Data Standards Body

Consumer Experience and Technical Working Groups

Decision Proposal 327: Authentication Uplift Approach

Contact: Bikram Khadka, Holly McKee, Mark Verstege, Michael Palmyre

Publish Date: 25 September 2023

Correction Date: 3 October 2023

Feedback Deadline: 24 October 2023

1. Table of Contents

2. Introduction

This decision proposal relates to the Consumer Data Right (CDR) authentication standards and how they might be uplifted. The prior decision, made in 2019, was for a single interaction flow utilising a standalone authentication method, called the 'Redirect with One Time Password' (OTP) flow. No other flows are currently allowed.

Offline customers

Offline customers are out of scope for this decision proposal. A security risk-assessment for offline customers is being considered to assess best practice security for that modality.

Summary of key recommendations

This decision proposal recommends:

- Phasing authentication uplift with the first phase aligning to the NBL implementation
- Introducing a Level of Assurance LoA4 that maps to the TDIF Credential Level (CL) CL3
- Allow Data Holders to support strong customer authentication methods permitted by CL3 with an exclusions list of authenticators that do not meet best practice security
- Recommend Data Holders support at least LoA3 for read access commensurate to existing digital channels
- Allow Data Holders to support MFA provided it aligns to their existing digital channels
- Where OTPs are supported, uplift the controls in line with the Independent Health Check Report
- Support App2App/Web2App as the preferred interaction flows for online customers
- Require certain interaction flows, such as App2App, if supported by the DH to enhance the CDR CX
- Retain LoA2 for offline customers only, until an offline customer security risk assessment has been conducted

These recommendations will increase flexibility for Data Holders, reduce compliance costs, and will improve both security and consumer experiences.

Summary of expected outcomes

If the recommendations are adopted, the most likely outcomes are expected to be as follows:

Banking sector:

- It is expected the prevailing outcome to be App2App authentication using multi-factor authentication with biometrics

Energy sector:

- If the retailer offers an app, and the consumer has online access, it is expected the prevailing outcome to mirror banking.

- If the retailer does not offer an app, or the consumer does not have online access to their account, it is expected the prevailing outcome will be retention of the web-based Redirect with OTP flow, until a dedicated security risk assessment has been conducted.

Non-Bank Lending sector:

- It is expected NBL will follow the same approach to the Banking sector.

Previous consultations and recommendations made to the Chair

Several reviews and inputs have proposed a review of CDR authentication, including:

- The Government's response to the Inquiry into Future Directions for the CDR,
- The 2022 Independent Health Check Report,
- The Data Standards Advisory Committee, including a November 2020 presentation on 'waterfall authentication',
- Community Change Requests (CR), including CR554, CR568, CR542, and CR405,
- Noting Paper 280 on the Consumer Experience (CX) of Authentication,
- Noting Paper 296 on offline customer authentication,
- CX research published and summarised in NP280,
- The Accessibility Improvement Plan,
- Internal reviews and analysis relating to security, risk, and consumer experience.

Collectively, these propose that the CDR authentication capabilities be expanded, which would necessitate an uplift to the CDR security profile and CX authentication standards. This is expected to occur in phases to prioritise higher value changes.

In addition, the Consumer Data Standards also rely upon several external standards which have seen revisions, amendments, and enhancements in the past few years, including:

- Trusted Digital Identity Framework (TDIF) revisions and updates,
- CPS/CGP 234 revisions,
- National Institute of Standards and Technology (NIST) guidelines for authentication and lifecycle management.

Purpose of this consultation

As per Rule 8.11(1)(c)(i), the Data Standards Chair has an obligation for the "authentication of CDR consumers to a standard which meets, in the opinion of the Chair, best practice security requirements".

The purpose of this consultation is to cover the high-level decisions for Phase 1 of authentication uplift. Targeted consultations on key decisions and standards changes for each separate work package will be consulted on in future change requests and Decision Proposals. These consultations will be shaped by the feedback provided to this proposal.

The overarching objective is to improve the consumer experience while maintaining strong security and offering more options for Data Holders that are supportive of a risk-based approach.

It is proposed that authentication uplift be progressed over three key phases:

Phase 1: Ready for Non-Bank Lending: providing operational improvements, security hygiene, and priority improvements to consumer experience backed up by the consumer research.

Phase 2: Enhanced Consumer Experience: providing broader channel choice appropriate to primary use cases and improvements for streamlined re-authentication.

Phase 3: Ready for Action Initiation: required strong customer authentication controls needed for Action Initiation such as step-up authentication along with more complex authentication improvements for business consumers and broad digital economy support.

3. Decision to be Made

- Determine the phasing of appropriate authentication measures that satisfy the Chair's requirements for best practice security in CDR;
- Consider appropriate obligation dates for supported option(s);
- Identify any other options to be considered.

4. Discounted Options

The DSB conducted analysis based on the reviews and inputs outlined in the beginning of this document. This work has highlighted the need to gradually pursue improvements relating to security and consumer experience. It has also ruled out certain options that the DSB is not proposing be pursued as part of authentication uplift, which are discussed further below.

4.1. No Change

This would result in CDR authentication remaining as-is. Given the risks, recommendations, and community requests highlighted in the previous section, along with the Data Standards Chair's obligation to support best practice security, the DSB has ruled out this approach.

4.2. No Framework

The initial consultation on CDR authentication in 2018-2019 considered if CDR authentication standards should defer to non-CDR Data Holder authentication approaches. This pathway was not considered appropriate, and this determination is being maintained for the purposes of this consultation.

When such an approach was taken in UK Open Banking it resulted in unnecessary friction, an inconsistent consumer experience, and higher rates of consumer drop-off during both initial authorisation and re-authorisation.

Further, deferring to external authentication approaches could undermine the obligation for the Data Standards Chair to support best practice security. The requisite level of security may not be present for all Data Holders in every current and future CDR sector.

Maintaining a high bar for CDR is an especially pertinent issue given the recent increase in high-profile data breaches. If the data standards deferred to non-CDR Data Holder authentication practices, the security and consumer experience of the CDR in general could be compromised. As such, the DSB is not considering this approach as part of authentication uplift.

4.3. Offline Customers

The CDR rules currently consider 'offline customers' to be eligible CDR consumers. Offline customers are consumers who do not have online accounts with the DH and are otherwise eligible to share CDR data.

This is only currently applicable in the energy sector but may be considered for future sectors that have similarly high numbers of offline customers. A significant proportion of energy consumers may be 'offline customers'. Based on limited data from major and non-major retailers in 2020:

- an average of 73% of SME customers were offline, which was projected to reduce to 58.5% in 2021.
- an average of 49% of residential customers were offline, which was projected to reduce to 40% in 2021.

Whilst it is likely the actual number of offline customers has further reduced in mid-2023, we expect that there remains a significant portion of energy customers who are considered 'offline customers'.

4.3.1. Issues and implications

Whilst modernising authentication is achievable for online CDR consumers, it is not achievable for offline CDR consumers. The current CDR rules may preclude the satisfactory execution of the Chair's duties when defining best practice authentication standards with regard to offline customers. The expected outcomes described above suggest offline customers could continue to authenticate in CDR in the interim, but it may not be appropriate to maintain this approach in the future due to security concerns.

If the current approach for offline customers were to be deprecated, it would mean the standards would no longer support the authentication of offline CDR consumers despite the rules considering them to be eligible CDR consumers. It would also mean that a significant portion of energy consumers, who are offline customers and can currently share CDR data, would no longer be able to share their CDR data because of this standards change.

Further, there may be implications to consider given energy retailers have implemented, or are in the process of implementing, support for offline customers, and that offline customers may in some cases represent a sizeable proportion of a retailer's customer base.

This issue was previously consulted on in March 2023 in Noting Paper 296, and is expected to be progressed further as part of the authentication uplift work. **Deprecating support for offline customers is not being proposed as part of this initial phase of authentication uplift.**

This decision proposal acknowledges the current friction between the Chair's duties to provide best practice security standards and the CDR rules requiring support of offline customers in the energy sector.

4.3.2. Current state

As noted in the Noting Paper 296 consultation on offline customer authentication, deprecating support for the Redirect with OTP flow would preclude the ability for offline customers to authenticate, which would have immediate impacts on the energy sector. Furthermore, if CL2 or above is mandated, this would prevent offline customers from authenticating to share CDR data. As a result, this would not satisfy the eligible consumer requirements in the energy sector.

Instead, the DSB proposes that improvements be made to the Redirect with OTP flow in a way that maintains support for offline customers in energy, as well as any future sectors with low levels of digital maturity, but to give preference to other authentication approaches in the standards for online customers.

4.3.3. Forward view

There are opportunities for the CDR to address this gap, which may include permitting online account registration as part of the CDR flow. However, this may require changes to the CDR Rules and could lead to a period of compromise before rules and standards could be aligned on best practice security.

Energy Data Holders, in reviewing their risk posture, may also determine it desirable to onboard their customers to be 'online customers' through processes external to the CDR. This would further reduce the cohort of offline customers in energy.

5. Identified Options – Phase 1

5.1. Levels of Assurance

The Data Standards currently state:

> *READ operations **SHALL** only be allowed where **at least** an LoA of 2 has been achieved during the establishment of consent.*

In addition, the Data Standards restrict the allowable authenticators to single-factor OTP authenticators (that is, Out-of-band Device, SF OTP Device, SF Crypto Software, or SF Crypto Device)

Whilst the Data Standards state that ***at least*** an LoA of 2 has been achieved, what this means in practice is that **only** an LoA of 2 can be achieved.

It is recommended that the Credential Level requirements be changed to CL3. To do this, the Data Standards would need to permit authenticators beyond single-factor OTP.

Option 1: No Change

This option does not define a change to Credential Level for read access. Instead, LoA 2 is retained for both online and offline customers. If this option is supported, it continues to limit the permitted authenticators to single-factor OTP authenticators within TDIF CL1.

As they are currently described, read access, regardless of sector or online customer status, would remain LoA 2 and write access LoA 3.

The DSB does not recommend this option.

Option 2: Allow LoA 2 or above for online customers

This option removes the single-factor OTP authenticator restriction. This would therefore allow Data Holders to support LoA 2 or above for read access for online customers.

What this means:

- Data Holders have more choice over which authenticators they want to support
- Data Holders can support LoA 3 or above and stop supporting LoA 2 / TDIF CL1 authenticators
- Data Holders can support CL2 and CL3 authenticators
- There is no change to the LoA statement for read access
- Multi-factor authentication is permitted
- Data Holders may support authentication methods other than OTP and the Data Holder must only use authenticators allowed by the target Credential Level
- Authenticators that ***only*** satisfy CL1 are still permitted for read access

Option 3: Require LoA 3 or above for online customers [DSB RECOMMENDED]

This option *requires* Data Holders to support LoA 3 or above for read access for online customers. In effect, it would mean only CL2 authenticators must be supported by Data Holders; and Data Holders are no longer permitted to support CL1 authenticators for online customers.

The TDIF defines a high-level risk assessment based on intended use of a digital identity. These definitions of transaction risk map Identity Proofing levels to the allowable Credential Levels. In line with these definitions, fraud of CDR data would be considered to have at least moderate risk to consumers. Therefore, supporting LoA 3 (CL 2) or above for online customers is considered both prudent and achievable. The consequence of increasing the LoA requirements for read access would be:

(a) The existing OTP requirements are insufficient to satisfy CL2 or above
(b) Data Holders should be allowed to support authenticators permitted by CL2 or CL3 as appropriate
(c) Data Holders could support multi-factor authentication as defined by CL2 or CL3 requirements as appropriate
(d) Biometrics (for authentication use) should be allowed

Table 1: Identity Proofing Levels

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Intended use:	For very low-risk transactions where no verification of identity is required, but the parties desire a continuing conversation	For low-risk transactions or services where fraud will have minor consequences for the service or *User*	For moderate-risk transactions or services where fraud will have moderate consequences for the service or *User*	For moderate to high-risk transactions or services where fraud will have moderate to high consequences for the service or *User*	For high-risk transactions or services where fraud will have high consequences for the service or *User*	For very high-risk transactions or services where major consequences arise from fraudulent verifications.
Approved technical *Credential* bindings	CL1/CL2/CL3	CL1/CL2/CL3	CL2/CL3	CL2/CL3	CL2/CL3	CL3

Figure 1 Identity proofing risk mapping to Credential Levels; Digital Transformation Agency - TDIF 05 Role Requirements

What this means:

- The levels of assurance for read access would be:
  *For online customers, READ operations **SHALL** only be allowed where **at least** an LoA of 3 has been achieved during the establishment of consent.*
- Data Holders must support at least one valid authenticator under CL2 or above
- Data Holders may support more than one valid authenticator under CL2 if LoA 3 is chosen, or more than one valid authenticator under CL3 if LoA 4 is chosen by the Data Holder
- Multi-factor authentication is permitted
- Data Holders may support authentication methods other than OTP and the Data Holder must only use authenticators allowed by the target Credential Level

5.1.1. Further proposals being made

The following enhancements are proposed:

- Introduce a Level of Assurance LoA 4 represented by the URI: urn:cds.au:cdr:4 where authenticators used to attain this level **MUST** conform with the TDIF Credential Level CL3

If Option 2 or 3 is supported, the following enhancements are proposed:

- The Data Standards state support for Biometrics (for authentication use) is allowed in accordance with TDIF section 4.3.3
- Data Holders may only support authenticators commensurate to their existing digital channels to ensure there is consistency across channels and customers are already enrolled for the Data Holder's preferred authenticators
- Data Holders may offer the consumer choice of their preferred authenticator if the Data Holder supports more than one authenticator
- An additional statement would be added to limit an LoA 2 for offline customers

Multi-factor authentication considerations

If either Option 2 or 3 is supported, the following considerations may be relevant.

Where MFA is supported by the Data Holder, there are different options in how MFA could be deployed. A Data Holder may require all consumers to use MFA or they may offer the consumer choice to enrol for MFA. If Data Holders require MFA, then it would be critical there are consumer friendly enrolment options that are accessible and commonly offered across the Data Holder's existing digital channels. If a Data Holder offers the consumer choice, then allowing consumers to opt-in or set a universal requirement for establishing data sharing authorisations may be offered via their CDR dashboard or security settings.

This would be aligned to how many Data Holder's present authentication controls today across their existing digital channels. It would also allow Data Holders to offer a parity experience in the CDR.

Where Data Holders require MFA for online customers to access consumer data they may still permit fallback to single factor authentication such as OTP. In accordance with the ACSC's ISM guidelines:

> *When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead (ISM-0417)*

Depending on consultation feedback, further options could be developed could be strengthened with appropriate SHOULD/RECOMMEND clauses for MFA support, guidelines that consider digital registration for offline customers, and minimum single-factor authentication requirements.

5.1.2. Associated Change Requests

Change Request 405: Alternative mechanisms for OTP

(DSB Item - Consider alternative mechanisms for OTP)

This change request proposes changes to allow alternative OTP authentication approaches beyond the user directly entering an OTP code into their authentication device for validation.

Change Request 542: SSO as an alternate authentication method

This change request proposes changes to allow an authentication method other than OTP specifically the Single Sign On (SSO) as an alternate authentication method.

> **Proposal:** These change requests are dealt with through Option 2 or Option 3 being supported for alternative authentication methods. These are further supported by **5.4 X2App (Web2App and App2App) Interaction Flows** to allow alternative interaction flows. Support for Business SSO has been tabled for phase 3 of the authentication uplift work.

5.1.3. 2022 Independent Health Check Recommendations

Recommendation 4: Credential Level Normative References

This recommendation considered adoption of NIST Authentication Assurance Levels and authenticator standards instead of TDIF Credential Levels and role requirements. The decision made by the Chair was to retain TDIF Credential Levels with relevant reference to NIST when needed.

> **Proposal:** Retain TDIF Credential Levels for national authentication standards cohesion.

Recommendation 10: Permit Strong Authentication

This recommendation considers improving the security posture of the Data Standards by enabling stronger, more secure, methods of authentication rather than OTP which is the only authentication method currently permitted by the Data Standards.

> **Proposal:** Permit authentication methods that are defined by TDIF Credential Levels in accordance with Option 3.

Recommendation 12: Require Credential Level 2

This recommendation considered adopting Credential Level 2 as the baseline authentication assurance level. Rather than CL1, all data sharing would require CL2 unless an industry-wide exception was necessary.

However, a blanket default of CL2 is not possible because the eligibility rules for consumers in Energy requires support for consumers that do not have online access to their accounts.

> **Proposal:** Permit CL2 in accordance with Option 3.

Consultation questions

1. Are there any reasons, or scenarios, when MFA ***must*** be required?
2. Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?
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?
4. Are there any specific accessibility requirements that should be considered in addition to the success criteria 3.3.8 and 3.3.9 of the WCAG 2.2?

5.2. Restricted Credentials

Currently, the Data Standards do not allow passwords—one instance of a Memorised Secret[1]—to be presented in the authentication flow and further, Data Holders must not include forgotten details links in redirect screens.

[1] Refer to section 5.1.1. Memorized Secrets, (NIST SP 800-63b Digital Identity Guidelines: Authentication & Lifecycle Management)

5.2.1. Constraining supported authenticator channels and delivery methods

With the uplift to authentication method support, it is important to also consider which authentication methods or authenticator channels should be *disallowed* from use either in an online customer context, or across both online and offline customers. In NIST's recent updated draft guidance, email joins voice-over-internet protocol (VoIP) on the list of delivery channels that are not allowed because they are not considered to be safe out-of-band (OOB) authenticator channels that can sufficiently prove a user's possession of a specific device.

NIST also requires[2] that authenticators make sure the user's telephone number is associated with a specific physical device that has been pre-registered for authenticator use when SMS (or voice) 2FA is used. NIST further recommends that verifiers watch for events such as "device [swapping], SIM change, number porting, or other abnormal behaviour before using the PSTN[3] to deliver an out-of-band authentication secret" because these activities could indicate a compromised channel.

The ability to intercept email or SMS is greater than other authentication channels. Given this reason, even when used in a multi-factor setting the Australian Cyber Security Centre (ACSC)'s Information Security Manual (ISM) recommends "...authentication factors that involve something a user has should be used with something users know"[4].

Furthermore, the ISM states that because messaging services like SMS "do not sufficiently encrypt data in transit, they cannot be relied upon for the communication of sensitive or classified data".

In addition to these considerations, the ACSC's ISM recommends that organisations should implement multi-factor authentication whilst NIST mandates the use of multi-factor authentication where personally identifiable information is shared.

TDIF allows authentication providers to support what it defines as "Restricted Credentials" which are defined as representing an unacceptable risk to any party. If an authentication provider chooses to support the use of a *Restricted Credential*, it *MUST*[5]:

1. *Offer Individuals at least one alternate Credential that is not restricted and can be used to authenticate at the required CL*
2. *Provide meaningful notice to Individuals regarding the security risks of the Restricted Credential and availability of alternative(s) that are not restricted*
3. *Address any additional risk to Individuals in its security Risk Assessment*
4. *Develop a migration plan for the possibility that the Restricted Credential is no longer acceptable at some point in the future.*

[2] See section 5.1.3.3, (NIST SP 800-63b Digital Identity Guidelines: Authentication & Lifecycle Management)
[3] PSTN stands for Public Switched Telephone Network, a network of telephone systems
[4] ACSC Information Security Manual; https://www.cyber.gov.au/sites/default/files/2023-06/Information%20Security%20Manual%20%28June%202023%29.pdf
[5] 4.3.9 Restricted Credentials, **TDIF Req:** CSP-04-03-10

5.2.2. Options for consideration

The following decision proposal options are considered for feedback.

Option 1: Allow Data Holders to support any suitable authenticator defined by TDIF (no restrictions)

This option places no restrictions on the allowable authenticators within a Credential Level.

This option may result in inconsistent implementation across Data Holders and would limit the Data Standards from limiting the use of authenticators that pose unacceptable risk to consumers and the CDR.

Option 2: Data Standards define an exclusion list of Restricted Credentials [DSB RECOMMENDED]

This option would continue to align with Credential Levels set out in the TDIF Role Requirements however the Data Standards would further disallow specific authentication methods such as passwords from use in the CDR, or, if necessary, allow their use only in specifically defined circumstances.

The DSB is minded to this position because it maintains alignment with existing Commonwealth guidance for Credential Levels whilst best satisfying recent external report recommendations made to the Data Standards Chair. This option is not envisaged to significantly constrain the authentication methods, but it may better support the Chair's decision when selecting which methods are appropriate and, where applicable, how those authentication methods should be selected.

Option 3: Data Standards define an "allowed list" of authentication methods

Under this option, only the authentication methods defined to be permitted in the Data Standards would be allowed. This would be an extension of how the current Security Profile treats authenticators by only allowing single-factor OTP authentications. The Data Standards, through consultation may expand the list of allowed authenticators but Data Holders would not be allowed to support any authenticators that the Data Standards to not explicitly allow.

One benefit of this option is that there could be greater consistency in consumer experience across Data holders.

This option would continue to align with Credential Levels set out in the TDIF Role Requirements however the Data Standards would further prescribe which authentication methods within each Credential Level are permitted.

One downside of this option is that enhancements inline with industry trends may be slower to introduce into the Data Standards.

Option 4: Data Standards define a "prescribed list" of authentication methods

This option would introduce mandatory support for a core set of authentication methods. This option would ensure there is consistency of experience across all Data Holders by requiring every Data Holder to support all required authenticators defined in the Data Standards. Whilst this offers a better consumer experience that achieves a high level of security, the drawback is that some Data Holders would be required to support authentication methods they don't currently support, which could result in higher implementation costs for some Data Holders. Equally, it may not be achievable for all Data

Holders if they do not offer the appropriate digital experience (for example, offering biometric authentication may not be possible if the Data Holder only offers a web-based experience.

—

Regardless of option, where consistency is important in the consumer experience, the Data Standards may also include guidelines or security controls that constrain how certain authentication methods are presented. An example of this could be the support of FIDO or WebAuthentication[6] Passkeys to ensure necessary information is conveyed to the consumer using standardised technical implementations.

All options support modernisation of authentication method support so biometrics and other strong authentication factors can be leveraged by Data Holders.

Consultation questions

5. What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why?
   The 2022 Independent Health Check recommended that entropy for OTP use should be increased and OTPs shouldn't be used by themselves, but only in multifactor authentication scenarios because of the phishing risk and issues with delivery of OTP through common mechanisms like SMS and email.
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?
7. Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?
8. How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?

5.3. Uplift the 'Redirect with OTP' flow

The 2022 Independent Health Check made several recommendations, which the Data Standards Chair responded to. Recommended changes included, among other things, changes to the OTP length, entropy requirements according to TDIF role requirements[7], and a customer's choice of delivery channel. These changes would impact the current 'Redirect with OTP' flow.

To address the recommendations from the 2022 Independent Health Check it is proposed to increase the minimum OTP length to six digits, from the currently allowed four digits to satisfy the entropy requirements set out in the TDIF Role Requirements, and mandate appropriate pseudo-randomness when generating OTPs.

[6] A more practical overview: https://webauthn.guide
[7] See CSP-04-02-03j, Digital Transformation Agency: TDIF 05 Role Requirements

It also seeks feedback on the longevity of OTP authentication and the trade-offs between security and existing CDR rules for offline customers and less digitally mature industries designated by the CDR.

Offline customers

This section applies to **both** offline and online customers.

5.3.1. Proposals being made

The following recommendations are proposed:

2022 Independent Health Check, Recommendation 3: OTP Channel Choice

Unless the channel that OTPs are delivered by has already been established as an authentication channel, the consumer should be advised of the OTP delivery channel and permission sought to use that chosen channel for OTP delivery. The 2022 Independent Health Check suggested that it is possible multiple customers within the same household or family could share the same communication channel, like a common email address. If the consumer is unaware that a communication channel will be used as a channel for delivering CDR authentication secrets, it should not be repurposed without the consumer's consent.

> **Proposal:** No proposal is made. Feedback is sought on whether a change in this area is appropriate and what considerations need to be factored in.

2022 Independent Health Check Recommendation 5: Set A Minimum OTP Length Of At Least 6

The recommendation proposed minimum length for an OTP must be 6 digits to satisfy the TDIF requirements for randomly generated authentication secrets. Furthermore, the review recommended that rate limiting should be applied to the number of attempts at OTP validation when the generated OTP has less than 64 bits of entropy.

> **Proposal:** Increase the minimum OTP length to 6 digits.

2022 Independent Health Check, Recommendation 6: Remove The Maximum OTP Length

The review recommends removing a maximum length for OTPs. Practically speaking, this could introduce unwarranted friction and may result in large OTPs that are difficult for consumers to input during the authorisation flow. Instead, the response to the review proposes the maximum length be increased to 10 digits.

> **Proposal:** Increase the maximum OTP length to 10 digits.

2022 Independent Health Check, Recommendation 8: OTP Pseudo-randomness

The review recommends that OTP codes must be generated with an approved source of randomness so an attacker cannot infer information about the OTP generation algorithm (e.g., a pseudo random number generated that uses a static input seed).

Proposal: Change the current *pseudorandomness statement to be:*
*"Data Holders **MUST** generate random OTPs in accordance with [TDIF] CSP-04-02-03j."*

This change would see the current requirement that OTPs *should* incorporate a level of pseudo-randomness to instead be a randomly generated OTP where random is defined as an approved random bit generator source according to TDIF and NIST[8].

Change Request 568: OTP SMS codes for CDR consent should be independent of online banking SMS settings

This change request proposes that OTP should not be delivered to a channel the customer hasn't registered or has security settings turned off for. It is similar to Recommendation 3 of the 2022 Independent Health Check which recommended that customers consent to a communication channel being chosen as their authentication channel before OTPs are delivered. If the consumer has chosen to disable a certain channel, or the Data Holder knows that the consumer cannot receive an OTP via a specific channel, it should not be presented as an option for OTP delivery.

Proposal: An additional statement be added to the Data Standards stating that Data Holders MUST NOT deliver OTPs where a channel has not been pre-registered by the customer, or the customer has elected that authentication secrets are not to be delivered by the specific channel.

Consultation questions

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

5.4. X2App (Web2App and App2App) Interaction Flows

This work package partially addresses **Recommendation 13: Alternative Authentication Flows** of the 2022 Independent Health Check.

The 2022 Independent Health Check recommended support for alternative authentication flows. The DSB's response was to consider support for App2App, which the community have previously proposed, including in the November 2020 Data Standards Advisory Committee.

[8] NIST SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

Lessons from UK Open Banking have also suggested that conversion rates, particularly for 're-authorisation', significantly improved with the introduction of App2App. The CX research demonstrated that App2App and Web2App flows performed very well in terms of usability, trustworthiness, and consumer expectations in general.

Given the collective insights and recommendations to date, the DSB is proposing that the standards be expanded to require support for App2App and Web2App. This would allow ADRs to use a redirect URL that deep links to a Data Holder's app, if available, for the consumer to authenticate with for the purposes of CDR authorisation. The consumer would be able to log in to their Data Holder app using their existing method, such as a pin code or biometric, which would help achieve parity between CDR and non-CDR authentication. Subsequent decision proposals will consult on Web/App2App in more detail, which may include support for the use of authenticators, biometrics, multi-factor authentication (MFA), and other security and usability considerations.

Offline customers

Where the Data Holder is authenticating an offline customer, it is proposed that the Data Holder is required to only implement the existing Redirect with OTP interaction flow.

The options being considered would apply to the Data Holder if the customer is 'online'.

5.4.1. Options for consideration

With all options it is proposed that the consumer **must not be required to enter any user identifier** (customer ID etc) irrespective of whether the consumer is establishing once-off or ongoing consent.

How alternative flows are standardised is a key consideration. In the UK, banks are required to support App2App authorisation in certain circumstances. Similarly, the CDR could choose to adopt mandated support requirements. Alternatively, what support is offered by which Data Holders may be left to the discretion of each Data Holder. It is quite possible that certain flows in conjunction with certain authentication method requirements would be necessary for Action Initiation, or a subset of Action Initiation use cases like in-store payments.

Option 1: Data Holder determined framework

This could see the standards support a range of interaction flows, but the specific approach to use will be determined by the Data Holder. For example, a range of approaches could be supported as 'MAY' or 'SHOULD' obligations in the standards, allowing Data Holders to choose which specific approach(es) to use. The DSB does not recommend this option as it may introduce unnecessary divergence across Data Holders, which in turn may undermine consistency, consumer experience, and the desired conversion rates of ADRs.

The choice of whether a Data Holder supports Web2App and App2App interaction flows is left to the discretion of the Data Holder. If a consumer initiates the consent flow on a device like a smartphone, the Data Holder could support deep linking to the correct location within their app.

The benefit of this option is that there is no CDR-wide obligation date required. If Data Holders choose to support x2app interaction flows, they can do so within their own timeframes.

Option 2: ADR determined framework

This framework could also see the standards support a range of interaction flows, but the ADR determines the preferred approach to use. For example, a defined range of approaches could be supported as 'MUST' obligations in the standards, and the ADR requests which specific approach to use. The DSB does not recommend this approach as there may be legitimate reasons for a Data Holder to have a reasonable amount of flexibility where certain methods are not available.

The advantage of this option is that ADRs can enforce preferred consumer experience outcomes but the disadvantage is that it defers authentication considerations to the ADR outside of the Data Holder's security perimeter and control.

Option 3: Fallback framework [DSB RECOMMENDED]

With this framework, a range of interaction flows could be supported, but the data standards determine the preferred approaches to use. For example, this could require that x2App and Redirection be supported, and the standards stipulate that x2App must be used if available and Redirection only where preferred methods are not available.

Where the Data Holder does not provide an app, or the consumer does not have the app installed, the Data Holder would not support x2App flows and may route the user through a web-based redirection journey.

The benefit of this proposal is that ADRs can rely upon consistency in the experience between ADR and Data Holder for same-device consent journeys. This option would impose a blanket implementation requirement across all Data Holders.

To support an expanded approach to CDR authentication while maintaining best practice security and an optimal CDR consumer experience, the DSB proposes Option 3: Fallback Framework. A fallback framework will establish preferred mechanisms for authentication and, where they fail or are not available, will outline 'fallback' approaches to be used instead. This could, for example, give primacy to Web/App2App as an authentication mechanism, followed by a Redirection mechanism where Web/App2App fails or is not available.

This is consistent with the DSB's response to Recommendation 13 of the 2022 Independent Health Check, as follows:

> *Where a Data Holder offers secure methods of authentication that satisfy the required Credential Level, these should be used in preference to any weaker security methods of authentication. Offering a fallback where consumers do not have possession of the more secure authentication method is prudent, but only used in a cascading manner.*

It also reflects community input to date, including the November 2020 Data Standards Advisory Committee, where members proposed that the data standards support a 'waterfall

authentication' approach that required primary support for App2App, followed by Redirect with OTP and/or other less preferable alternatives.

The below diagram illustrates how such a framework could operate in the context of the CDR with Web/App2App, Decoupled, and Redirection included as supported authentication examples.

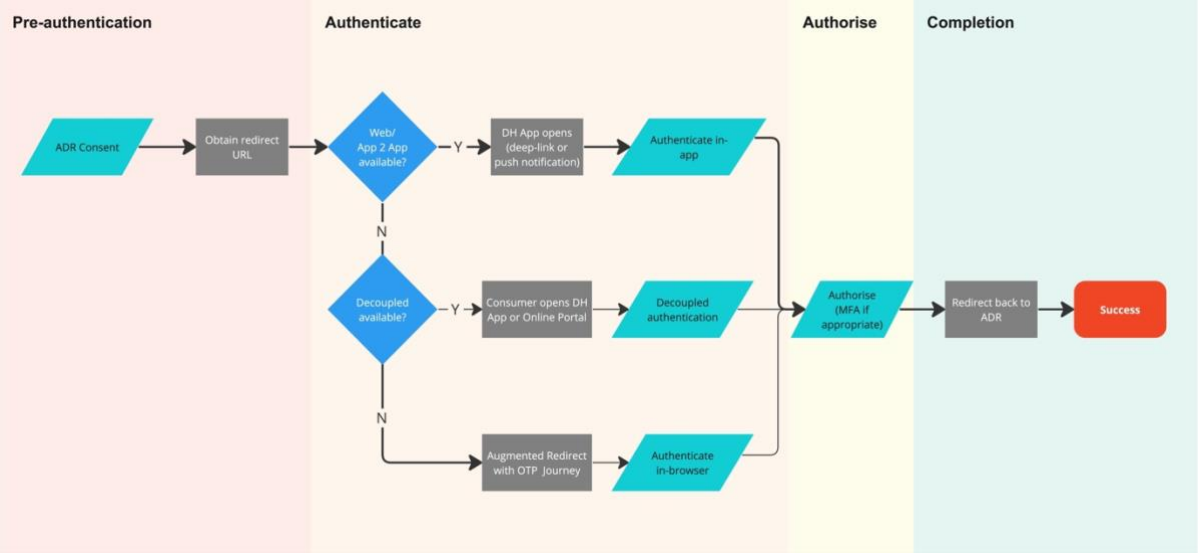

Figure 2 An example decision flow for different authentication flows proposed in this paper

In the above diagram, the choice taken by each Data Holder would represent the interaction flows available but would also remain cognizant of the required Credential Level for the data being shared which may still require the Data Holder to present authentications challenges compliant with TDIF CL2 or above.

Consultation questions

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?

5.5. Transition Roadmap: phasing in of authentication uplift obligations

Authentication uplift will require transition. Within the timeframes of the proposed changes both the Non-Bank Lending sector go-live and Action Initiation readiness have been considered.

Phase 1 of authentication uplift is proposed to be aligned to the earliest date of either 11th November 2024 (Y24 Obligation Milestone #5) or the first NBL go-live date for consumer data sharing.

<table>
<tr><th colspan="2">Phase 1</th></tr>
<tr><td colspan="2">End of 2024 (earliest of 11 Nov 2024 or NBL consumer data sharing go-live date)
Ready for Non-Bank Lending</td></tr>
<tr><td colspan="2">Credential Level support
Enhanced authentication methods
Redirect with OTP Authentication Enhancements
Multi-factor authentication
X2App Interaction Flows
Non-Functional Requirements</td></tr>
<tr><th>Phase 2</th><th>Phase 3</th></tr>
<tr><td>July 2025 (indicative)
Enhanced Consumer Experience</td><td>End of 2025 (indicative)
Ready for Action Initiation</td></tr>
<tr><td>Streamlined re-authentication
Push-Based Decoupled Interaction Flows</td><td>Step-up authentication
Pull-Based Decoupled Interaction Flows
Federated Identity
Business SSO</td></tr>
</table>

Consultation questions

12. Are the dates proposed for Phase 1 achievable?
13. Do you propose any other enhancements to the uplift of authentication for the CDR?

5.6. Non-Functional Requirements (NFR)

5.6.1. Rate-limiting

Section 4.3.2 “Rate limiting (*Throttling*)” of TDIF control requirements to limit unsuccessful authentication attempts.

With the uplift to authentication to support App2App and strong authentication factors, authentication challenges will more commonly be applied for both CDR authentication and access to existing digital services.

For example, if App2App is supported and a PIN code authentication factor secures a bank’s mobile banking app, the rate limiting may apply to any attempts to access the mobile banking app. If the consumer failed to enter their PIN code for mobile banking purposes, then failed two consecutive times for CDR access, the Data Holder may apply a credential lock on the mobile application which requires unlocking via an out of band process.

How rate limiting is applied may need to cater for how authentication controls are applied, and the breadth of applications and services common authentication controls apply to.

Further to this, TDIF requirement SP-04-03-02b states that consecutive failed authentication attempts must be limited to 100. In banking, the limit is often significantly lower (e.g., 3 attempts). A further consideration is whether the Data Standards should apply a minimum requirement on unsuccessful authentication attempts and a maximum limit.

2022 Independent Health Check, Recommendation 7: Guidance for Defending Against Enumeration Attacks

This recommendation suggested making improvements that guide Data Holders to defend against enumeration attacks on credentials. This recommendation considers CAPTCHAs as one pathway to defence but also states that uplifting authentication standards would be a better approach.

> *Consider more detailed guidance about defending against enumeration attacks, for example that Data Holders should be alert for attacks against multiple different accounts at once.*

TDIF role requirements offer general credential guidance including requirements that verifiers implement rate limiting[9] credential verifications.

In practice, many websites employ rate limiting techniques for login. Banks often permit between three and five attempts before locking an account which then requires the customer to phone the bank to unlock.

> **Proposal:** The following changes are proposed:
>
> 1. Data Holders must comply with TDIF 05 Role Requirements section 4.3.2 for rate limiting authentication attempts
> 2. Data Holders may apply a single rate limit control for application access where it is the same authentication control for CDR and non-CDR services
> 3. The use of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) in the CDR authentication flow are **not** permitted

5.6.2. Metrics and reporting

In the UK, the equivalent of Data Holders report on authentication efficacy including the ADR-equivalent's request channel, the Data Holder's authentication channel and the type of authentication model[10].

It is proposed that CDR metrics be extended to support observability on authentication performance but this will be consulted on in a subsequent proposal to incorporate the feedback to this paper.

---

[9] See CSP-04-03-02; CSP-04-03-02a; CSP-04-03-02b; CSP-04-03-0c; CSP-04-03-0d, Digital Transformation Agency: TDIF 05 Role Requirements

[10] MI Reporting Data API Specification v3.1.11 ASPSP, Open Banking Implementation Entity, https://openbankinguk.github.io/mi-docs-pub/v3.1.11-aspsp/specification/mi-data-reporting-api-specification.html

Consultation questions

14. Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?
15. Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?

6. Current Recommendation

This section outlines the DSB's recommended options to pursue in Phase 1 of authentication uplift:

- **Levels Of Assurance**
  - Option 3: Require LoA 3 or above for online customers, and
  - Introduce a Level of Assurance LoA 4 represented by the URI: urn:cds.au:cdr:4 where authenticators used to attain this level **MUST** conform with the TDIF Credential Level CL3
  - The Data Standards state support for Biometrics (for authentication use) is allowed in accordance with TDIF section 4.3.3
  - Data Holders may only support authenticators commensurate to their existing digital channels to ensure there is consistency across channels and customers are already enrolled for the Data Holder's preferred authenticators
  - Data Holders may offer the consumer choice of their preferred authenticator if the Data Holder supports more than one authenticator
  - An additional statement would be added to limit an LoA 2 for offline customers
- **Restricted Credentials**
  - Option 2: Data Standards define an exclusion list of Restricted Credentials
- **Uplift the 'Redirect with OTP' flow**
  - Increase minimum OTP length to 6 digits
  - Increase maximum OTP length to 10 digits
  - OTPs must be random
- **X2App Interaction Flows**
  - Option 3: Fallback framework
- **Non-Functional Requirements**
  - Data Holders must implement rate limiting on authentication attempts in accordance with TDIF 05 Role Requirements section 4.3.2
  - Data Holders may apply a single rate limit control for application access where it is the same authentication control for CDR and non-CDR services
  - The use of CAPTCHAs is **not** permitted
  - Consult on metrics for authentication methods and interaction flows

The supported approach and options will be consulted on in more detail in the coming months. They are then expected to be proposed as binding standards with future dated obligations.

The DSB proposes that the supported options be implemented by December 2024, with the aim of finalising the first phase of standards in 2023.

The DSB then proposes two subsequent phases of authentication uplift that will continue to build on the work done to support Action Initiation. These later phases of work can also consider any other approaches proposed by the community, along with additional considerations as required, such as for Action Initiation.

7. Implementation Considerations

Changes to the CDR security profile and CX authentication standards will result in implementation impacts to all sectors and CDR participants. However, given these changes are deemed necessary to improve the security and consumer experience of CDR authentication, the DSB is proposing a tighter scope to sustainably manage and limit its impact.

The DSB invites views on the options outlined in this paper, their implementation impacts, and the proposed timeline for implementing the first phase of authentication uplift.

When reviewing this proposal and formulating feedback, please consider the following questions:

1. Do this paper's recommendations adequately tend to the security and consumer experience issues raised to date, or are there other options that need to be considered?
2. Which options (if any) are supported?
3. If no options are supported, what alternatives exist to address the identified issues?
4. Do you agree with the proposal to support certain approaches now and alternatives in a subsequent phase of authentication uplift?
5. What unforeseen impacts (if any) could these recommendations have?
6. What timeframes for implementation would need to be considered?

Following the completion of this initial consultation, the DSB intends to conduct targeted consultations on any supported options in the coming months, with a view to finalising the associated standards in 2023 for a 2024 obligation date. A subsequent phase of authentication uplift to examine alternative authentication approaches is expected to take place in 2024, which may need to consider Action Initiation requirements.

7.1. Sector specific requirements

The DSB has considered the differing levels of digital maturity offered by Data holders across different sectors as well as the different security postures and current capabilities. Ensuring the safe and secure disclosure of CDR data to ADRs is paramount and by applying a context specific approach based on Credential Levels security controls are selected based on the intended usage of the data being shared—or in future, the action being performed—supports an objective and scalable framework to assess security risks and apply consistent authentication controls. This approach recognises the differences between the sectors designated in the CDR but also the different data clusters included in each designation.

7.2. CDR usability and offline customers

Stronger authentications measures tend to be predicated on Data Holder having the ability to assign security controls against a pre-existing digital identity. Stronger forms of authentication, like biometric enrolment and soft token apps, often include the enrolment of devices controlled by the consumer.

Offline customers are however a challenge with the expansion of authentication requirements because they are, by definition, consumers who interact with a Data Holder without a digital identity. The consumer experience, digital and cyber security maturity of some existing and potentially new sectors that are designated for inclusion may therefore require careful consideration in how inclusivity of consumer access to their data as defined by the rules can be balanced against the needs for strong security.

Any changes to the authentication framework will need to consider how to cater to offline customers, to ensure they can seamlessly access CDR services, while attempting to improve on existing non-secure processes that the CDR aims to replace.

This paper asks questions on whether authentication uplift needs to be supported by identity registration / enrolment standards and what limitations or impacts must be considered with offline customers.

The DSB acknowledges the challenges of maintaining best practice security as per 8.11(1)(c)(i)[11] whilst maintaining support for offline customers, such as in the energy sector where no requirement exists for the consumer to have online account access as there is in banking.

7.2.1. Pathway towards universally strong authentication

To achieve stronger authentication protections in the energy sector changes to the rules would need to consider mechanisms that allow a stronger security posture. For example, permitting energy retailers to digitally onboard offline customers within the CDR whether that is achieved through the authentication flow or pathways that facilitate online registration prior to consumer authentication.

7.3. Ongoing Review and Uplift

Whilst this paper considers uplift over the medium-term, security is a continually changing landscape and it is important to recognise the need for continual evolution of authentication standards to keep pace with industry trends and security threats. This decision proposal outlines what are considered the primary areas for authentication uplift at present to provide a strong and secure data sharing ecosystem that is also well prepared for Action Initiation. Along with regular independent security reviews, there is a recognised need to conduct ongoing reviews and monitoring of the threat landscape and security controls in place for the CDR.

[11] CDR Rule 8.11(1)(c)(i): *"authentication of CDR consumers to a standard which meets, in the opinion of the Chair, best practice security requirements"*

7.4. Milestones and dependencies

In proposing the proposed phasing dates for authentication uplift, both the Non-Bank Lending and Action Initiation timeframes have been considered. Stronger authentication standards are a necessity for Action Initiation, whilst we are cognizant of reducing additional effort as the Non-Bank Lending sector comes online.

Appendix A

8. List of consultation questions

Community feedback is sought for the following list of consultation questions. These questions in this proposal have been consolidated below.

Section 5.1 Levels of Assurance

Consultation questions

1. Are there any reasons, or scenarios, when MFA ***must*** be required?
2. Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?
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?
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?

Section 5.2 Restricted Credentials

Consultation questions

5. What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why?
   The 2022 Independent Health Check recommended that entropy for OTP use should be increased and OTPs shouldn't be used by themselves, but only in multifactor authentication scenarios because of the phishing risk and issues with delivery of OTP through common mechanisms like SMS and email.
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?
7. Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?
8. How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?

Section 5.3 Uplift the 'Redirect with OTP' flow

Consultation questions

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

Section 5.4 X2App (Web2App and App2App) Interaction Flows

Consultation questions

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?

Section 5.5 Transition Roadmap: phasing in of authentication uplift obligations

Consultation questions

12. Are the dates proposed for Phase 1 achievable?
13. Do you propose any other enhancements to the uplift of authentication for the CDR?

Section 5.6 Non-Functional Requirements (NFR)

Consultation questions

16. Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?
14. Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?