ABA endorses efforts to make consent sharing as simple and frictionless as possible for customers. We do not believe this would be achieved through bank agnostic, industry consistent experiences, and oppose a pivot towards mandating these.

Banks provide innovative customer centric digital experiences that are constantly enhanced for functionality, consistency, and accessibility. As the digital anchor for an individual's financial affairs, these experiences are familiar to customers and intuitive to navigate.

Attempts to produce an industry consistent experience would introduce an unfamiliar experience to customers, a departure from the app/website they engage with regularly, without the look and feel they expect from their bank. We are concerned that this disjointed experience would be jarring for many customers, and counterproductively may diminish ease and trust in the consent process.

Australian Banking Association

Consultation questions

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

Banks already securely facilitate authentication at scale. The current regulatory model allows for variety in processes and authenticator types to be used, reflecting diversity in the industry's digital platforms, technology stacks, and customer experiences. Directives to deploy specific authenticator types should be informed by existing models of industry regulation, and reference to commonly accepted standards.

Where there is existing regulation specific to authentication, we believe deference should be given to it where possible. Specifically for multi-factor authentication, we note that APRA has provided guidance for MFA application under CPS 234 and CPG 234, requiring adoption of strengthened authentication controls for high-risk activities (e.g. third party funds transfer). Determination of authentication controls for CDR should follow this model with the appropriate level of assurance required first assessed, with specific controls informed by existing models for standard setting.

While the ABA does not advocate for a specific set of standards, we see a compelling rationale for convergence upon principles-based standards. Using NIST 800-63B as a reference point for illustrative purposes, an appropriate level of assurance could be determined (e.g., AAL2 – a high degree of confidence), which would provide both flexible and repeatable guidance on how the required assurance could be obtained. Under an AAL2 scenario, data holders would have the option to deploy MFA, but also could achieve the same level of confidence through a combination of other authenticator types.

We believe this approach would both ensure CDR authentication standards are not delineating from other instances of assurance, while preserving the ability for data holders to tailor their authentication processes to the specific needs of their customers (e.g., non-digital customers).

2. Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?

While we recognise that TDIF Credential Levels provide guidance for authentication, the specific intent and purpose of TDIF is to provide accreditation of organisations within a Trusted Digital Identity scheme.

Fundamentally, the CDR is about a consumer's right to move their data from one organization to another – it is not about demonstrating ownership of that data to another organisation. Given that the strength of identity proofing is outside the scope of the CDR, we are concerned that reference to TDIF will introduce substantial complexity and ambiguity into the standards and complicate compliance and assessment activities performed by the participant and the ACCC. Such complication could additionally lead to disjointed customer experiences, such as forcing data holders to re-identify existing customers before they use CDR, embedding more friction than they are used to, disincentivising engagement with the CDR.

Reference to TDIF Credential Levels as they pertain to authentication solely is reasonable, however this is predicated on the extent to which the authentication specific TDIF standards can be genuinely isolated from the remaining standards. We do not believe this isolation is in practice always guaranteed, presenting an ongoing risk of conflicting standards. As our preference is for delineated, authentication specific standards, NIST would be more appropriate for alignment to.

Australian Banking Association

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?

See response to Question 2 in reference to TDIF.

TDIF provides accreditation standards specifically related to identity proofing, which is out of the scope of the CDR. On this basis, and reflecting the positions expressed in Questions 1 and 2, the role requirements should not be incorporated into the Data Standards.

We are concerned that the explicit intent of TDIF role requirements to *"supplement existing obligations and apply specifically to Identity services that undergo the TDIF Accreditation Process"* leads to inadequate generalisation. This presents difficulty in isolating the authentication specific standards, introducing regulatory ambiguity and complexity.

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 WCAG 2.2?

The ABA supports accessibility in financial services and the incorporation of accessible design standards into the CDR. Password-less experiences are an important inclusion in accessibility, however given their relative nascence we urge careful evaluation of their reliability and consistency in providing secure authentication prior to imposing compliance requirements 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?

In principle we believe that inclusion or exclusion of specific authenticators or authentication channels should be guided by reference to existing appropriate standards and regulation. We are concerned that adopting a prescriptive approach to specific authentication types and channels would create conflict with existing standards and increase compliance complexity as existing standards become less applicable. With significant variance in how data holders currently authenticate their customers, prescriptive authentication requirements could unevenly impact certain banks which otherwise authenticate according to the current standards.

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

Requirements pertaining to the classification of specific credentials should reflect consideration of the following principles.

- In general, consent flows should where reasonable avoid embedding new risks. Consent flows via more secure credentials i.e., x to app, are desirable and should be encouraged. This reflects our acknowledgement that less secure flows risk exposing customers to new risks – e.g., consent flows via web page redirect could expose customers to new phishing risks.
- Consideration should be given to the trade-offs associated with restriction of OTP delivery, which may lead to non-digital, non-app customers being excluded from the CDR. Where exclusion concerns exist, we encourage discussions on pragmatic workarounds that

mitigate security risks while maximising access (e.g., utilising OTP authentication for read only consent).

- Regulatory simplicity is always preferable. Alignment to principles-based standards like NIST provides clarity in compliance requirements, however we would encourage alignment to be considered holistically rather than on an ad hoc basis.

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

See response to Question 6.

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

TDIF is not designed specifically for authentication. Section 4.3.9 references an 'applicant', something that a CDR participant is not. Data Standards should ensure consistency and clarity in terminology, and where roles are ascribed, they are fit for purpose.

We believe alignment to an authentication specific standard should be encouraged to ensure terminology reflects the implementation environment. For example, NIST 800-63B refers to Restricted Authenticators in 5.2.10 and refers to "organisations" - as reference to the organisation that is subject to the standard.

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.

The creation of specific standards should be avoided where possible to limit the introduction of regulatory complexity. We would prefer that an assurance level requirement was determined (e.g., CL or AAL), with the data holder required to adhere to the authentication requirements for that level.

Specifically, to the example given, we would encourage assessment of the proposed security benefits that a second factor of authentication (a PIN) would deliver against the potential burden this could place on customers, especially in the context of other security uplifts. E.g., if OTPs were retained for non-digital customers, the requirement of memorising a PIN secret where they have not been required to before, may disincentivise participation.

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

Generally, yes. Where an existing channel is already established, the preference should be for OTPs to be received via this channel. Standards should not for change the delivery preferences of the consumer, unless that preference is determined as weak or compromised (e.g., Restricted Credentials), which would require a new CDR compliant channel to be established.

Australian Banking Association

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?

Banks already have robust, risk-based controls in place to protect their customers when engaging with a bank's digital channels. Reflecting this significant expertise and experience, we believe Data Holders should be given some discretion to determine the best authentication method, in line with data standards.

While we acknowledge the security rationale supporting more secure interaction flows such as x2App vs other methods, we are concerned this mandate could introduce new risks. Responding to current cybersecurity threats and emerging attack vectors may require banks to modify their control environment rapidly. We believe imposing arbitrary standards on interaction flows could inhibit a bank's ability to respond in such a crisis. We are also concerned that the above issues may disproportionately burden smaller banks, that often have less resources at their disposal.

Notwithstanding these concerns, were this to be required, the proposed decision flow in figure 2 is reasonable on the assumption that the fall back to an OTP web redirect addresses potential risks (e.g., by supporting read only consent flows). We reiterate our belief that a principles-based approach that allows banks to determine their authentication types – in reference to a standard – is preferred.

12. Are the dates proposed for Phase 1 achievable?

We do not believe the dates proposed for Phase 1 are achievable. The nature of changes being considered are not insignificant and will require extensive planning by organisation to integrate the workflow with their other change activities. We are unable to propose with confidence an alternative date, as the implementation timeframe estimate will need review based on the finalised Phase 1 scope, and implementation commencement is dependent on final endorsement.

Indicatively, we believe that 12 – 18months implementation time will be required. This would suggest a revised completion date of November 2025 would be feasible, assuming there are no material changes in scope and endorsement is granted comfortably in the first half of 2024.

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

Uplifts to authentication standards should promote alignment with existing industry regulation and principles-based standards.

Compliance requirements should be informed by both a determination of the level of assurance necessary, and the acceptable methods to obtain that assurance under an authentication specific standard. In principle, data holders that meet or exceed the required assurance standard through other controls should automatically meet this requirement for ADR Accreditation.

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

Consideration of performance requirements should be undertaken in a separate consultation. As the number of CDR participants expands, this represents a large and diverse set of authentication permutations. We urge that detailed consultation on performance requirements is undertaken to determine what is reasonable, safe, and drives a meaningful uplift in user experience.

While CDR uptake is limited, we believe core functionality and security should remain the priority. In this nascent environment, some authentication friction is beneficial insofar that it promotes security, which could conflict with performance requirements.

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

Further consultation on service level agreements should be considered to assess the extent to which they are driving meaningful benefit to the CDR as it stands currently.