Data Standards Body

Technical Working Group

Decision 258 – The Data Standards Chair's Response to Independent Security Health Check

Contact: Mark Verstege
Publish Date: Friday December 9th, 2022
Decision Authority: Data Standards Chair, Friday December 16th, 2022

Context

The Data Standards Chair (**Chair**) commissioned Thinking Cybersecurity to conduct an Independent Health Check (**Health Check**) of the Consumer Data Standards (v1.17.0).

Under the Consumer and Competition Act 2010 (CCA), Part IVD, Division 6, Section 56FA (1)(c), the Chair may make Data Standards about the collection, use, accuracy, storage, security and deletion of Consumer Data Right (**CDR**) data. And because the Chair has duties for care and due diligence, the Health Check is therefore an important source of advice they receive with respect to making, and reviewing, Data Standards. This is especially important because in accordance with CDR Rules Division 8.4 Paragraph 8.11 (1)(c)(i) the authentication of CDR consumers must, in the opinion of the Chair, meet best practice security requirements.

The Health Check was published on July 7th 2022, which included 31 recommendations.

The Chair wishes to thank the Health Check's authors Vanessa Teague, Chris Culnane, and Ben Frengley; and CDR participants that provided their feedback to Noting Paper 258.

This document is the Chair's response to their Health Check for each recommendation, indicating the intended processes to be used in order to inform future Decision Proposals (**DPs**). In accordance with Part 8 Section 8.9 of the Rules, the Chair must consult when developing or amending the data standards. Consequently, different change processes are proposed to allow for consultation when responding to the recommendations in the Health Check, which include:

- Consumer Experience (**CX**) Research
  The CX workstream of the Data Standards Body (**DSB**) conducts Consumer Experience Research, where they assess hypotheses with members of the public, including vulnerable consumers, and make recommendations accordingly.

- Change Requests (**CRs**)
  The Data Standards Maintenance Iteration (**MI**) process is a Data Standards development process that involves CRs, which may be raised by the ecosystem, or the DSB. These CRs are considered as part of a given MI cycle and enable consultation to be conducted prior to a new version of the Data Standards being issued.

- Support Guidance Documentation
  Knowledge base articles are created, and/or amended, in order to address the specific questions arising from the ecosystem.

- Decision Proposals (**DPs**)
  Data Standards development processes result in Decision Proposals (**DPs**) that are provided to the Chair for his approval through his function to make, and review, Data Standards under CCA Part IVD Div 6 Section 56FH(1). DPs may be raised without a prior Data Standards development process. DPs are made in accordance with the CDR Rules Part 8 Division 8.3.

The Chair also invited comment from the Data Standards Advisory Committee (**DSAC**) which is included as an appendix at the end of this document.

Responses to Recommendations

Summary of responses to the Health Check's recommendations:

#	Recommendation	DSB's Response	Change Process	Chair's Decision
1.	**Data Holder URLs**	Endorsed	CX Research	Approved
2.	**Consumer Awareness of ADR Providers**	Endorsed	CX Research	Approved
3.	**OTP Channel Choice**	Endorsed With Changes	CX Research Decision Proposal	Approved
4.	**Credential Level Normative References**	Endorsed With Changes	Change Request	Approved
5.	**Set A Minimum OTP Length Of At Least 6**	Endorsed With Changes	Change Request, Decision Proposal	Approved
6.	**Remove The Maximum OTP Length**	Endorsed With Changes	Change Request	Approved
7.	**Guidance For Defending Against Enumeration Attacks**	Not Endorsed – Alternative Proposed	Decision Proposal	Approved
8.	**OTP Pseudo-randomness**	Endorsed With Changes	Change Request	Approved
9.	**CDR Lock**	Endorsed	CX Research Inter-Agency Assessment	Approved
10.	**Permit Strong Authentication**	Endorsed	CX Research Decision Proposal	Approved
11.	**Authentication Constraint Messaging**	Endorsed	CX Research	Approved

#	Recommendation	DSB's Response	Change Process	Chair's Decision
12.	**Require Credential Level 2**	Endorsed	CX Research Decision Proposal	Approved
13.	**Alternative Authentication Flows**	Endorsed	CX Research Decision Proposal	Approved
14.	**Intermediate Certificate Authority Key Length and Lifetime**	Endorsed	Change Request	Approved
15.	**Leaf Certificate Lifetimes**	Endorsed	Change Request	Approved
16.	**Key Rotation Policies**	Endorsed	Change Request Support Guidance	Approved
17.	**Certificate Validation Instructions**	Endorsed	Support Guidance	Approved
18.	**Revise Existing Certificate Validate Documentation**	Endorsed	Support Guidance	Approved
19.	**MTLS Requirements**	Endorsed	Change Request	Approved
20.	**Fix Documentation Anchor Link**	Endorsed	Change Request	Approved
21.	**JWKS Endpoint Documentation**	Not Endorsed – Alternative Proposed	Change Request	Approved
22.	**Dynamic Client Registration RFC Alignment**	Endorsed	Decision Proposal	Approved
23.	**Accreditation State Transitions**	Endorsed	Support Guidance	Approved
24.	**Sender Constrained Refresh Tokens**	Not Endorsed	No Change	Approved
25.	**MTLS And Certificate Expiration**	Not Endorsed	No Change	Approved
26.	**Refresh Token Rotation (FAPI)**	Not Endorsed	No Change	Approved
27.	**Refresh Token Rotation (Data Standards)**	Not Endorsed	No Change	Approved
28.	**Refresh Token Expiry and Sharing Duration**	Endorsed	Change Request	Approved
29.	**CDR Register JWKS Location**	Endorsed	Change Request	Approved

#	Recommendation	DSB's Response	Change Process	Chair's Decision
30.	**Non-Repudiable Authorisation Receipt**	Endorsed	Decision Proposal	Approved
31.	**Security Trade-offs**	Endorsed	Change Request	Approved

Additional Recommendations

#	Recommendation	Proposal	Process	Chair's Decision
32.	**Future Independent Health Checks**	Perform regular independent health checks	External Review	Approved

Feedback Received

Feedback to the Health Check was sought in Noting Paper 258. The feedback has been summarised below:

- Broadly, there was support for most recommendations and suggestions presented in the report.
- There was strong support for the open, transparent, and consultative model the DSB has adopted for community consultation and standards development.
- Participants expressed the importance that the authentication standards meet the Australian Government Digital Identity System's (**AGDIS**) Trusted Digital Identity Framework (**TDIF**) Credential Level 2 (**CL2**) authentication requirements for data sharing.
- Concerns were raised with the current OTP authentication standards. This feedback is further covered in Recommendation 13.
- Energy participants related that their sector had lower identity proofing requirements to Banking. This feedback is further covered in Recommendations 5.
- Participants supported uplifting the authentication standards to be more secure, streamlined and in line with existing Data Holder practices.
- Questions were raised about increasing the cognitive burden on consumers to understand and counteract phishing risks. This feedback is further covered in Recommendations 1 and 2.
- The OIDF provided feedback in relation to the FAPI profile. This feedback is further covered in Recommendations 24—28.
- Participant feedback considered broadening the scope of the next independent health check. This feedback is further covered in Recommendation 32.

Glossary

Term	Definition
2FA	Second or Two Factor Authentication

Term	Definition
ACCC	Australian Competition and Consumer Commission
ACSC	Australian Cyber Security Centre
ADR	Accredited Data Recipient
AGDIS	Australian Government Digital Identity System
API	Application Programming Interface
CA	Certificate Authority
CAEP	Continuous Access Evaluation Protocol
CDR	Consumer Data Right
CL	Credential Level
CX	Consumer Experience
DCR	Dynamic Client Registration
DH	Data Holder
DOMS	Disclosure Option Management Service
DSAC	Data Standards Advisory Committee
DSB	Data Standards Body
FAPI	Financial-grade API
FIDO	Fast IDentity Online
JAMS	Joint-Account Management Service
JSON	JavaScript Object Notation
JWKS	JSON Web Key Set
MTLS	Mutual-TLS *(see TLS)*
NIST	National Institute of Standards and Technology (US)
OIDC	OpenID Connect
OIDF	OpenID Foundation
OTP	One-Time Passcode
RFC	Request For Comments
RISC	Risk Incident Sharing and Coordination
SMS	Short Message Service
SSA	Software Statement Assertion
SSE	Shared Signals and Events
SSL	Secure Sockets Layer
TDIF	Trusted Digital Identity Framework *(see AGDIS)*
TLS	Transport Layer Security

Term	Definition
WAF	Web Application Firewall

Health Check Report Recommendations and Responses

Recommendation 1

> *Consumers should be clearly warned that they need to check the URLs of their Data Holder OTP entry, even if they have been directed there by a trusted source. They should also be informed that the OTP entry should never be via an ADR's website or app.*

Response
The DSB endorse the Chair accepting this recommendation, provided it is supported through CX research.

Change Process
Consumer Experience Research

Rationale
CX research is conducted to determine the efficacy and usefulness of this recommendation. Findings from the CX research will be integrated into any potential CX standards and guideline changes.

Feedback Received
There wasn't strong support for increasing burden on the consumer to check URL links and verify the legitimacy of participants.

Feedback was supportive in principle of improving consumer comprehension provided it didn't burden consumers and it was complementary to additional security controls in the system.

One suggestion offered in feedback and supported by some participants was the introduction of CDR "trust markers" or trust ratings for data holders and data recipients to give consumers more confidence when choosing providers.

To reduce consumer burden one solution may be the inclusion of a dynamic "water mark" CDR logo or participant logo that is cryptographically signed by the CDR Register and can be verified similar to an SSL certificate lock icon presented in web browsers.

Recommendation 2

> *Consider ways to raise awareness of the existing list of current providers. The existing CX requirement for ADRs to provide a link is good, but needs to be supported by clear messages so that consumers know to be suspicious of a purported ADR that doesn't provide the link.*

Response
The DSB endorse the Chair accepting this recommendation, provided it is supported through CX research.

Change Process
Consumer Experience Research

Rationale
CX research will be conducted to determine the efficacy and usefulness of this recommendation. Findings from the CX research will be integrated into any potential CX Data Standards and Guideline changes.

Further discussion between CDR responsible agencies will be conducted to ascertain whether awareness can be raised through government-owned CDR channels outside of the consent model.

Feedback Received
There wasn't strong support for increasing burden on the consumer to check URL links and verify the legitimacy of participants. Feedback was supportive in principle of improving consumer comprehension provided it didn't burden consumers and it was complementary to additional security controls in the system.

Recommendation 3

Require Data Holders to ask consumers for permission to use a certain channel as the CDR OTP delivery channel if it was not originally set up as an authentication channel.

Response
The DSB endorse the Chair accepting this recommendation with changes.

Endorsed changes are:

- The DSB will consider the appropriateness of CX Standards and/or CX Guidelines on how Data Holders provide a choice of channel(s) to consumers
- The DSB will consider alignment with TDIF identity proofing and credential requirements. For example, if the OTP is delivered by SMS, then the consumer must first prove possession of the phone number before an OTP can be delivered to the consumer for CDR authentication.
- The DSB will consider the appropriateness of each channel to ensure they meet general industry information security best practice.

Change Process
Consumer Experience Research leading to a future Decision Proposal on Authentication Uplift.

Rationale
The DSB sees advantages in aligning the Data Standards with the respective requirements of the TDIF accreditation framework for Digital Identity services.

The DSB is mindful that the Australian Cyber Security Centre (**ACSC**) strongly recommends Multi-Factor Authentication (**MFA**) as an essential step towards cyber security. And whilst the ACSC notes vulnerabilities in SMS OTPs, they still recommend this channel.

Additionally, offering consumer choice is an emerging trend for authentication of digital services, and choice is a fundamental principle of the CDR. It offers agency to the consumer for expressing how they wish to authenticate, affording them the option of consistent and familiar processes across a variety of digital services.

Forcing consumer choice, however, is not always a practical approach for data holders because there is only one channel offered or there are preferred channels based on the security posture of the data holder. For example, a data holder may offer a soft-token authenticator app and SMS OTP delivery, however, they may prioritise soft-token authentication OTP use where the consumer has a registered authenticator app. In this scenario, falling back to SMS OTP would only be offered for consumers that do not have a registered soft-token authenticator app.

Further to this, the Data Standards have consistently stated that Data Holders' CDR solutions must align to the existing processes and consumer expectations with the Data Holder:

- *Data Holders **MUST** provide a one-time password (OTP) to the customer through an existing channel or mechanism that the customer can then enter into the redirected page*
- *The delivery mechanism for the OTP is at the discretion of the Data Holder but **MUST** align to existing and preferred channels for the customer and **MUST NOT** introduce unwarranted friction into the authentication process*

That being said, the TDIF does support guidance in regard to the validation of the delivery mechanism where the user is receiving a secret to a verifiable user claim such as an email address or mobile phone number.

Applicable TDIF Role Requirements from section 4.4 Credential Lifecycle Management include:

> **TDIF Req:** CSP-04-02-03l; **Updated**: Jun-21; **Applicability**: C
> If *out-of-band verification* is to be made using the *PSTN*, the *Applicant MUST* validate that the pre-registered telephone number being used is associated with a specific physical device.
>
> **TDIF Req:** CSP-04-05-04; **Updated**: Jun-21; **Applicability**: C
> The *Applicant MAY* choose to *validate* a *User*'s contact details (i.e. email, mobile phone number) and *MUST* suspend a *Credential* reported to have been compromised.

In addition, the TDIF defines applicable identity proofing requirements in section 3.2 Identity Proofing (see Table 1) and section 3.6 Attribute collection, verification and validation (see Table 2, Identity System metadata).

Feedback Received

Feedback was supportive of strong authentication standards. However, concerns were raised that increasing complexity and cognitive burden for consumers should be avoided. And the DSB is mindful that mandatory accessibility guidelines address cognitive impairment, and suggest alternate approaches. Further, feedback contradicted increasing consumer choice in preference to adopting

standardised improvements to authentication, and, in some situations, alignment to existing Data Holder security solutions.

Recommendation 4

> *As defined in the referenced TDIF requirements [TDIF- ACR-1.3], Credential Levels are directly equivalent to NIST's Authenticator Assurance Levels [NIST-SP800-63B, s4]. Update references to use [NIST-SP800- 63B] rather than the TDIF for both defining Credential Levels and authenticator properties. If the Credential Levels from the TDIF are retained, refer directly to [NIST-SP800-63B] for authenticator standards to maintain the intended security level.*

Response
The DSB endorse the Chair accepting this recommendation with changes.

Endorsed changes are:

- TDIF references be retained with direct references to NIST where applicable.

Change Process
Maintenance Iteration Change Request

Rationale
The DSB sees advantages in aligning the Data Standards with the respective requirements of the TDIF accreditation framework for Digital Identity services, for the Credential Levels, but referring to NIST for the authenticator standards, as proposed by the Health Check.

This will ensure any jurisdictional requirements for Australia are incorporated into the core requirements.

Additionally, this provides a pathway for the expansion of the CDR to include TDIF accredited Identity Providers.

If the alternate proposal was accepted, to align with the NIST standards, instead of TDIF, this may create barriers to future expansion.

Feedback Received
Feedback supported alignment to NIST if adjacent standards did not enhance the meaning of the requirements leveraged by the CDR.

Recommendation 5

> *Set a minimum OTP length of at least 6 digits and require rate limiting measures to be implemented.*

Response
The DSB endorse the Chair accepting this recommendation with changes.

Endorsed changes are:

- A minimum OTP length of 6 digits.
- Rate-limiting measures of no more than 5 retries.

Change Process

Maintenance Iteration Change Request – OTP length
A future Decision Proposal – User Claim Verification and Identity Proofing

Rationale

The DSB sees advantages in aligning the Data Standards with the respective requirements of the TDIF accreditation framework for Digital Identity services.

In accordance with the TDIF requirements, random authentication secrets to an out-of-band device require at least 20 bits of entropy.

> **TDIF Req:** CSP-04-02-03j; **Updated**: Jun-21; **Applicability**: C
>
> The *Applicant* *MUST* generate random *Authentication* secrets with at least 20 bits of entropy.

This would require adopting a minimum 7-digit OTP:

$$\text{let } \boldsymbol{E = \log_2(R^L)}, \text{ where}$$

$E =$ *the secret's entropy,*
$R =$ *the number of possible characters within the selection pool. In a numerical passcode, R = 10,*
$L =$ *the secret's length, i.e. the number of characters in the secret*

if L = 6; then $\boldsymbol{E = \log_2(10^6) = 19.93}$
if L = 7; then $\boldsymbol{E = \log_2(10^7) = 23.25}$

However, many software token apps and hard token devices generate 6-digits, and these are commonly used in banking environments. Whilst the same entropy requirements do not apply to single -factor OTP device (compared to out-of-band devices), adopting a 7-digit OTP length for out-of-band devices would create a divergence in experience. Furthermore, 6-digit OTPs achieve close to the required 20 bits of entropy and the change to OTP length is intended to be accompanied by additional CL2 requirements as well as the consultation on stronger authentication flows.

Rate limiting, as endorsed, is also in accordance with the TDIF requirements, for authentication secrets with less than 64 bits of entropy:

> **TDIF Req:** CSP-04-02-03k; **Updated**: Jun-21; **Applicability**: C
>
> If the *Authentication* secret has less than 64 bits of entropy, the *Applicant* *MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity* account.

The TDIF role requirements on rate limiting are further emphasised in section 4.3.2 Rate limiting (*Throttling*).

Feedback Received
Feedback was supportive of ensuring OTP authentication was secure. Participants also indicated a strong desire for the CDR to offer stronger authentication alternatives in preference to OTP. Nevertheless, in less digitally mature industries, OTP was still considered an important mechanism to employ.

That said, it was acknowledged that in a lower identity proofing environment such as Energy, OTP spear phishing attacks are more easily executed. This suggests additional security measures may be worth consideration for the verification of user claims that are used for authentication. For example

- requiring a Data Holder to verify the OTP delivery channel before trusting the OTP, or
- verifying the user has ownership of the phone number an SMS OTP is delivered to, or
- implementing tenuring rules on the change of verified claims before a claim can be used or changed, and
- defining standards for maximum retry attempts.

Recommendation 6

Consider removing the maximum OTP length and allowing Data Holders or even consumers to choose to make them longer than 6 digits.

Response
The DSB endorse the Chair accepting this recommendation with changes, subject to CX research.

Endorsed changes are:

- To retain, but increase, the maximum OTP length.
- Increasing the maximum OTP length from 8 digits to 10 digits.

Change Process
Maintenance Iteration Change Request

Rationale
The rationale for this proposal is to ensure consumer usability is weighted against the increased OTP strength requirements. Allowing data holders to increase the OTP length arbitrarily may result in increased consumer friction and inconsistency in the implementation across data holders. Such risks can be mitigated through CX research and CX standards as appropriate

Based on community feedback the changes to improve the security of OTP authentication are worthwhile. This recommendation is necessary but insufficient to achieve best practice security by itself. For example, it needs to be combined with a second factor of authentication to achieve CL2 (Recommendation 12). This recommendation and others related to OTP uplift will be considered

together as part of the holistic uplift to the authentication standards because of the sensitivity of CDR data.[1]

Feedback Received
No direct community feedback was received for this recommendation. Feedback was strongly in support for moving beyond OTP authentication to more secure solutions. Specific reference to the UK authentication flows was also mentioned.

Recommendation 7

> *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.*

Response
The DSB endorse the Chair **does not** accept this recommendation, but instead endorses an alternative change.

Specifically:

- Consider the sharing of security event signals between participants to reduce fraud and malicious attacks across the CDR ecosystem.

Change Process
A future Decision Proposal –Shared Signals and Events

Rationale
Many large organisations have internal security consulting teams whose job it is to review the security controls and protections for their software systems. Guidance on the protection against enumeration attacks and other preventative security measures are better left to internal consulting discussions within the data holder.

It is also noted that many Web Application Firewalls (**WAFs**) and security edge protection appliances allow for configurable "silent CAPTCHAs" which can be effectively deployed without inconveniencing consumers.

In adopting recommendations 8—10, 12, and 13 this will deliver more secure authentication standards and reduce the dependency on mechanisms like CAPTCHAs to be deployed with single-factor authentication. The report acknowledges that "uplifting authentication standards would be a better trade-off than CAPTCHAs for improving security without inconveniencing consumers."

Further to this, the DSB has previously indicated that Continuous Access Evaluation Protocol (**CAEP**) and Risk Incident Sharing and Coordination (**RISC**) Event Types are worth consideration along with the sharing of security events between ecosystem participants to strengthen the cybersecurity posture of the entire ecosystem and help protect consumers and data holders.

[1] Please refer to Recommendation 10 and Recommendation 12

Th DSB is mindful of the Shared Signals and Events (**SSE**) framework being developed by the OIDF.

Feedback Received
Feedback suggested adopting sharing of authentication and login signals between participants in the event of failed security attempts. Events of interest to participants included repeated failed authentication attempts at a Data Holder, high numbers of sessions from a single source, enumeration attacks, or other behaviours considered outside of 'normal' bounds.

Recommendation 8

> *Align the Data Standards with NIST [NIST-SP800-90A, NIST-SP800-63B] to provide requirements for appropriate sources of randomness. Change the "SHOULD" requirement about levels of pseudorandomness to a "MUST" requirement, or defer to NIST.*

Response
The DSB endorse the Chair accepting this recommendation with changes.

Endorsed changes are:

- Align with the TDIF 05 Role Requirements for memorised secrets including CSP-4-02-03j and CSP-04-02-03k

Change Process
Maintenance Iteration Change Request

Rationale
The DSB sees advantages in aligning the Data Standards with the respective requirements of the TDIF accreditation framework for Digital Identity services, instead of aligning with the United States of America's NIST Standards, as proposed by the Health Check.

In accordance with the Recommendation 4 response, TDIF alignment is retained, and the applicable requirements:

TDIF Req: CSP-04-02-03j; **Updated**: Jun-21; **Applicability**: C

The *Applicant MUST* generate random *Authentication* secrets with at least 20 bits of entropy.

TDIF Req: CSP-04-02-03k; **Updated**: Jun-21; **Applicability**: C

If the *Authentication* secret has less than 64 bits of entropy, the *Applicant MUST* implement a *Rate-limiting* mechanism that effectively limits the number of failed *Authentication* attempts that can be made on the *Individual's Digital Identity* account.

Feedback Received
No direct community feedback was received for this recommendation.

Recommendation 9

Require Data Holders to provide a CDR Lock that is initially on by default and prevents all CDR requests from being approved. Consumers can switch this lock off via their current stronger authentication method if they wish to take the risk and start using CDR. Should a stronger authentication flow be permitted by default the CDR lock could remain, but default to being off.

Response
The DSB endorse this recommendation being considered collectively by the CDR agencies, subject to CX Research.

Change Process
Consumer Experience Research and CDR Cyber Security Settings Assessment.

Rationale
This recommendation has policy and enforcement implications, consequently it requires inter-agency consultation. The Rules, however, require the Chair to apply industry best practice with regard to security, therefore this needs to be considered.

Feedback Received
Some feedback indicated that a "kill switch" may increase cognitive load on consumers and whilst the original joint-accounts management service was well intentioned, it created complexity which needs to be carefully considered in any changes like a CDR Lock in future.

Recommendation 10

Permit stronger authentication flows to be implemented and allow weaker ones to be disabled by default for user accounts that already have stronger authentication methods established.

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Consumer Experience Research leading to a future Decision Proposal on Authentication Uplift

Rationale
Stronger consumer authentication mechanisms would be consulted on in a targeted Decision Proposal. Empowering consumers with strong authentication standards that are both secure and convenient to use will deliver better consumer outcomes and protections.

Whilst stronger consumer authentication methods are supported, it is recommended that the Data Standards Chair look to research and consultation on uplifting authentication standards that offer ease of use, familiarity, and usability for consumers. Since the first publication of the Consumer Data

Standards, much more secure authentication methods have become commonplace including the prevalence of devices capable of biometric authentication, and the FIDO family of authentication standards incorporating WebAuthN and PassKeys.

Further to this, the Data Standards strive to deliver a commonality of experience through a commonality of process to maintain consistency across a diverse range of data holders. The purpose of this principle is to develop standardised CDR-wide experiences that are familiar to consumers in all point-to-point interactions between ADRs and Data Holders. Where new authentication flows are introduced, this will act as an additional quality control for consumers and the security of the CDR.

Feedback Received
Participant feedback supported the app-to-app authentication model and streamlining authentication flows.

Participants indicated that modern authentication standards including WebAuthN and App2App as alternatives to OTP were desirable.

Recommendation 11

> *Ensure messaging about constraints is consistent across providers and publicise those constraints outside of the CDR authorisation flow so that users are educated before starting the process about what to expect and reject.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Consumer Experience Research

Rationale
The recommendation covers Treasury's consumer engagement strategy as well as CX standards and guidelines that are the responsibility of the Chair. The recommendation is sound in principle. Given the recent data breaches within the Australian data environment, increased education that helps consumer be more aware of their privacy and security is valuable. To determine what, if any, additional consumer messaging and education is helpful to reduce phishing and social engineering risks, consumer research will be conducted. The findings of that research will inform the Chair's response to this recommendation.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, indicated that increasing the cognitive burden on consumers should be avoided and where possible, simplification and ease of use should be promoted. Again, this is consistent with the mandatory accessibility guidelines.

Recommendation 12

> *The default Credential Level in the Data Standards should be a minimum of CL2. Allowance can be left for industry-wide exceptions in the case that there is a strong argument that an industry does not handle sensitive data, but it is unclear if such an exemption would ever apply.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Consumer Experience Research leading to a future Decision Proposal on Authentication Uplift

Rationale
The DSB sees advantages in aligning the Data Standards with the respective requirements of the TDIF accreditation framework for Digital Identity services.

A single factor OTP such as an SMS OTP or email OTP satisfies Credential Level 1 in the TDIF 05 Role Guidance. Credential Level 1 is defined by the TDIF as follows:

> *Provides a low level of confidence that the Individual controls a Credential bound to their Digital Identity.* ***The intended use of this level is for services where the risks of getting Credential binding wrong will have negligible to minor consequences to the Individual or the service****. At a minimum, single-factor authentication is used at this level.*

Credential Level 2 is defined by the TDIF as follows:

> *Provides a medium level of confidence that the Individual controls a Credential bound to their Digital Identity.* ***The intended use of this level is for services where the risks of getting Credential binding wrong will have moderate to high consequences to the Individual or the service****. Proof of possession and control of two different authentication factors (multi-factor authentication) is required through a secure authentication protocol.*

If banking, energy, or telecommunications data was obtained by a malicious user this will result in moderate to high consequences to the individual. In the scenario that seven years of banking transaction data is exfiltrated, this would be a significant breach of the consumer's privacy. As such, CL2 should be enforced as a minimum.

Again, the DSB is mindful that the Australian Cyber Security Centre (**ACSC**) strongly recommends Multi-Factor Authentication (**MFA**) as an essential step towards cyber security.

CL2 authentication methods required by the TDIF include:

ONE OF:

- Multi-Factor OTP Device
- Multi-Factor Cryptographic Software
- Multi-Factor Cryptographic Device;

OR
Memorised Secret[2] AND ONE OF:

- Look-up Secret
- Out-of-Band Device
- Single-Factor OTP Device
- Single-Factor Cryptographic Software
- Single-Factor Cryptographic Device

Consequently, a single factor OTP is insufficient on its own to meet CL2.

Feedback Received
Participant feedback was supportive of requiring CL2 for data sharing. Participants also indicated that supporting authentication methods other than OTP were supported such as biometrics, WebAuthN and App2App authentication.

Recommendation 13

> *Consider alternative authentication flows that provide a higher level of consumer authentication without exacerbating phishing risk, for example, an app-based two-factor authentication flow.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Consumer Experience Research leading to a future Decision Proposal on Authentication Uplift

Rationale
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.

Feedback Received
Participant feedback was supportive of uplifting authentication standards to modernise authentication requirements in line with consumer expectations and increase the security of data sharing. Again, the DSB is mindful that the Australian Cyber Security Centre (**ACSC**) strongly recommends Multi-Factor Authentication (**MFA**) as an essential step towards cyber security.

Participant feedback indicated that using an OTP as a single factor was insufficient for read access. Participants also indicated that a User Identifier and OTP as an authentication mechanism was inconsistent with many data holder's existing authentication flows and there was a desire to align to how data holders authenticate customers via other digital channels.

[2] **Secrets** are the credentials used to perform digital authentication whenever users must access data or sensitive applications and services. Secrets can take multiple forms including: Passwords, API Keys, and Tokens.

Furthermore, feedback suggested that certain industries such as Energy were more susceptible of phishing attacks on OTP authentication, which increased the imperative to look at stronger authentication flows.

Recommendation 14

> *Specify a longer key length or shorter lifetime for the intermediate CA key, in keeping with best practice recommendations.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request for a Register Data Standard

Rationale
Adopting this change to both increase the key length and reduce the intermediate CA lifetime will reduce the risks of key compromise.

In consulting on this change, it may be that old and new CA keys could be used in parallel, thereby minimising change impact.

Because renewing the Intermediate CA will affect every participant in the ecosystem, participants would need to trust both chains for a period of time (old and new) to give the ecosystem time to cutover to the new chain. Migration and phasing impacts will be considered in the change request.

Feedback Received
No direct community feedback was received for this recommendation. Feedback did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 15

> *Consider limiting the lifetime of leaf certificates to 398 days.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request for a Register Data Standard

Rationale

The ACCC employs this practice for certificates issued to participants. Whilst the ACCC may benefit from a more automated process to facilitate this change, it is an achievable change that will improve security.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 16

> *Review [NIST-SP800-57-pt1-r5] for determining crypto periods and key rotation policy. Publish that policy and include notification periods that will be used when performing key rotation. Establish notification process to warn participants of when a key rotation will take place.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request for a Register Data Standard and Support Guidance Documentation

Rationale
Notification of upcoming key rotation may be facilitated through existing scheduled maintenance solutions such as Get Outages and/or Get Status for Data Holders and other mechanisms for the CDR Register.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

Recommendation 17

> *Provide (or link to) a single, complete, set of instructions for certificate validation.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Support Guidance Documentation

Rationale
Noting that the responsibility for this recommendation is with the ACCC, they have indicated a willingness to work with their certificate partners to improve guidance in this area.

Feedback Received
No direct community feedback was received for this recommendation. Feedback did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 18

> *Revise Certificate Validation document to remove duplication opting for the first two paragraphs. The duplicates (latter two) contain a contradiction in themselves. If the certificate status services are available 24x7 without interruption there cannot by definition be times when they are unavailable.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Support Guidance Documentation

Rationale
The current knowledge base support article, from March 11 2021, is ambiguous and requires updating in order to provide clarity.

Feedback Received
No direct community feedback was received for this recommendation. Feedback did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 19

The above quoted section should clarify the following:

- *The exact list of endpoints requiring MTLS is presented in the Security Endpoints section.*
- *MTLS is only required for DH-hosted endpoints and Register-hosted end- points which require authentication.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request

Rationale
With the inclusion of the CDR Register Data Standards within the Consumer Data Standards, ambiguity has arisen. The Certificate Management section of the Data Standards should be updated in order to provide clarity for implementers where MTLS is required.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

Recommendation 20

From the Data Standards, Security Profile, Transaction Security:

> **Use of MTLS**
>
> All back-channel communication between Data Recipient Software Product and Data Holder systems MUST incorporate, unless stated otherwise, **[MTLS]** as part of the TLS handshake:
>
> - The presented Client transport certificate MUST be issued by the CDR Certificate Authority (CA). The Server MUST NOT trust Client transport certificates issued by other authorities.
> - The presented Server transport certificate MUST be issued by the CDR Certificate Authority (CA). The Client MUST NOT trust Server transport certificates issued by other authorities.
>
> End points for transferring CDR Data that are classified as not requiring authentication do not require the use of **[MTLS]**.

The word "endpoints" in the above quote from the Certificate Management section is a link to a non-existent fragment #end-points. This should likely lead to the Security Endpoints section, which has the correct fragment #security-endpoints.

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request

Rationale
The section quoted in the report is actually from the Transaction Security section (above), not Certificate Management. Although this section from Certificate Management (below) contains the broken link in question.

Issued by the Register CA for Data Recipients

Certificate	Function	Notes
Client Certificate	Secures the following: - Consuming Register APIs - Consuming Data Holder APIs	
Server Certificate(s)	Certificate is issued to a FQDN. Secures the following: - Revocation endpoint - CDR Arrangement Management endpoint - JWKS endpoint	ADRs may choose to secure their endpoints with an the Register CA issued certificate or a certificate issued by a public CA.

Where both sections mention "endpoints", however, these should link to the Security Endpoints section of the Data Standards.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

Recommendation 21

> *The documented JWKS and OpenID Provider Config endpoints and the equivalent endpoints in the production Register API should be aligned, such that the documented endpoints are valid in the context of the production API.*

Response
The DSB endorse the Chair accepting an alternate change.

Specifically:

- The ACCC operates two JWKS endpoints for two specific purposes. The URIs for one of these JWKS endpoints is not discoverable based on how the Data Standards currently document the URI.

Change Process
Maintenance Iteration Change Request

Rationale
The Register standards define one MTLS base URL and one TLS base URL. It does not include the "/idp/" prefix that the operator of the CDR Register utilises in production. In actual fact, there are two MTLS base paths and two TLS base paths. A Change Request is required to remove this

ambiguity and clearly document all four base paths and how they map to all CDR Register hosted endpoints.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 22

> *This process is derived from the Open Banking UK registration profile, which itself extends the OAuth 2.0 Dynamic Client Registration Protocol. As the RFC specifies that Registration requests must use the application/json content type [OAUTH-DCR, s3.1] while the approach taken by OBUK and the Data Standards requires the use of a application/jwt content type, it is not clear that this is a valid extension of the RFC.*
>
> *Consider an approach which is a valid extension of the RFC while also providing a signature on both the SSA and the data from the ADR. One such approach may be to require that the request object is presented as a raw JSON object which contains two fields: the software_statement field defined in the RFC [OAUTH-DCR, s3.1.1] and already used by the Data Standards, and another field containing the signed JWT from the ADR with the addition of a new subfield ssa_hash, which contains a hash of the SSA it accompanies.*
>
> *This approach would allow the signatures to be verified in order and the processing to be immediately abandoned on a failed verification, while also pre- serving the binding between the SSA and ADR's JWT through the use of the ssa_hash.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
A future Decision Proposal about the FAPI 2.0 Uplift

Rationale
This change would improve the inspection of the Software Statement Assertion (**SSA**) and follow best practice, as is required by the Rules. Holistic uplift of the CDR Register is anticipated to support cross-sector data holders and Action Initiation. This DP would be consulted on in the holistic consultation for version 2 of the CDR Register.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 23

> *In consultation with ACCC, specify procedures (whether electronic or human-mediated) for authorisation state transitions. The transition from Revoked or Suspended back to Active is particularly challenging, because the decision to Revoke may have been motivated by credential compromise.*

Response
The DSB endorse the Chair accepting this recommendation.

Clear guidance will be developed in conjunction with the ACCC and update any state machines where movement between states is not possible based on the regulator's implementation.

Change Process
Maintenance Iteration Change Request and Support Guidance documentation.

Rationale
Feedback from the ACCC indicated that:

> *Decisions about the status of accredited data recipients are made by the ACCC in its capacity as the Data Recipient Accreditor. The processes for surrender, suspension and revocation of accreditation are specified in the CDR Rules, at rules 5.17-5.21.*
>
> *Further, the independent health check states that 'For example, Data Recipients may transition among Active, Suspended, Revoked, or Surrendered states.' However, we note that once a data recipient's accreditation has been surrendered or revoked they are unable to transition back to active.*

Without encroaching on the ACCC's responsibilities, it is recommended that the standards defining the state machine for accredited data recipients clearly reflect the state transitions that are enforced. Additional guidance may be offered through support channels such as the CDR's Zendesk knowledge base.

Feedback Received
No direct community feedback was received for this recommendation. Feedback did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change. The ACCC has responsibility for maintaining the status of data recipient accreditation. The processes for surrender, suspension and revocation of accreditation are specified in the CDR Rules, at rules 5.17-5.21.

Recommendation 24

Recommend that FAPI restores the requirement for refresh tokens to be sender constrained. In the meantime, specify explicitly that refresh tokens should be sender constrained.

Response
The DSB endorse the Chair **does not** accept this recommendation.

Change Process
NIL

Rationale
Recommendations 24 to 27 all relate to changes being made by OIDF to the FAPI standard. The DSB does not endorse these changes, but does endorse recommendation 28, which was made in the event that these changes to the FAPI standard were not made.

Whilst the DSB can comment on change requests and raise change requests to the FAPI working group, it cannot adopt a recommendation to force the FAPI working group.

It is noted that a change request (Issue #523) was created with the FAPI working group. The outcome of this change request was that refresh token cycling is not required by FAPI.

This issue has been discussed extensively by the FAPI working group including:

- Issue 523: Rotation of Refresh token - Compromised client highlighted by AU - CDR Independent review.
- Issue 456: Proposal - should we remove support for refresh token rotation from FAPI 2.0 (one of the drafts)
- Issue 306: Add refresh token rotation clause and note

Further to this, the DSB consulted on removal of refresh token cycling with the migration to FAPI 1.0 Final. The outcome, based on community feedback, was to remove refresh token cycling because of the direct consumer experience impacts that were occurring in the ecosystem when loss of refresh token occurred. Further information on this issue can be found here:

- Decision Proposal 209 - Transition to FAPI 1.0 Advanced Profile
- Standards Maintenance Issue #219: Allow retrieval of current refresh_token by arrangement ID
- Standards Maintenance Issue #175: Premature Completion of Consent (Hybrid) Flow

Feedback Received
Feedback was received by the OIDF indicating the security requirements quoted by the Health Check relate to public clients. As such, they are not applicable to the confidential clients adhering to FAPI.

OIDF feedback suggested that the combined used of private_key_jwt client authentication or MTLS client authentication provide sufficient proof of possession at the Token endpoint when exchanging the refresh token for an access token. Beyond this, the view was that additional sender-constrained token requirements are not required for confidential clients.

Recommendation 25

Define how certificate expiration will be handled by the MTLS sender-constrained tokens. Update specifications as necessary in terms of what should be being checked during verification and how it is to be used to enforce the sender constraint.

Response
The DSB endorse the Chair **does not** accept this recommendation.

Change Process
NIL

Rationale
Recommendations 24 to 27 all relate to changes being made by OIDF to the FAPI standard. The DSB does not endorse these changes, but does endorse recommendation 28, which was made in the event that these changes to the FAPI standard were not made.

Feedback Received
The OIDF provided feedback that for confidential clients, no standards defined a method for sender constraining a refresh token other than (as FAPI 1 Advanced does) using OAuth client authentication. Further, the OIDF indicated that the "*'simple' approach of binding it as is done for public clients, using the method in https://datatracker.ietf.org/doc/html/rfc8705#section-7.2 results in the client losing all consents if it rotates its keys, as it is no longer able to use the refresh tokens that were bound to the old key. (So for confidential clients, FAPI 1 has never defined any interoperable way to practically sender constrain refresh tokens, other than OAuth client authentication).*"

Recommendation 26

Recommend that FAPI re-evaluates the security implications of not performing refresh token rotation if a confidential client is compromised.

Response
The DSB endorse the Chair **does not** accept this recommendation.

Change Process
NIL

Rationale
Recommendations 24 to 27 all relate to changes being made by OIDF to the FAPI standard. The DSB does not endorse these changes, but does endorse recommendation 28, which was made in the event that these changes to the FAPI standard were not made.

Whilst the DSB can comment on change requests and raise change requests to the FAPI working group, it cannot adopt a recommendation to force the FAPI working group.

For further explanation, please see the rationale for Recommendation 24.

Feedback Received
No direct community feedback was received for this recommendation. It is noted that members of the FAPI working group raised a change request for consideration of this change to FAPI.

Recommendation 27

> *If no changes are forthcoming to FAPI, the Data Standard should be consistent with it and only discourage but not prohibit token rotation.*

Response
The DSB endorse the Chair **does not** accept this recommendation.

Change Process
NIL

Rationale
Recommendations 24 to 27 all relate to changes being made by OIDF to the FAPI standard. The DSB does not endorse these changes, but does endorse recommendation 28, which was made in the event that these changes to the FAPI standard were not made.

The DSB has previously consulted extensively on refresh token cycling with the CDR community. It received feedback from the OIDF, data holders and data recipients in support of removing refresh token cycling. Feedback indicated that refresh token cycling was having a direct impact on the consumer experience and that loss of refresh token during cycling orphaned the consumer's consent from the Data Holder's authorisation, thus inhibiting data sharing without a full re-authorisation.

Past feedback also indicated that refresh token cycling was primarily developed for public clients where the additional FAPI security measures for confidential clients did not exist. Because no international standard exists for exchange of refresh tokens to avoid loss of tokens and orphaning of the authorisation, the only path would be a custom standard defined on top of oAuth. Because of the challenges with this approach and the documented consumer impacts in addition to the security measures FAPI provides for confidential clients, it is not recommended to re-introduce refresh token cycling.

Feedback Received
No direct community feedback was received for this recommendation.

Recommendation 28

> *If Data Holders MUST NOT cycle refresh tokens then Refresh Token MUST be issued with an "exp" equal to the sharing duration authorised by the Customer.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request

Rationale
The Data Standards currently include requirements for refresh token expiry prior to September 2022. After September 16th, 2022, the following requirement applies, which is in line with Recommendation 28:

> ***From September 16th 2022 (FAPI 1.0 Migration Phase 2):***
>
> *Data Holders MUST NOT cycle refresh tokens (rotation). In other words, Refresh Tokens SHOULD be issued with an "exp" equal to the sharing duration authorised by the Customer.*

The Change Request will consult on upgrading the "exp" requirement to a "MUST" and to remove historic references to refresh token cycling.

Feedback Received
No direct community feedback was received for this recommendation.

Recommendation 29

> *The CDR [Data] standard should explicitly specify the location of the JWKS used to verify the JWT signature in self-signed JWT client authentication.*

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Maintenance Iteration Change Request

Rationale
Standards Maintenance Issue #552: Make corrections to Register base URLs and indicate the base URL for all endpoints has already been raised to address this issue.

Feedback Received
No direct community feedback was received for this recommendation. Feedback did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

The ACCC is supportive of this change.

Recommendation 30

Consider more detailed specifications for how a consumer can be assured of a binding and detailed receipt for the consents that they have granted, possibly one that uses CDR Arrangement IDs and links a specific collection consent to other ADR consents.

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
A future Decision Proposal – Non-Reputable Authorisation Receipt

Rationale
A Decision Proposal will be developed for cryptographically bound authorisation receipts within the FAPI 2.0 uplift of the CDR. With the introduction of action initiation, the CDR would benefit from a digital receipt of the consent authorisation and actions instructed. This could offer a digital equivalent to a physical purchase receipt as proof of goods as well as offering a non-repudiable statement of the authorisation granted accessible to both the consumer and the ADR.

It is worth highlighting the distinction between the consent (arrangement between the consumer and the ADR) from the authorisation (arrangement between the consumer, the ADR and the Data Holder) that is representative of the disclosure consent obtained by the ADR from the consumer.

Feedback Received
Participant feedback supported the introduction of verifiable consent receipts. Feedback indicated that verifiable consent receipts may be applicable to future use cases such as cross border transactions.

Recommendation 31

Consider making non-security requirements and tradeoffs explicit, in order to allow for concrete analysis of the tradeoffs. If a requirement serves a purpose other than authentication security, make sure that its reason is explained clearly.

Response
The DSB endorse the Chair accepting this recommendation.

Change Process
Noting Paper and a Decision Proposal

Rationale
The DSB intend to incorporate this approach into the Chair's risk management framework, and Data Standards development process.

Feedback Received
No direct community feedback was received for this recommendation. General feedback, however, did indicate support for the recommendations on key management, certificate management, security endpoints, and registry endpoints.

Recommendation 32: Future Independent Health Checks

In accordance with their requirements for risk management, the DSB recommends that the Chair consider regular independent health checks, including:

- Coverage of existing Data Standards or where Data Standards can be made in relation to:
    - ADR Access Arrangements including Outsourced Service Providers, Sponsor/Affiliate arrangements and Principal/Representative arrangements;
    - Multi-user accounts including Secondary Users, Joint Accounts, partnerships, and Nominated Representatives;
    - Disclosure Consents including AP disclosures, Trusted Advisor disclosures, Insight disclosures, and, if introduced to CDR, Business Consumer disclosures;
    - Vulnerable Consumers; and
    - Consumer Experience standards that relate to consent, accessibility, and security.
- The review on completion of consultation and drafting Data Standards incorporating significant changes or evolutions, such as Authentication Uplift, the FAPI 2.0 migration target state, Consent Review, and Action Initiation security framework Data Standards
- That the review occurs before the development of Payment Initiation and Action Initiation Data Standards

Feedback Received
Participant feedback proposed broadening the scope of the next security review to incorporate access arrangements, nominated representatives and vulnerable person scenarios, as well as the accreditation and Register portal security.

Authentication Uplift

Authentication uplift recommendations in this report require consultation. In summary the recommendations include:

- Increase the minimum OTP length to at least 20 bits of entropy (Recommendation 5, Recommendation 8)
- Increase the maximum OTP length (Recommendation 6)
- Require a minimum of Credential Level 2 for data sharing (Recommendation 12)
- Support alternative authentication flows with strong customer authentication including app-to-app authentication (Recommendation 10, Recommendation 13)
- Deprecate less secure authentication flows (Recommendation 10)

The Chair has indicated a Decision Proposal consultation with the community would be conducted on the holistic uplift of authentication. To achieve CL2, at a minimum, Data Holders would be required to use an OTP plus a second factor of authentication (**2FA**) such as biometric or memorised secret such as a PIN code. How stronger customer authentication is phased in whilst deprecating less secure authentication flows for existing Data Holders as well as new sectors would be a key focus of

the Decision Proposal consultation. A pathway that provides incremental improvements to the baseline authentication standards whilst enabling optional adoption of a higher benchmark will support both existing sectors as well as new sectors. This uplift would need to factor in the data sharing obligations of the Telecommunications and Non-Bank Lending sectors as well as foundational uplift in time to support Action Initiation.

Implementation Considerations

The DSB is interested in the likely implementation impacts of adopting these recommendations to existing data recipients and data holders so the DSB can proactively work with the CDR community to deliver important information security uplift in an efficient and effective way.

The DSB recognises that authentication uplift has been supported by the community, and is eagerly anticipated, but that it comes with significant implementation effort. The DSB is interested in what challenges authentication uplift presents both ADRs and DHs, as well as any considerations for implementation.

The DSB also recognises that many smaller changes identified as change requests may be agreed upon with the community individually, but they could benefit from bundling into groups of changes to reduce implementation releases. This may benefit from alignment to FAPI 2.0 migration milestone planning to coordinate Information Security uplift across several phases.

Finally the DSB recognises that the recommendations in this report may have relevance to Data Holders beyond their CDR implementations and be more generally applicable to the uplift of their information security posture. In this respect, there may be existing regulatory requirements or considerations outside the CDR that Data Holders must currently meet, or are seeking to meet, that impact or relate to these recommendations. The DSB is interested in hearing feedback from participants in relation to any relevant adjacent regulations that should be considered in the consultation of implementing these recommendations.

Data Standards Advisory Committee Feedback

This decision document has been reviewed by the Data Standards Advisory Committee (DSAC). The contributions of committee members have been included below as well as a response from the Chair.

Recommendation 3

Comment

Whilst I am not sure this may apply to many banking Data Holders, if a consumer had not originally setup an authentication channel then it should be established not only as a specific CDR channel but one for other authentications required. Else it will become another different process for consumers. This may also be the opportunity to look at app2app authentication.

Agree to conduct research with the suggested notes provided.

Response

Consistency of experience with existing digital channels is an alignment goal for the Data Standards so that consumers have an experience equivalent to the way they interact with the Data Holder today. The DSB agrees that where practical, and where choice is offered to consumers of the authentication channel, this is aligned to the prevailing norms for that Data Holder. These considerations will be factored into the CX research.

Recommendation 6

Comment

Agree with retaining the 6 characters but I believe it will limit choice if more than 6 characters can be used since common mechanisms such as Google /Microsoft authenticators only use 6 today.

Response

Recommendation 5 considers increasing the 'floor' for OTP length. The comments in relation to common authenticator apps was an input into recommending a minimum length of 6 digits be chosen. The endorsement of Recommendation 6 will result in a Change Request being drafted for community consultation that proposes increasing the 'ceiling' for OTP length. Whilst the maximum length for OTPs may increase above 6 digits, this would be a decision for each Data Holder on what is *practical* to set for their customer bases. If a given Data Holder offers an authenticator app to their customers, the OTP length would be determined by the length of OTP that the authenticator app can issue. Selecting a larger OTP for SMS issued OTPs may be more likely.

Recommendation 7

Comment

Consideration as to how feedback is asked/provided regarding security event signals [given sensitive security information may be disclosed].

Supporting of this recommendation in principle though an evaluation on the level of information that DSB wants shared in the eventing by internal security/policy teams would be required to ensure they're comfortable with this. Noting there aren't any 'broadcast/event' mechanisms in the standards at this point, so would need to see how this is achieved.

Response

The DSB appreciates the security considerations when consulting on the sharing of security context in any signalling framework. With the introduction of action initiation, and more specifically, payments initiation, design of a framework to share vectors of trust[3] and threat intelligence will be important to prevent fraud and establish trust in the CDR as a channel for initiation. The DSB has indicated that the framework will be consulted upon as a Decision Proposal. The DSB also recognises that the sharing of threat intelligence and security context to consult on these changes is sensitive for Data Holders and ADRs. The DSB will consider proposals for how engagement with ADRs, Data Holders and vendors will be without disclosing the sensitive information.

Recommendation 9

Comment

While the intent behind implementation of such a feature is understood, it seems like it would impose a significant barrier to participation. It is very similar to the original position on JAMS where joint account holders were unable to share data by default. In this case we're considering blocking all consumers rather than just a joint account banking subset. Given that JAMS was replaced by DOMS with joint account sharing enabled by default, this proposed move seems counter-productive to the desire to increase participation. It would also appear to overlap with secondary user instruction and DOMS functionality. I suspect ADRs would not wish to see a lock feature as it would be a further blocker and a point of frustration for unaware consumers – particularly during early stage CDR awareness and adoption.

Response

The report suggests a CDR Lock that may be applied by default or allow the consumer to toggle CDR permissions on and off. The report also considers the need for a CDR Lock in the context of stronger customer authentication methods being supported by the Data Holder.

The DSB acknowledges that aspects of this recommendation overlap with JAMS and the original provisions for opt-in data disclosure which was later changed to the JAMS opt-out approach. DSAC feedback includes valuable suggestions on how a form of CDR Lock may be achieved.

It was felt that the worthiness of such a measure be considered to determine efficacy, commercial value and consumer protections.

The DSB has proposed this recommendation as adopted be taken up by the CDR Cyber Security Working Group for further consideration. In endorsing the recommendation this is contingent on further analysis including CX research and consultation with the community. This will inform the opportunities for CDR Lock style protections, and where such protections introduce unnecessary friction or barriers to uptake.

Comment

This would introduce more friction at a time when we already know additional upfront selections cause confusion

Response

The DSB has proposed this recommendation as adopted be taken up by the CDR Cyber Security Working Group for further consideration. In endorsing the recommendation this is

[3] Vectors of Trust, https://www.rfc-editor.org/rfc/rfc8485

contingent on further analysis including CX research and consultation with the community. This will inform the opportunities for CDR Lock style protections, and where such protections introduce unnecessary friction or barriers to uptake.

Comment

I would suggest we look at this recommendation in conjunction with similar capability in the Credit Bureaus known as Credit Bans as they appear to be looking to achieve the same outcome around data and preventing access to the consumer's data unless the lock/ban has been switched off. In the Credit Bureau situation, I believe the Credit Ban can be requested by the Consumer and this is initially put in place for 21 days and if another Credit Ban is requested post this, the lock is put in place for 12 months. If we are looking to provide consumers control of their data, then I would support the notion of having CDR Lock/Credit Ban being readily accessible to thew consumer to switch on/off in same vain you can do it nowadays for blocking international transactions on your credit/debit card.

Could potentially link Recommendation 9 with Recommendation 12 and when the consumer removes the CDR lock, they could put in place a Secret word that could become one-aspect of a Multi-Factor Authentication that is noted in Recommendation 12.

Response

Such mechanisms that pause data sharing, CDR authorisations from being initiated or banning interactions with certain data recipients may be considered in the future CX research.

Suggestions to consider how additional secrets may be onboarded for satisfying Recommendation 12 are also interesting and will be considered in consultations for Recommendation 12.

Recommendation 12

Comment

On the surface this makes complete sense – particularly given the current heightened state of anxiety around personal information security. There will be significant impacts on the consent flow, both for DHs and ADRs if more than just an OTP is required at login. This move has already been foreshadowed for certain types of AI actions, but if we are bringing such a change forward now, that could be challenging for many providers. It would be good to understand anticipated timelines for such a change and appetite for a deprecation period.

Combining these two recommendations would no doubt improve the security posture of CDR, but there will be UX and adoption impacts – that's the tightrope we must walk.

Response

The DSB has indicated that the pathway for these changes are CX research and one or more Decision Proposals to uplift authentication standards. The DSB agrees that the holistic uplift of authentication standards for the CDR should consider the context of action initiation as well as the timing of action initiation implementation as well as the introduction of new sectors. The DSB intends to consult on foundational uplift to authentication that will satisfy not just data sharing but also support action initiation. How and when existing methods of authentication are deprecated will be consulted on to elicit community feedback to ensure a practical and managed transition is defined.

Comment

With AI on the horizon research will be essential but at the appropriate time.

Response

The DSB agrees that authentication uplift must be cognizant of the introduction of action initiation. The TSB intends to consult on foundational authentication uplift to support implementation timeframes that work for action initiation as well as the introduction of new sectors.

Recommendation 14

Comment

I would propose more time to seek feedback on items where impacts have not adequately been considered by participants. Realising participants have had opportunity, and that the amount of change and consultations in CDR has been considerable.

My comments for other recommendations where no direct community feedback was received is the same as recommendation 14.

Response

The DSB is grateful for the feedback and agrees further consultation is valuable. In adopting these recommendations, this decision document has identified the appropriate pathway is through a Change Request consultation that will require community input to arrive as an agreed position.

Recommendation 32

Comment

Very supportive of the recommendation to conduct future independent health checks to ensure that we continuing to evolve best practice.

Response

This feedback is acknowledged.

Implementation Considerations

Comment

'Bundling' Changes – with a number of the recommendations looking to commence consultations like DPs or CX research, and new sectors likely to come onboard in the coming year, it would seem sensible to look at how a number of the recommendations could be bundled into single delivery dates. This would be a more efficient approach for all CDR Participants, avoiding multiple rounds of development, testing and deployment. It would also provide greater certainty on standards for new sectors as they go live.

Response

The DSB agrees that the implementation considerations for a variety of these recommendations should be considered together. The DSB will seek feedback on how future dated obligations will be chosen in consultation with the CDR community.