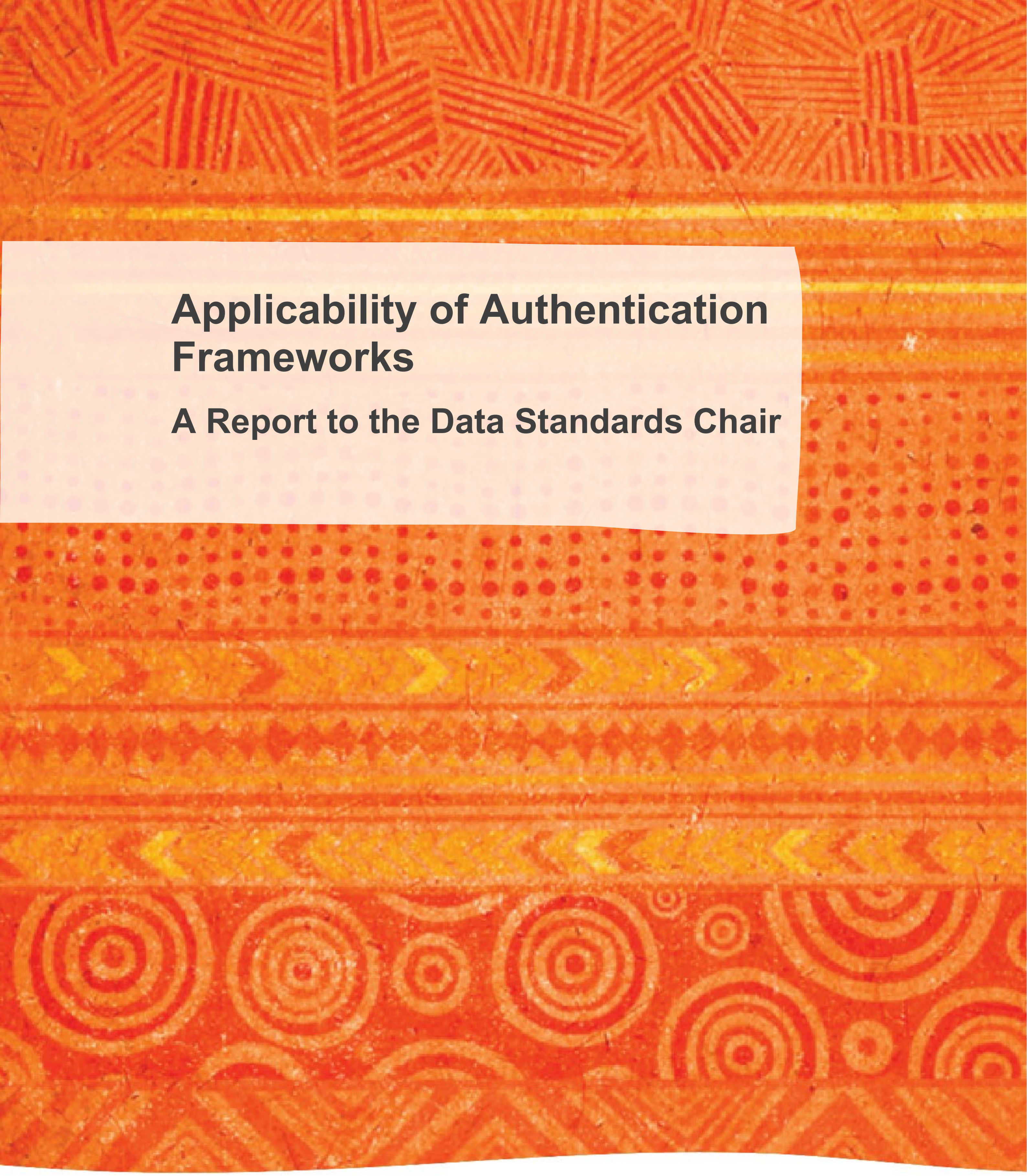
Applicability of Authentication Frameworks

A Report to the Data Standards Chair



PwC Indigenous
Consulting

Disclaimer

This report is not intended to be read or used by anyone other than the Department of Treasury.

We prepared this report solely for the Department of Treasury's use and benefit in accordance with and for the purpose set out in our engagement letter with the Department of Treasury dated 14 December 2022. In doing so, we acted exclusively for the Department of Treasury and considered no-one else's interests.

We accept no responsibility, duty or liability:

- to anyone other than the Department of Treasury in connection with this report
- to the Department of Treasury for the consequences of using or relying on it for a purpose other than that referred to above.

We make no representation concerning the appropriateness of this report for anyone other than the Department of Treasury. If anyone other than the Department of Treasury chooses to use or rely on it, they do so at their own risk.

This disclaimer applies:

- to the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute
- even if we consent to anyone other than the Department of Treasury receiving or using this report.

Liability limited by a scheme approved under Professional Standards legislation.

Purpose Statement

About this report

This report is commissioned pursuant to a Statement of Work between PwC Indigenous Consulting and the Department of the Treasury dated 14 December 2022. This report is specifically tailored to the requirements of the Data Standards Chair (the **Chair**) and is to be read within the context of the Consumer Data Right (**CDR**). A series of bilateral discussions took place over the duration of work, with changes made in consultation with relevant Data Standards Body (**DSB**) stakeholders.

Objectives

The purpose of this report is to consider the applicability of the current authentication framework applied by the Data Standards and compare them with other extant and emerging standards and frameworks in order to determine whether the current situation is fit-for-purpose or opportunities for improvement exist.

The report also considers the recommendation from the 2022 Independent Health Check of the Data Standards “The default Credential Level (**CL**) 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".

Scope of this report

The scope of this report includes:

- outlining the decisions that led to the current authentication framework and currently scheduled improvements
- assessing other leading extant and emerging authentication frameworks and standards and determining potential future considerations for adoption within the Data Standards
- identifying existing data practices and authentication considerations and determining applicability of Data Standards uplift to address deficiencies
- considering the unique use cases presented by the CDR data use scenarios and suitability for standardised approaches to authentication across CDR participants.

Intended audience

The Chair is the primary owner and audience of this report.

Executive summary

PIC notes that the Data Standards' utilisation of open and widely adopted authentication standards was an appropriate direction for the Consumer Data Right (**CDR**). This includes their use for the initial authentication Data Standards, which incorporated key elements and insights from Australia's Trusted Digital Identity Framework (**TDIF)**.

Our review of leading existing and emerging authentication frameworks and standards[1] employed globally found that they are risk-based; and that the Data Standards have adopted a risk-based approach through TDIF, which we consider broadly fit-for-purpose for the CDR.

Concerns were identified, however, with the authentication Data Standards. Firstly there was the question as to who must authenticate, and to what standard, when accessing CDR data. The second concern was on the optionality of authentication methods and factors that can be applied by CDR participants, and in particular the absence of Multi-Factor Authentication (**MFA**) controls.

This optionality is described by a Credential Level (**CL**), which is defined in TDIF as, "the level of assurance or confidence in the authentication process". During our assessment, the Data Standards mandated that authenticators must conform with CL1 for READ operations, and CL2 for WRITE operations, which is also known as action initiation, and includes payments.

Consistent with the recommendation from the 2022 Independent Health Check that the minimum level (i.e., READ operations) in the Data Standards should instead be CL2, however, is the guidance by the Australian Cyber Security Centre (**ACSC**) that MFA should be used by all organisations for internet-facing services[2]; such as the CDR.

For increased levels of threat, the ACSC also provides additional guidance. Although considerations of threat are out-of-scope for this report, the Chair should, however, consider the CDR's threat landscape when making risk-based authentication Data Standards.

CL2 is defined as a strong authenticator, requiring two-factors of authentication (a form of Multi-Factor Authentication), as compared to CL1 that allows a single-factor. The Australian Communications and Media Authority released the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022[3] which mandates the use of MFA for high-risk customer interactions.

PIC recommends that appropriate risk-based MFA methods and options be provided in the Data Standards for any and all access to CDR data where appropriately determined to be commensurate with the anticipated risk of exposure and harm to consumers.

[1] ISO/IEC 29115:2013, NIST SP 800-63-3 and eIDAS Regulation (EU) 910/2014 were identified as the leading authentication frameworks and standards for comparison against the CDR's authentication framework.

[2] Essential Eight Maturity Model https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

[3] Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 https://www.legislation.gov.au/Details/F2022L00548

Summary of Recommendations

Recommendation 1 – Consider uplifting the current Data Standards risk management maturity in order to ensure that risk-based authentication Data Standards remain fit-for-purpose

PIC recommends that the Chair matures the Data Standards risk management capability maturity[4] in order to ensure appropriate levels of assurance requirements are maintained for emerging CDR scenarios and data requirements. The risk management framework guiding these processes and decisions should articulate numerous relevant context including data sensitivity, authentication requirements and known consumer data exposure risks. Assessments of specific data sets for inclusion into the CDR should be made against this risk framework and would determine the minimum-security controls required.

Recommendation 2 – Consider uplifting authentication methods and mandating risk-based Multi-Factor Authentication

In conjunction with uplifting the risk management maturity,[5] PIC expects the current Credential Levels (**CLs**) mandated by the Data Standards would no longer be fit-for-purpose. Consequently, the Chair should consider risk-based assessments that analyse the current and emerging threat landscape, and the potential harms of the respective CDR use cases, and the sensitivity of the CDR data involved.

The authentication flows mandated by the Data Standards outlined approved OpenID Connect authentication flows, which were then further enhanced by the international Financial-Grade API (**FAPI**) standards. The Chair should continue, however, consulting with industry to determine if there are other standards that are appropriate alternatives, which could be leveraged as existing investments made by CDR participants in order to support higher levels of authentication. The Chair should consider allowing optionality to the technologies that can be implemented, either through explicitly noting approved methods or combinations of methods within the Data Standards.

Recommendation 3 – Consider the Chair's requirement to make risk-based authentication Data Standards for consumer access to consumer data hosted by non-Data Holder CDR participants.

The accumulation of consumer data within CDR participants may result in threat actors attempting to access this through provided access channels and controls. Current Data Standards provide guidance around the authentication processes required during consent collection, but do not discuss how consumers should authenticate when accessing these richer data sets held by Accredited Data Recipients and other non-Data Holder Consumer Data Right participants.

The individual data sets may be of various levels of sensitivities, but when combined may well have an increased overall sensitivity, that requires higher levels of assurance to access than is required for a given act of consent under the CDR.

Recommendation 4 – Consider maturing the management of how external standards are incorporated by reference

PIC notes that although the Data Standard incorporates by reference TDIF as its authentication framework, terminology is not consistent between the two. The Chair should consider further adoption of TDIF terminology

[4] Department of Finance, Benchmarking Risk Management Capability https://www.finance.gov.au/government/comcover/risk-services/management/benchmarking-risk-management-capability

[5] Ibid.

within the Data Standards to provide greater levels of consistency between the two frameworks and ensure that ambiguity is kept to a minimum.

Where previous recommendations note updates to the Data Standards, alignment to TDIF terminology can be included within the same discussions and updates for inclusion within the standards.

The same applies to other standards incorporated by reference in the Data Standards.

Recommendation 5 – Consider conducting risk assessments for patterns of authentication to which the current Data Standards do not apply

While other recommendations have primarily recommended strategic uplift of risk-based processes and maturing the Data Standards, PIC recommends that the Chair assess current data use scenarios and consumer authentication patterns to which the Data Standards are not currently applied.

For example, TDIF is not applicable to address consumers wishing to authenticate and interact using physical processes or through non-digital channels, i.e. “offline” consumers. But there are data use scenarios applicable to CDR consumers that must be addressed. Therefore the Chair needs to determine where development of fit-for-purpose risk-based authentication Data Standards is warranted.

Facilitation of onboarding these consumers into the CDR, and the required controls to protect them, has a number of associated risks that deal with privacy, security and further consumer considerations that require detailed assessment. Furthermore, the legislative provisions must be considered and their applicability determined

Contents

1 Overview of the CDR Ecosystem

1.1 The Chair's Duties

In discharging their duties, the Data Standards Chair (the **Chair**) is legally obliged to take a risk-based approach to developing data standards pertaining to the collection, use, accuracy, storage, and security of Consumer Data Right (**CDR**) data. Consequently, the Chair needs to minimise and mitigate risks where possible.

Cyber risk will only continue to increase, proportional to the CDR's continued expansion – both in scope and functionality. These risks will continue to emerge through the aggregation of various data sets, but they can also result from the combination of small but particularly sensitive consumer data sets or sensitive insights.

Under their duties, the Chair must maintain their understanding of current authentication standards and how these compare with extant and emerging trends in order to manage these risks. With fit-for-purpose authentication standards and frameworks in place, consumers can trust that the CDR ecosystem and services will provide them with a seamless and familiar user experience for authentication, while simultaneously protecting their consumer CDR data from unwarranted exposure to unauthorised persons.

As more industries are designated as participants in the ecosystem, and consumers are enabled to have greater control over their data sharing and usage, the amount of interaction points for consumers will continue to grow and having appropriate, risk-based access controls will require a robust process to determine where greater security is warranted.

1.2 Applicability of Authentication Frameworks to the CDR

Organisations and government entities invest in, deploy, and implement various mechanisms to proactively protect, detect and respond to threats. This is done in alignment with regulatory requirements, risk appetite and consumer expectations. One key element to this is that appropriate authentication controls are used to validate that the person attempting to access data or services is the actual individual. These processes introduce a level of friction, however, to the usability and experience of interacting with these services that must be balanced with the associated risks. This balance can be found through an ongoing risk-based approach.

The continued expansion and adoption of CDR services and mechanisms will see consumers shift from expectations of their data being solely managed and enforced by individual organisations to a holistic view of a secure ecosystem comprised of interconnected organisations and participants. Consumers interact not only with Data Holders (**DHs**) but also with Accredited Data Recipients (**ADRs**) in the provisioning of services and transferral of data in support of consumer data requests and activities.

Within the context of today's CDR, this has primarily surfaced as consumer authentication for informed consent and their authorisation to share data, however, the CDR's potential is not limited to this being the only consumer touchpoint where authentication may be applicable.

It is important to understand that authentication security controls could be applied in numerous situations throughout the CDR. However, the scale and scope of whether it should be enforced on certain CDR participants may overreach the expectation of the CDR's Data Standards and would instead be addressed through other existing obligations including the Privacy Act 1988 (Cth), Australian Privacy Principles, professional standards and obligations and industry specific requirements.

Consumers are largely unaware of the distinctions of differing security responsibilities across the CDR and instead may view the CDR as a monolithic service that consistently applies the same security baseline with every participant. Therefore, to ensure that a level of consistency can be applied, while balancing the needs for consumer experience and security requirements, the Data Standards defines the consumer authentication requirements each applicable participant[6] must adhere to.

It is these provisions that this paper aims to address in understanding the applicability of authentication frameworks and standards to the CDR ecosystem and where possible uplift and alignment can therefore be achieved.

[6] Applicable participants are defined within the Consumer Data Right Rules 2020 (CDR Rules)

2 The existing CDR Authentication Framework

Australia's CDR empowers Australian consumers to have greater control and visibility over the usage and sharing of their data between accredited participants and third parties. Fundamental to this scheme is the ability for consumers to provide informed consent to these parties, validating themselves through appropriate authentication controls and authorising the transmission of their data across secure channels. In consultation with industry participants, and designed with consumers in mind, the Data Standards defines a standardised authentication framework that has been adopted across multiple industries.

2.1 Data sharing and digital data capture outside of the CDR

Traditional processes for sharing consumer data between organisations often relies on service providers performing digital data capture (also known as screen-scraping) activities on a consumer's behalf. This is typically achieved through the sharing of sensitive consumer credentials, such as their internet banking password, allowing the provider unrestricted access to the user's account.

When sharing user credentials with service providers, the consumer must trust the provider to only perform the necessary service(s). This direct access by non-account holders could result in actions being performed beyond what a consumer may expect, or had consented to, and introduces additional risks for potential misuse that can lead to fraud. Additionally, the lack of control by the consumer can lead to the establishment of large data sets, that may contain sensitive information and could be utilised for unintended purposes, or simply present an ongoing risk for potential exposure (data breach) and misuse.

Use of the CDR instead reduces this risk by not providing unfettered access to consumer accounts while still supporting the ability to move data between participants. Additionally, consumers provide their informed consent that guides the use and duration this data can be used for.

As an unregulated method for the sharing of consumer data, digital data capture / screen-scraping activities do not provide consumers with the same oversight or known standards for the collection, management and destruction of consumer data that has been aggregated over time.

A summary of the key differences is included below:

Table 1: Differences between Digital Data Capture and CDR data sharing methods

Digital Data Capture	Consumer Data Right (Current)
Unregulated	Established under the *Competition and Consumer Act 2010* (Cth) and the *Privacy Act 1988* (Cth)
Access to data provisioned through sharing of account passwords	Authentication is performed by consumer through standardised mechanisms
No formal time-bound requirements	Consumer consent is provided and is time-bound
Unfettered access to accounts	Data access is limited to defined payloads and consent restrictions
No accreditation process	Accreditation program for CDR participants
No standardised process for data management	Standards for data management, storage, and destruction
Able to screen scrape any available data	Can only be used for designated industries and defined data sets

Digital Data Capture	Consumer Data Right (Current)
Service provider access through consumer front ends and subject to fraud detection and controls	Standardised Application Programming Interface (APIs) used to facilitate data transfers securely and by known CDR participants

2.2 Background and design of the CDR Authentication Framework and Data Standards

Defined within Competition and Consumer (Consumer Data Right) Rules 2020 (**CDR Rules**) 8.11 (1)(c), the Chair must make Data Standards relating to the 'authentication of CDR consumers to a standard which meets, in the opinion of the Chair, ***best practice security requirements***. Currently, the CDR has primarily enabled the secure transmission of consumer data between CDR participants beholden to the Data Standards. The Data Standards outline the authentication and informed consent workflow that consumers must follow.

For this the Data Standards outline[7] the use of OpenID Connect Core 1.0 (**OIDC**)[8], supported by the OAuth 2.0 Authorization Framework (**OAuth 2.0**)[9] to facilitate the secure disclosure of consumer data from DH to ADRs[10]. These protocols are further enhanced by FAPI[11] requirements.

This approach has enabled CDR participants to provide consistent consumer-centric experiences across the ecosystem, collecting consent, authenticating consumers, and authorising data sharing requests using secure methods that are widely adopted globally. The adoption of popular standards also promotes the CDR for potential future expansion because of the likelihood that new participants would be aligned with them.

As the CDR continues to expand and includes more industries across the Australian economy, current designation instruments have been registered for Authorised Deposit-taking Institutions (Banking), Energy, Telecommunications (Telco) and Non-Bank Lender sectors. Banking and Energy sector data standards are currently being enforced while Telco standards are still under consultation.

Consistent across all industries is the need for consumers to provide informed consent, authenticating themselves and authorising the disclosure of their consumer data. This authentication and authorisation process is outlined within the Data Standards and utilises supported authentication flows[12] including OIDC Hybrid Flow[13] and Authorization Code Flow[14].

The authentication of consumers with their DHs to disclose their data, where appropriate consent has been provided, in both approved authentication flows requires the use of one-time passwords (**OTPs**) delivered through existing channels or mechanisms that the consumers should already be familiar with to reduce unwarranted friction (i.e. SMS communications to the consumers previously defined mobile numbers or pre-established authenticators). The current Data Standards disallow the usage of existing password authentication mechanisms, also known as memorised secrets. This provides several benefits to help drive adoption of CDR services including:

- ensuring a consistent authentication experience for consumers between various DHs
- reducing the need to setup and activate digital accounts with passwords before attempting to authenticate, leveraging existing known consumer details held by DHs

[7] https://consumerdatastandardsaustralia.github.io/standards/#security-profile

[8] https://openid.net/specs/openid-connect-core-1_0.html

[9] https://datatracker.ietf.org/doc/html/rfc6749

[10] https://consumerdatastandardsaustralia.github.io/standards/#cdr-federation

[11] https://openid.net/wg/fapi/

[12] https://consumerdatastandardsaustralia.github.io/standards/#authentication-flows

[13] https://openid.net/specs/openid-connect-core-1_0.html#HybridFlowAuth

[14] https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth

- minimising usability concerns related to remembering or resetting passwords (something they need to know).

This option was selected based on extensive consultation with CDR participants[15] [16]. These same requirements may also restrict DHs from enforcing existing authentication controls, even where the DH would normally seek to apply other more secure authentication controls (such as Multi-Factor Authentication (**MFA**)). DHs currently employ more secure and sophisticated authenticators and authentication flows compared to the CDR.

The Data Standards also require DHs to utilise approved authenticator methods to ensure that appropriate Levels of Assurance (**LoA**)[17] are met. These levels are used to determine the "degree of confidence in the processes leading up to and including the authentication process itself"[18] and provide assurances that the individual authenticating is an appropriate user of the account being authenticated against.

The Data Standards' security profile currently uses Credential Level 1 (**CL1**) from the Trusted Digital Identity Framework (**TDIF**).[19] While TDIF contains multiple authenticator options for CL1, these are options that are constrained by the Data Standards specifying the use of OTPs. By ensuring that authentication flows utilise the approved authentication methods and processes, a resultant LoA of 2 can be achieved to provide assurances that the appropriate consumer is authorising the transaction, and this is required for all READ operations where consent is collected in the CDR.

The Data Standards also defines Credential Level 2 (**CL2**) from TDIF for WRITE operations on consumer data also known as action initiation. This functionality is yet to be utilised within the CDR.

2.3 High level deficiencies and considerations

While the Data Standards outline security requirements and authentication standards that have been successfully adopted across the CDR ecosystem, they do not contemplate security of consumer data in emerging and future data use scenarios. Some of these use cases have already surfaced and include:

2.3.1 CDR authentication currently focusses on consent collection

As consumer data continues to transfer between CDR participants, data sets will aggregate. This aggregation poses a greater cyber security risk.

Consumers are empowered to provide informed consent for ADRs to collect only the necessary data, reducing the accumulation of unnecessary data, and this is primarily secured behind a standardised consumer authentication process. The existing CDR authentication framework is primarily focused on the initial authentication process for consent collection and authorisation of data sharing. This minimises friction and encourages a consistent user experience.

The current process does not assess the risk associated with combining the requested data with any pre-existing data sets that may have already been collected. Nor does the authentication process apply to accessing insights or raw data gained through the aggregation of consumer data. Considerations must be given to new scenarios that are emerging as the CDR continues to evolve.

In addition to aggregation, the sensitivity of action initiation data use scenarios may require elevated levels of controls proportionate to the potential harm to consumers.

[15] https://github.com/ConsumerDataStandardsAustralia/standards/issues/35

[16] https://github.com/ConsumerDataStandardsAustralia/standards/issues/62

[17] https://consumerdatastandardsaustralia.github.io/standards/#levels-of-assurance-loas

[18] ISO/IEC 29115:2013, Section 6 Levels of assurance

[19] https://www.digitalidentity.gov.au/tdif

The Data Standards also does not currently specify the minimum authentication controls that should be enforced by other CDR participants, such as ADRs, Trusted Advisor and Third Parties or include provisions for consumers to access their own data. Such access controls should be risk-based and assessed appropriately.

2.3.2 Authentication controls are static

The Data Standards outline only two levels of authentication controls, one for READ operations (CL1) and another for WRITE operations (CL2)[20]. Replacing this broad approach with risk-based assessments for specific data sets and data use scenarios would enable the Data Standards to specify a minimum set of applicable risk-based security controls to be enforced or establish a consistent baseline to which specific controls could be applied.

This would also enable participants to implement risk-based authentication controls. These would be derived from a risk-based understanding of data sensitivities and the impact to consumers and organisations if the data were breached. In uplifting existing risk management processes and assessments of the sensitivity of CDR Data across the ecosystem, incorporating the consumer authentication related risks into these processes will help determine the granular applicability of LoAs / CLs to protect consumer data better and prepare for future data use scenarios.

2.3.3 Authentication flows disallow more secure authentication methods

The use of only OTPs for authentication, without other controls in place, is less secure than existing authentication methods employed by some CDR participants and has independently been assessed to no longer be a best-practice method of authenticating consumers[21] [22]. The Data Standards prohibit the use of Multi-Factor Authentication (**MFA**) in the current regime.

Ostensibly, this is in order to maintain a simple and replicable experience to all consumers across all CDR participants, which has been declared by Treasury as facilitating adoption through minimal overhead friction. However, this is not reflective of current authentication methods enforced by individual CDR participants within their own (non-CDR) service offerings. In line with previous observations, appropriate levels of authentication to secure access to data methods could be defined and adopted if a risk-based approach were implemented, considering sensitivities of the data being accessed and the risk associated with transacting on the data.

2.3.4 CDR usability and offline consumers

The current authentication requirements to provide informed consent mandates the use of OTPs and must be paired with a known unique identifier belonging to the consumer. The adopted approach aims to maximise the ability for consumers to interact with CDR services and has been designed to encourage adoption through ease of use and repeatability across participants. Adoption of more complex digital authentication methods may hinder consumers from interacting with the CDR ecosystem, due to digital literacy, personal circumstance and / or cultural or social backgrounds and characteristics.[23]

Offline consumers are of particular concern for the CDR's expansion of authentication requirements[24] as the consumer experience, digital and cyber security maturity of some existing and potentially new industries that are designated for inclusion will vary. Alternative authentication flows to the redirect with OTP approach and restriction of allowed authenticator methods may not be feasible for all consumers. Additionally, the opportunity to encourage adoption of the CDR is hindered should changes become too restrictive for consumers.

Any changes to the authentication framework should consider how to cater to these consumers, to ensure they can seamlessly access CDR services and increase inclusivity, while attempting to improve on existing non-secure

[20] https://consumerdatastandardsaustralia.github.io/standards/#levels-of-assurance-loas

[21] https://github.com/ConsumerDataStandardsAustralia/standards/issues/258

[22] https://github.com/ConsumerDataStandardsAustralia/standards/issues/280

[23] https://github.com/ConsumerDataStandardsAustralia/standards/issues/279

[24] https://github.com/ConsumerDataStandardsAustralia/standards/issues/296

processes that the CDR aims to replace. In addition to considering authentication mechanisms and processes, the industry specific data sets that are in scope of the CDR should consider whether an appropriate LoA and associated authentication mechanism can feasibly be mandated and affect consideration for inclusion within the CDR, or if less secure authentication methods can be utilised for low-risk transactions only.

2.4 Scheduled improvements and future practices

While several high-level observations have been identified and should be considered, the Chair is already in the process of assessing and improving on existing processes in consultation with industry. Key scheduled improvements and consultations of note include:

- Alignment of Authentication Flows to FAP 1.0 requirements, enabling the use of Authorization Code Flow and retirement of OIDC Hybrid Flow[25]
- Ongoing CX Research and Authentication Reviews, covering consent collection[26], accessibility improvements[27], authentication CX uplift[28] and offline consumer interactions[29]
- Development of a Data Sensitivity Model to inform the Data Standards Chair's risk management framework
- Various recommendations adopted by The Government as outlined in "Government Response to the Inquiry into Future Directions for the Consumer Data Right"[30] and largely categorised into the following authentication related topics:
  - Action initiation framework and Action Initiation processes (associated authentication requirements)
    - Payment Initiations, fine grained authorisations, and specific actions authorisations
    - More explicit requirements for accredited persons to authenticate customers
- Interoperable authentication solutions

Minimum assurance standard for authentication (including risk taxonomy).

[25] https://consumerdatastandardsaustralia.github.io/standards/#future-dated-obligations

[26] https://github.com/ConsumerDataStandardsAustralia/standards/issues/273

[27] https://github.com/ConsumerDataStandardsAustralia/standards/issues/279

[28] https://github.com/ConsumerDataStandardsAustralia/standards/issues/280

[29] https://github.com/ConsumerDataStandardsAustralia/standards/issues/296

[30] https://treasury.gov.au/publication/p2021-225462

3 Key insights into existing and emerging Authentication Practices

The Data Standards have adopted a risk-based framework using TDIF. This has been done in consultation with industry participants. The authentication requirements are contained within the Security Profile; however, these only leverage certain aspects of the TDIF. The adoption of this framework helps prepare the CDR for potential future integrations with TDIF accredited parties and digital IdPs.

Whilst there is merit in maintaining this alignment, the TDIF itself also leverages aspects of international authentication standards and updates to TDIF may be delayed as changes to these international standards require detailed assessment and eventual implementation. Continued updates to international authentication standards and frameworks warrant exploration to identify if key insights and behaviours could be adopted by the Data Standards to enable future innovations, prior to them included within the TDIF or otherwise.

PIC has assessed the Data Standards Security Profile against existing and emerging authentication frameworks including ISO/IEC 29115:2013, NIST SP 800-63-3 and eIDAS Regulation (EU) 910/2014 and identified that broadly speaking, each of them have core commonalities. A key feature of these frameworks, mirrored by TDIF, is the use of risk-based processes to determine the appropriateness of varying levels of authentication controls and determining the applicability of them to data use scenarios. Detailed within Appendix A is a breakdown of this assessment and mature examples of how this approach could be applied in practice (NIST SP 800-63-3 AAL Decision Tree, Page 33).

In support of these risk-based assessments, PIC has also identified a number of applicable leading standards and frameworks relevant to sensitivity analysis and broader risk management practices (Appendix B). They can be used in conjunction with other risk factors and indicators to inform the risk assessment process better and include greater insights that can be used to determine suitable security control requirements that the Chair may wish to consider in a matured risk-based approach to authentication.

It is important to note that while working towards maturing the risk-based processes and building on from insights found in this section, various risks and factors would need to be contextualised for the unique CDR use cases. Leveraging these international risk and sensitivity frameworks initially, which are interoperable and widely adopted, and therefore are broadly applicable to the CDR as a whole, should be considered.

In order to use TDIF effectively in a risk-based way, it is necessary for the Chair to determine the risk associated with data use scenarios and the consequences of potential data breaches. They can leverage the above identified frameworks and processes and other TDIF specific elements such as the Identity Proofing (IP) levels as found in Table 2 below. Initially the Chair should use the table provided in the TDIF policy document, but as the Chair further develops their risk management framework, this framework should further augment their decision making.

The IP levels are as follows:

Table 2: TDIF Identity Proofing Levels Intended Uses

IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
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.

Once the Chair has determined the level of risk, and if a corresponding IP level is required, this decision then translates into the corresponding Credential Levels (**CL**s) permitted by TDIF.

Table 3: TDIF Identity Proofing Levels Approved technical credential bindings

IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
CL1 / CL2 / CL3	CL1 / CL2 / CL3	CL2 / CL3	CL2 / CL3	CL2 / CL3	CL3

TDIF Credential Levels provide a list of permitted credential types, or authentication methods, as follows, that can be defined within the Data Standards as permitted authentication methods :

Table 4: TDIF Credential Levels Permitted Credential type combinations

CL1	CL2	CL3
ONE OF: • Memorised Secret [31] • Look-up Secret • Out-of-Band Device • SF OTP Device • SF Crypto Software • SF Crypto Device • MF OTP Device • MF Crypto Software • MF Crypto Device	**ONE OF:** • MF OTP Device • MF Crypto Software • MF Crypto Device. **OR** Memorised Secret AND ONE OF: • Look-up Secret • Out-of-Band Device • SF OTP Device • SF Crypto Software • SF Crypto Device	• MF Crypto Device **OR** • SF Crypto Devices AND Memorised Secret **OR** • SF OTP Device AND MF Crypto Software **OR** • SF OTP Device AND MF Crypto Device **OR** • SF OTP Device AND SF Crypto Software AND Memorised Secret

As the Data Standards currently only allow a Single Factor OTP, this only meets CL1 and "provides a low level of confidence that the Individual controls a Credential bound to their Digital Identity", which TDIF reserves for only very low risk and low risk transactions (IP1 and IP1 Plus). Additionally, as the Chair reviews this risk-based decision, the Chair needs to account for two additional matters:

1 **First**, the CDR has taken a policy position that passwords will not be used in order to ensure the CDR is not an additional burden to the phishing attacks on internet banking passwords. Consequently, all memorised secret options are not applicable from the above CL table. These have been highlighted in grey

2 **Second**, the Australian Cyber Security Centre (ACSC) advises that, "MFA [should be] enabled by default for an organisation's non-organisational users (but they can choose to opt out) when they authenticate to the organisation's internet-facing services." Although for higher threat levels, the ACSC provides further advice. Implementing MFA through the Data Standards would mean selecting at least CL2, which is described by TDIF as being for moderate risk transactions (IP2).

Consequently, the Chair will need to consider the current cyber security threat level, and the data sensitivity, in order to decide on a proportionate risk-based authentication Data Standard. This decision should be supported by a capability that constantly monitors the environment for change. Fraud risk is clearly also a factor in this decision and should therefore also be monitored constantly.

[31] Due to the current restriction on memorised secrets allowed within the Data Standards, various authentication methods and combinations are not permitted and these are highlighted in grey appropriately

3.1 Comparison to existing and emerging authentication frameworks and standards observations

Leading existing and emerging authentication frameworks and standards, including ISO/IEC 29115:2013, NIST SP 800-63-3 and eIDAS Regulation (EU) 910/2014, were assessed to determine whether the Data Standards Security Profile's approach to authentication and adoption of TDIF requirements aligned with current trends or if additional insights should be considered.

Analysis has identified that the Data Standards' approach is in principle, largely aligned with these frameworks core elements to authentication, though CDR specific use cases and historical design decisions are applied to the current implementation. A summary of the key behaviours has been included below and further details can be found in 6.5 Appendix A.

Table 5: Authentication frameworks and standards observations

Authentication Topic	Data Standards Security Profile	ISO/IEC 29115:2013	NIST SP 800-63-3	eIDAS Regulation (EU) 910/2014
Levels Of Assurance (LoA)	Two LoAs (Level 2 and Level 3). Relates to authentication and the establishment of consent.	Four LoAs (Low, Medium, High, and Very High). Requires both sufficient identity proofing and authentication requirements to achieve higher levels.	Splits LoAs into three distinct categories covering identification, authenticator, and federation assurance levels. Three Authenticator Assurance Levels (AAL1, AAL2 and AAL3)	Three LoAs (Low, Substantial and High). Requires both sufficient identity proofing and authentication requirements to achieve higher LoAs.
Selection of Assurance Levels	READ and WRITE data use scenarios are associated with LoA 2 and LoA 3 respectively. Inclusion of payloads and endpoints is determined based on a risk-based approach initially and access is aligned to the defined LoAs.	Recommends alignment with organisational approach to managing residual risk. Use an approved risk-based assessment process and associated and relevant risk criteria.	Provides a risk-based process flow to select appropriate AALs to enforce. Combine with context specific risk frameworks and align with organisational and consumer needs.	No specific regulation-based framework for the alignment of LoAs. Allows organisations to define their own risk appetite and attempts to access services must adhere to minimum levels defined.
Permitted Authenticator Types	LoA 2 and LoA 3 are mapped to Credential Level 1 (CL1) and Credential Level 2 (CL2) of TDIF respectively.	Guidance is provided to determine where appropriate authentication methods are sufficient for different LoAs (i.e., MFA required for LoA 3 and LoA 4, cryptographic	Detailed list of permissible authenticators is provided per AAL along with combinations of authenticators that can be used for MFA purposes.	Provides a basic framework to identify appropriate controls relative to the applicable assurance levels.

Authentication Topic	Data Standards Security Profile	ISO/IEC 29115:2013	NIST SP 800-63-3	eIDAS Regulation (EU) 910/2014
	Permitted authenticators are further restricted by the approved CDR authentication flows and baseline security provisions detailed within the Data Standards and currently only allow the use of an OTP in conjunction with an account identifier.	authentication methods not required for LoA 1) Specific controls are not outlined for any level and instead requires context to select the appropriate combination to address risks of concern.	Provides additional context and restrictions on some factors that are seen as higher risk and require additional controls (i.e., using out-of-band verifiers with communication over the public switched telephone network).	Defines the minimum authentication method requirements but does not specify specific technologies to use for the various levels.
Other considerations	Security Profile authentication requirements are derived from TDIF, which in turn is built upon NIST SP 800-63-3.		Revision 4 of NIST SP 800-63 is currently out for public consultation and has an increased focus on reducing risk for consumers. Major authentication relevant additions include equity considerations and greater guidance and outlined processes for Digital Identity Risk Management which are detailed in 6.5Appendix A.	

3.2 Consumer Data Standards terminology and alignment to reference frameworks

Assessing the Data Standards' Security Profile and defining the baseline authentication framework characteristics for comparisons identified several general observations for improvement that could be made to align to TDIF better and provide greater clarity to CDR participants. These were not assessed against the other frameworks but instead were noted as potentially requiring additional attention and consideration for uplift:

- The Data Standards reference TDIF authentication credential requirements while defining LoAs but do not align in terminology in various areas. Adopting TDIF terminology within the Data Standards would provide better consistency between dependent frameworks and references and reduce ambiguity of expected requirements. Examples of such terminology differences include:
  - TDIF outlines the Credential Types that are supported with the associated constraints while the Data Standards identifies these as authenticators
  - Data Standards baseline security provisions reference the disallowance of 'passwords', however TDIF instead refers to this same credential type as a 'memorised secret'.
- The Data Standards currently provides various normative references including to TDIF and outlines the relevant version (April 2019). However, TDIF has undergone further revisions since this date and contains follow-on references that may not be dated. The Data Standards should be reviewed and against these updated references and standards on a frequent and scheduled basis while also outlining where follow-on reference requirements are adopted within the Data Standards for clarity and standardisation. Examples include:
  - The Data Standards currently references the third iteration of TDIF (released April 2019) while the fourth iteration was released in May 2020 and has since been updated to release 4.8 and last published in February 2023
  - Various credential types outlined within TDIF make references to the security strength specified in the latest version of the Information Security Manual (**ISM**)[32] and could lead to various versions of controls being enforced throughout the CDR ecosystem.

3.3 3.3 Risk-based approaches

A common observation among all the assessed authentication frameworks was the usage of a risk-based approach to determine appropriate assurance levels that should be enforced as part of the authentication processes. Although the various frameworks called out different approaches to performing this risk assessment, key similarities include:

- Developing an understanding of the risks of incorrectly applied authentication processes for given scenarios to consumers, organisations and other relevant parties. Risks would need to be considered within the wider context of organisational risk management, but also the consumer harm that may eventuate, as well as reputational damage to the CDR
- Defining the risks in the context of the intended data use scenarios if incorrectly applied to assess the importance of applicable minimum authentication controls required
- Appropriate documentation of assurance levels, with guidance to the intended usage of each level, to enable future integration with other models and frameworks
- Providing optionality, either through outlining specifically allowed authentication methods, or minimum expectations of authentication controls (i.e., cryptographic methods, MFA) within each assurance level without mandating one specific method over another.

The CDR is comprised of a distributed network of participants, and each has their own existing risk management processes, data classification guidelines and minimum organisational security controls. Integrating and standardising controls between them presents unique challenges to achieve alignment and must be considered for any centralised authentication framework to operate. These challenges include:

[32] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

- Uplift of existing CDR risk management capability in order to implement risk-based authentication controls for all CDR data use scenarios
- Developing consistent data classifications and sensitivity ratings across all applicable data sets and data use scenarios to inform privacy impact and risk assessments and standardisation of minimum-security control implementations to protect CDR data
- Mapping of data use scenarios (including collection of sensitive and non-sensitive information or action initiation) to required LoAs that can be enforced by CDR participants
- Aggregation of large data sets, that may be exposed to consumers, could fall under the authentication framework as risk of exposure may be high, or require de-anonymisation before being exposed. While it is expected that individual smaller data sets from DHs could be assessed to be low risk, combinations of data sets from multiple DHs, potentially from different industries, could be aggregated and conceivably be considered higher sensitivity (consumer spending habits combined with communication data and other behavioural insights to form a holistic representation of an individual) that may require stronger authentication controls to secure
- Supporting stronger authentication methods than the current OTP flow, extension of authentication flows to support additional use cases (Single Sign-On etc.) and considering how to cater for approved offline consumers scenarios without compromising on security
- Consistency of applied data sensitivity classifications between CDR participants and monitoring of approved authentication methods being enforced across the ecosystem commensurate with the exposure risks being protected against
- Adoption of updated standards across all CDR participants, extending on the coverage of existing authentication requirements and data disclosure authorisation processes.

3.4 Global trends in authentication and best practices

Upon reviewing the leading authentication frameworks and relevant published research, several common trends emerged. These are the following four categories:

1. Consumer data theft and fraud
2. Enabling MFA
3. Adoption of biometrics and alternative authenticators
4. Federated access to services.

3.4.1 Consumer data theft and fraud

Authentication is a primary security control used to provide assurances to organisations and entities that the persons attempting to access consumer details and accounts are as intended, and to protect against fraud. CDR data would be a prime target for fraud and could be viewed as increasingly lucrative due to the aggregation of sensitive information across CDR participants, spanning an increasing number of industries. This is compounded by the possibly varying levels of maturity of security controls between these industries and individual participants. Once data is breached, consumers are at risk of becoming victims to identity theft and other types of fraud.

The Australian Bureau of Statistics report into Personal Fraud[33] for the 21/22 financial year contained key insights related to consumer security and fraud. The report noted an estimated 0.8% (159,600) of Australians were victims of identity theft within that financial year alone. This was the same rate found for the previous year (20/21). Stolen personal information was primarily used to obtain money from bank accounts and other financial services. Second to financial service fraud was the usage of personal details to open new accounts for both utilities and phone services. Additionally, 2.5% (509,500) of Australians were found to be the victim of online impersonations whereby their personal details were misused by fraudulent actors to impersonate them online or over the phone.

[33] https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2021-22

Authentication controls must be enforced consistently and holistically across all participants of the CDR ecosystem where CDR data exists to prevent against these risks and reduce the likelihood of harm to Australian consumers. Unintended exposure of consumer data from any participant would also damage the reputation of the CDR ecosystem and trust in the regime.

3.4.2 Enabling MFA

The leading frameworks all recommend the use of risk-based approaches to determine the appropriate LoA and authentication challenge(s) (factor(s)) required for any data use scenario and enable organisations to understand whether the potential impact of consumer data exposure warrants the need for additional security. Depending on the outcome of the risk assessments, a level of control can be applied commensurate with the identified risks, and this could require the use of MFA.

Each of the leading authentication frameworks assessed in this report highlight the need to migrate away from single-factor authentication methods and implement MFA for scenarios where even moderate consequences to the consumer may arise if incorrect access is provided. This ensures that an appropriate LoA can be met in line with the expected risk of exposing consumer data, or access to authenticated channels. Issuing authentication challenges to individuals against preconfigured, tamper-proof, and more secure authentication methods ensures that an appropriate LoA can be met in line with the expected risk of exposing consumer data, or access to authenticated channels.

In line with these leading frameworks, Australian Government Agencies including the Australian Signals Directorate and the Australian Cyber Security Center[34] also provide guidance for consumers and organisations to enable MFA as it “defends against the majority of password-related cyberattacks” and should be used for all accounts.

The Data Standards’ Security Profile currently defines the need for DHs to issue authentication challenges to consumers using OTPs across a channel the consumer is familiar with but does not allow a second factor to be presented alongside this. A common scenario enforced by DH’s is to deliver the OTP via an SMS to the user’s mobile device and this has explicitly been identified as a restricted authenticator by NIST[35]. This is a less secure method than other alternatives as noted by Australian Government Agencies mentioned previously. Organisations require a greater understanding of the additional risks associated with using SMS (unencrypted delivery of OTP, device swaps, SIM changes, porting of numbers etc.) as an authentication method compared to the additional security offered by alternative options.

Additionally, the Australian Communications and Media Authority released the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*[36] which mandates the use of MFA for high-risk customer interactions.

3.4.3 Adoption of biometrics and alternative authenticators

Research undertaken by Australian federal and state governments[37] alike aims to understand current consumer sentiment towards various authenticators that can be used to securely authenticate users and alleviate reliance on insecure authentication factors. Biometric technology has continued to improve in accuracy and efficiency in recent years and is being widely adopted as a form of authentication for personal devices.

However, challenges and concerns must be addressed and accounted for when adopting biometric authentication methods and storage of this data, as certain consumer demographics continue to be sceptical and concerned about the ramifications of using biometrics as an authentication mechanism due to the perceived impact and possibility of

[34] https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-authentication

[35] https://pages.nist.gov/800-63-3/sp800-63b.html#restricted

[36] https://www.legislation.gov.au/Details/F2022L00548

[37] https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

fraud or data misuse if their biometric data are compromised.[38] Awareness of the details around the storage and security for biometric data amongst consumers remains low, and is also coupled with low concern for this topic.[39]

3.4.4 Federated access to services

Federated access enables consumers to authenticate themselves for a service provider's offering by using an already existing account setup with another Identity Provider (**IdP**)[40], and a common example would be leveraging existing Google accounts. This reduces the reliance on needing to create additional accounts and enables single sign-on capabilities. With the increased reliance on digital services and data flows between them, the use of approved IdPs for federated access enables seamless interaction to services for users.

NIST SP 800-63-3 highlighted the importance of federation with its split of LoAs to include Federated (Identity Architectures) and Assertions Levels (**FALs**) and revision 4 of takes this further by highlighting the Federated Digital Identity Model up front and identifying the relevant process flows expected. Similarly, TDIF is structured to support a federation-style of interconnectivity to support trusted digital identities and explicitly outlines requirements and guidance that should be followed to integrate with the Australian Government Digital Identity System.[41]

Currently all leading commercial off-the-shelf Access Management solutions provide federation out of the box and integrations between trusted organisations can be established to reduce the reliance on multiple passwords and authenticators. Modern identity protocols including Security Assertion Markup Language and OIDC are standards of implementing federation and have widespread adoption across the world

[38] https://doi.org/10.52922/sr04169

[39] https://www.aic.gov.au/publications/rr/rr20

[40] An Identity Provider is a system or service that creates, maintains, stores and manages digital identity information and provide authentication services to other applications and systems

[41] https://www.digitalidentity.gov.au/tdif

4 Data Practice and Usage Considerations

Secure and authorised access to consumer data is fundamental to protecting against data breaches and fraud. However, without conducting the necessary assessments to understand the sensitivity of consumer data, the risk and impacts associated with inappropriate access, securely managing, and monitoring the data over its lifetime and maintaining an appropriate level of data hygiene and cleanliness, data can unwittingly be misclassified, mishandled, and eventually lost. This section talks about key supporting insights to enable appropriate and secure authentication practices to appropriately protect consumer data.

4.1 Data classifications and sensitivity

Not all CDR data should be treated with the same sensitivity and require equal levels of security controls. Consumer data use scenarios that can encapsulate both mundane and sensitive information being shared between CDR participants for different purposes. As additional industries and obligations are introduced, the allowed scenarios will continue to expand, as will the variety of consumer data sets. Appropriate classification and categorisation of distinct consumer data sets will allow a more granular authentication framework to be applied across authentication processes. This would reduce the need for overly strict controls for access to less sensitive or immaterial data sets while enforcing security when it's needed most.

Data sensitivity labels and classifications can also be used to assess the risk presented by aggregated data sets that CDR participants construct over time, with the appropriate consumer's consent, and determine if stronger authentication challenges should be presented to consumers to access and share their own data (if part of a service offering). This risk assessment and authentication control would be applicable to all CDR participants that have access to the consumers data and expands upon the current authentication requirements applying only during consent process flows and authorisation to share data and ensures that possible sign-in authentication controls are commensurate with the level of risk and impact of this data being exposed to unintended audiences.

In line with the collection of large sets of data, the uplifted risk assessment processes and framework could consider heightened risks associated with the collation of varying data sets and sensitivities to provide aggregated data classifications and risk profiles, leverage known cyber threat patterns and the impact of large data breaches.

4.2 Authentication Levels of Assurance and Authenticators

The Data Standards' Security Profile currently outlines two available Levels of Assurance[42] (**LoA**) that must be enforced during the establishment of consent. These are defined in the Data Standards as LoA of 2 and LoA of 3 and are the minimum authentication requirements for READ and WRITE operations respectively. These LoAs are mapped to TDIF's Credential Levels (**CL**). The LoA of 2 in the Data Standards is mapped to TDIF's CL 1, and the LoA of 3 is mapped to TDIF's CL 2. The use of the term LoAs in the Data Standards, however, diverges from their use in TDIF. TDIF contains two LoAs, the CL and the Identity Proofing (**IdP**) Level. The selection of a risk-based IdP Level in TDIF then maps onto an appropriate TDIF CL. The Data Standards are silent, however, on IdP Levels. Additionally, where the Data Standards refer to LoAs, as outlined above, but do so without reference to TDIF, these terms are then essentially being defined, although they lack any definition.

With continued uplifts to the risk assessment processes and inclusion of a data sensitivity model to inform and assess the risk and sensitivity of consumer data, the existing risk framework could be expanded upon to determine the appropriate LoA for each data use scenario and inclusion of data sets into the CDR regime. This uplift would also consider the relevant authentication and consumer exposure risk factors for a holistic view on the necessary authentication security requirements to protect consumer data.

[42] Previously defined in Section 2.2 as the "degree of confidence in the processes leading up to and including the authentication process itself and provides assurances that the individual that is authenticating is an appropriate user of the account being authenticated against.

Upon assessment of the data sensitivity and risk factors of existing and emerging data use scenarios, additional Levels of Assurance may be required to provide enough granularity to apply appropriate access controls, and these should be reflected within the Data Standards for consistent application by all CDR participants. Fundamentally this is in line with the assessed leading authentication frameworks and their inclusion of a risk-based assessment processes to determine suitability of authentication controls. It may also be determined that READ operations for highly sensitive data sets require higher assurance than the current LoA before data should be shared.

4.3 Usability and Adoption of Authenticators

The current TDIF credential levels outline minimum authentication requirements and permitted combinations of authentication types that should be enforced for the appropriate LoA mappings. However, the authentication types that can be utilised are further constrained by the Baseline Security Provisions[43] included within the Security Profile that disallows the use of passwords, while simultaneously requiring the use of OTPs through known channels. This was originally defined to mitigate the risk of potential phishing attacks and reduce the possibly of consumers providing their credentials to malicious websites. But this has resulted in the inability of CDR participants to incorporate MFA controls that may already exist on their current service offerings. Whilst this is a seamless and consistent pattern that can be applied across all CDR participants, it has been noted by CDR participants and external specialist assurers to be an out-of-date model that is no longer best-practice[44].

Further analysis and industry consultation must be undertaken to understand the appetite for the inclusion of varying assurance levels and authentication types being applied across the various data sets and data use scenarios involved in the CDR ecosystem, determine whether DHs can utilise existing authentication mechanisms that are in use across their existing services and familiar to consumers, and where uplift is required to meet any changes to the minimum security requirements that would need to be enforced.

Changes to increase the minimum authentication security must consider whether the existing controls remain an appropriate option for any current data use scenarios. In determining how to address consumers without access to more sophisticated authenticators, it would be prudent to understand whether alternative consent flows would also be feasible as a measure to maintain a level of security, even if certain authenticators are unviable or if low sensitivity data can continue using the current authentication processes.

[43] As outlined under the Authentication Flows section of the Security Profile https://consumerdatastandardsaustralia.github.io/standards/#authentication-flows

[44] https://github.com/ConsumerDataStandardsAustralia/standards/issues/258

5 Applying Authentication Frameworks to CDR data practices

The TDIF authentication framework adopted by the Data Standards currently covers consent scenarios addressing the authorised transmission of consumer data from DHs to ADRs, and nominally has allowances for WRITE based actions should the authentication requirements be updated to allow authentication patterns consistent with CL2 of the TDIF. The current authentication framework enables a consistent and accessible model of authentication across all DHs that is familiar to CDR consumers and continues to operate based on pre-defined Levels of Assurance.

This section will address key considerations that could also be adopted into the existing framework and outlines where additional extension of controls could be applied within the scope of CDR data flows.

5.1 Summary of key considerations

Key considerations identified that could be adopted or uplifted within the CDR include:

1. Uplift of existing risk management frameworks and risk assessment processes to incorporate relevant authentication and consumer data exposure risks, to address data sensitivity concerns and assess the appropriate LoA applicable to data use scenarios
2. Assessment of existing and upcoming data use scenarios against the updated risk management framework, to identify granular LoA requirements and update the Security Profile to outline the authentication requirements that CDR participants must enforce during authentication flows
3. Inclusion of approved authenticator methods and versioned references to upstream standards within the Data Standards, to ensure consistent application of authentication requirements where ambiguity exists (NIST, ISM etc.)
4. Uplift of existing Data Standards authentication flows to support SSO capabilities and provide greater choice to CDR participants to implement more secure authenticator types. These authenticator types would be permitted under the approved LoAs and CLs defined within the risk assessment process. This may enable organisations to leverage their existing authenticator patterns currently used in existing service offerings
5. Further analysis into alternative or process flows to support consumers without access to secure authenticator types, or retaining less secure authentication methods, for lower risk transactions only i.e., offline consumer access.

5.2 Extension of coverage

Currently the Data Standards only contain consumer authentication flows for consent collection and disclosure. Unauthorised or inappropriate access and disclosure of consumer CDR data could occur, however, due to weak identification / authentication practices employed by ADRs and other non-DH CDR participants. Therefore, the Chair should consider how to address the current requirement defined in the CDR Rule 8.11 (1)(c)[45] for the authentication of CDR consumers to meet, in the Chairs opinion, best practice security requirements. Considerations would also include whether the authentication of consumers accessing their own data from an ADR should be addressed and whether the Chair is required to specifically address this increasingly complex situation of aggregated data sets moving across the CDR ecosystem, such as from non-DH participant.

[45] https://www.legislation.gov.au/Details/F2022C00187/Html/Text#_Toc96610666

6 Recommendations for Improvement

PIC has determined that the overall authentication framework adopted by the CDR is fit for purpose and meets the requirements of the CDR today. The usage of OIDC and OAuth 2.0 protocols, and building upon requirements of the TDIF enables the CDR to provide services to consumers that improves upon existing screen-scraping practices. However, the risk management framework needs to mature further in order to prepare the CDR for increasing amounts of data use scenarios and to address data sensitivity and security concerns better.

PIC recommends that the Chair should uplift the existing risk management framework and risk assessment processes to include data sensitivity, authentication, access control and consumer data exposure risks. The framework can then be used to assess and understand the potential risk associated with including additional data sets and data use scenarios into the CDR regime better and identify an appropriate authentication security control commensurate to the risk. This would take the form of a mininum LoA that would be enforced by CDR participants once included into the Data Standards.

To do so, the Chair should build on the risk management framework and better engage with industry participants that can identify key inputs, risks and impacts of particular data use scenarios or specific data sets. This will support the Chair in determining suitable Levels of Assurance and Credential Levels. To secure access to this data, we suggest that the Chair develops and refines the approved authentication processes that CDR participants must present to consumers and allows greater flexibility of permitted authenticators, commensurate with the risk of providing access to consumers.

This would provide more granular security options to protect and strengthen the authentication process that secures access to consumer data, and improves on the broad LoA approach currently in operation.

Building on the risk assessment process to determine authentication requirements for data, the Chair should consider extending the scope of these assessments to cover situations where the aggregation of various consumer data sets by singular participants presents a potential risk if malicious access was gained. The required level of authentication that must be sought to authenticate users before presenting this data should be defined.

PIC also recommends that the Chair consider updating specific authentication terminology found within the Data Standards to align with TDIF phrases. This should provide greater clarity to CDR participants and reduce the likelihood of misinterpreting the authentication requirements of the Data Standards and TDIF. In conjunction with this, the Chair should consider performing recurring reviews of the normative references defined within the Data Standards to validate that the associated information is still relevant and determine whether further updates to the Data Standards are warranted based on recent changes. This would be coupled with appropriate versioning recordings to enable CDR participants to align on approved authentication requirements using the same source information.

Finally, the Chair should consider conducting risk assessments across authentication patterns that the Data Standards do not currently address, to ensure appropriate review and consideration is given to the suitability of data use scenarios that TDIF was not originally intended for (i.e. offline consumers). As these scenarios may continue to be supported and expanded upon, the relevant processes must be assessed to determine what suitable controls should be implemented and to understand the associated risks, though they may not be for the Chair to manage within their obligations or duties.

6.1 Recommendation 1 – Consider uplifting the current Data Standards risk management maturity in order to ensure that risk-based authentication Data Standards remain fit-for-purpose

Risk-based assessment frameworks are a fundamental component of the leading authentication frameworks and are used to identify the appropriate levels of authentication necessary to protect from data breaches. As the CDR continues to expand and include more industries and data use scenarios, it is imperative that risk-based access controls are applied to reduce the ability of unauthorised access to consumer data.

PIC recommends that the Chair matures the Data Standards risk management capability maturity[46] for current and future authentication levels of assurance requirements of CDR scenarios and data requirements. The risk management framework should consider data sensitivity, authentication and consumer data exposure risks against known CDR risks and considerations. The framework would be used to assess and understand that the unwarranted exposure of specific data sets or data use scenarios may present greater risks to consumers or organisations, and therefore require stronger security controls commensurate with the identified risks. An appropriate LoA, and permitted authenticators, can be defined for the data, and included within the Data Standards for enforcement by CDR participants during consumer authentication flows.

This will enable CDR participants that transmit data to align to the minimum authentication requirements outlined, but provides optionality to the authentication methods employed. By presenting the information publicly, future interconnectivity and alignment between other CDR-like ecosystems could also be facilitated through standard mappings between CDR aligned TDIF CLs and other LoAs, such as IdP Levels, could be defined.

6.2 Recommendation 2 – Consider uplifting authentication methods and mandating risk-based Multi-Factor Authentication

PIC expects that as the assessment of authentication requirements continue to cover more data use scenarios, the current LoAs and associated CLs mapping contained with the Data Standards would no longer be fit for purpose. The direct split between READ and WRITE operations would instead be replaced with LoAs of 1, 2 or 3 (or equivalent terminology) as determined by the uplifted risk management framework and may require higher CL and authenticator security to address secure access to sensitive data. External specialist assurers previously recommended that the default CL in the Data Standards should be a minimum of CL2 (Recommendation 12 of the 2022 Independent Security Health Check). This observation was endorsed by the DSB[47].

The authentication flows section with the Data Standards outlines the currently approved OIDC authentication flows, further enhanced by FAPI that are supported and note the baseline security provisions that should be enforced by participants. The Chair should continue consulting with industry to determine appropriate alternatives that can leverage existing investment by CDR participants to support higher levels of authentication. The Chair should consider allowing optionality to the technologies that can be implemented, either through explicitly noting approved methods or combinations of methods within the Data Standards or aligning to authentication frameworks (TDIF, NIST etc.) without specifically constraining flows to utilising specific authentication methods unless absolutely necessary e.g. OTPs.

Upon confirmation of approved alterations to the authentication flows to support higher CL requirements, these should be captured within the Data Standards and adopted by all CDR participants that provide access to those data sets.

In a similar vein, step-up authentication, Single Sign-On, federated identity access requirements and further session management scenarios could be considered as part of this recommendation to provide a seamless user authentication experience with minimal required friction if multiple authentication requirements are necessary to collect consent of varying sensitivity levels to the same DH, or across CDR participants that utilise external IdPs, to initiate actions on a consumer's behalf that require higher CLs.

6.3 Recommendation 3 – Consider the Chair's requirement to make risk-based authentication Data Standards for consumer access to consumer data hosted by non-Data Holder CDR participants

A unique and emerging risk to the CDR is the excessive accumulation of consumer data within CDR participants and may result in threat actors attempting to access consumer records through legitimate channels by exploiting weak access controls. PIC identified that CDR Rules 8.11 (1)(c) requires the Chair to make one or more data

[46] Department of Finance, Benchmarking Risk Management Capability https://www.finance.gov.au/government/comcover/risk-services/management/benchmarking-risk-management-capability

[47] https://github.com/ConsumerDataStandardsAustralia/standards/issues/258

standards that relates to the disclosure and security of CDR data including the authentication of CDR consumers which meets, in the Chair's opinion, best practice security requirements. Current data standards only provide guidance around the authentication processes required during consent collection.

The Chair should consider how to address the currently defined CDR rules and whether additional rules are required to uplift existing risk-based authentication requirement assessments to include and standardise authentication requirements for scenarios of accumulated data sets. The data sets may be of various levels of sensitivities, or aggregation of discreet consumer data sets that when combined might require higher levels of security to protect due to having higher sensitivity and determine appropriate access controls to apply to secure consumer access by ADRs or other CDR participants that expose this data.

Paramount to this success is to ensure that the existing LoAs and CL defined are still fit-for-purpose and cover the use cases expected of all CDR participants when exposing consumer data. The step-up authentication noted in Recommendation 2 should be revisited within the context of Recommendation 3 to identify whether data use scenarios and access to consumer data may require higher levels of assurance and associated CLs when increasingly sensitive data or aggregated data sets are presented and exposed to the consumer through CDR service offerings and can be prompted using just-in-time principles.

6.4 Recommendation 4 – Consider maturing the management of how external standards are incorporated by reference

PIC notes that although the Data Standard incorporates by reference TDIF as its authentication framework, however, terminology is not consistent between the two. The Chair should consider further adoption of TDIF terminology within the Data Standards to provide greater levels of consistency between the dependent frameworks and ensure that ambiguity is kept to a minimum. Examples of such terminology differences include:

- TDIF outlines the credential types that are supported with the associated constraints while the Data Standards identifies these as authenticators
- Data Standards baseline security provisions reference the disallowance of 'passwords', however TDIF instead refers to this same credential type as a 'memorised secret'
- The Data Standards refers to LoAs that do not exist within TDIF.

Where previous recommendations note updates to the Data Standards, alignment to TDIF terminology can be included within the same discussions and updates for inclusion within the standards.

While TDIF is the primary authentication standard incorporated by reference, there are other standards that are also included within the Data Standards. The Chair should consider ongoing reviews of the normative references outlined within the Data Standards and determine whether applicable changes and newer versions warrant updates as well. This should be coupled with relevant versioning of the assessed references to accurately record the latest assessed and relevant reference for CDR participants to align with. In addition to reviewing the references, PIC also recommends the Chair to consider identifying where follow-on references within these should also be documented within the Data Standards to help align security controls across CDR participants. Examples of such scenarios include:

- The Data Standards currently references the third iteration of TDIF (released April 2019) while the fourth iteration was released in May 2020 and has since been updated to release 4.8 and last published in February 2023.
- Various credential types outlined within TDIF make references to the security strength specified in the latest version of the Information Security Manual (**ISM**) and could lead to various versions of controls being enforced throughout the CDR ecosystem.

6.5 Recommendation 5 – Consider conducting risk assessments for patterns of authentication that the current Data Standards do not apply to

While other recommendations have primarily recommended strategic uplift of risk-based processes and maturing the Data Standards, PIC recommends the Chair to assess current data use scenarios and consumer authentication patterns to which the Data Standards are not currently applied. As previously noted, the authentication framework that the Data Standards has adopted is TDIF and this framework is primarily designed to standardise digital identity and online authentication processes between participating entities.

However, TDIF is not applicable to address consumers wishing to authenticate and interact using physical processes or through non-digital channels, i.e. “offline” consumers. As there are data use scenarios applicable to these consumers that the CDR must address, the Chair needs to determine where development of the Data Standards is warranted, and the risk-based approach and controls that must be developed.

Facilitation of onboarding these consumers into the CDR, and the required controls to protect them, has a number of associated risks that deal with privacy, security and further consumer considerations that require detailed assessment. Furthermore, legislative provisions must be considered to determine their applicability.

Finally, the Chair’s duty and obligations may not require the Chair the manage these risks, but it is imperative to understand the implications and uplift of Data Standards to address these scenarios.

Appendices

Appendix A Existing and Emerging Authentication Frameworks Observations

This section of the report details the leading global authentication frameworks that were assessed as part of this report and outlines several key observations that were identified in each. The frameworks identified and compared against the Data Standards were:

- ISO/IEC 29115:2013
- NIST SP 800-63-3
- eIDAS Regulation (EU) 910/2014

Several commonalities were found between them, and this is mirrored in TDIF that the Data Standards has adopted as its authentication framework. The primary finding among this assessment was the need to use a risk-based approach to determine the appropriateness of implementing varying security levels of authentication and their applicability to manage risk.

ISO/IEC 29115:2013

The International Standardisation Organisation (**ISO**) and International Electrotechnical Commission (**IEC**) first published ISO/IEC 29115:2013 - Information technology - Security techniques - Entity authentication assurance framework in April 2013 and was last reviewed in 2020. The framework focuses on managing authentication of entities, in line with the Entity Authentication Assurance Framework (**EAAF**) and defines four levels of assurance that correspond to varying degrees of confidence in the authenticated entity.

Level of Assurance

ISO/IEC 29115:2013 outlines four LoAs but notes they are used to describe the "degree of confidence in the processes leading up to and including the authentication process itself". This spans all phases of the EAAF including Enrolment, Credential Management, and Authentication. As this covers the authentication process, understanding how the LoAs are determined and differentiated is paramount. The four levels are:

- **1 – Low:** Little or no confidence in the claimed or asserted identity
- **2 – Medium:** Some confidence in the claimed or asserted identity
- **3 – High:** High confidence in the claimed or asserted identity
- **4 – Very High:** Very high confidence in the claimed or asserted identity

To achieve higher levels of assurance, not only must authentication requirements be met, but so too must identity proofing requirements. While identity proofing addresses concerns around capturing and verifying the information necessary to identify a particular individual can be trusted, authentication requirements attempt to verify that the user attempting to access data and services is the same trusted individual. This tight coupling of assurance levels, that considers both identity proofing and authentication concepts, creates a rigid framework that combines assurances in multiple areas that focuses on securing access and ensuring the current user of an account has been appropriately validated is the intended and trusted user.

The standard does note that not all domains may adhere to the same LoA requirements and levels, and it may be necessary to document and explain how various schemes might interoperate[48]. In documenting and populating this information, it is possible for other organisations and domains to understand clearly how they may enter into federation-like agreements. By understanding where integrated domains may be using three-level assurance models (Low, Medium, High) and others are using four-level assurance models (Low, Medium, High, and Very High), how each defines and allocates the necessary LoAs and where they are applied, it is possible to map and understand how levels may correlate with one another between domains.

Selection of Assurance Levels

The EAAF outlines the need to select an appropriate LoA to secure access to data, transactional activities and services by assessing against risks that have been identified as relevant to an approved risk-based assessment process and associated risk criteria, but leaves defining the risk-based approach open to interpretation of each individual organisation and could align with an organisations approach to managing residual risk[49]. Potential impacts of incorrectly applying LoAs are defined within the framework for consideration, alongside possible consequences, but the standard notes that the assessment should be conducted against each phase of the EAAF.

Permitted Authenticator Types

Guidance is provided to understand whether general authenticator methods should be applicable for individual levels of assurance (cryptographic authentication methods not required for LoA 1, MFA enforced for LoAs of 3 and 4 etc.), but ISO/IEC 29115:2013 explicitly states outside of this situation, it is “not appropriate to delineate specific controls in terms of LoA for the authentication phase”. The standard makes a point[50] that context is required to identify what an appropriate control would be, and this is in line with the reliance on organisation specific risk frameworks.

NIST SP 800-63-3 - Digital Identity Guidelines

The National Institute of Standards and Technology (**NIST**) Special Publication 800-63-3 - Digital Identity Guidelines was originally published in June 2017 and included several key considerations that have informed the design of the TDIF. In the context of authentication, NIST SP 800-63-3 has a few key differences when compared with other frameworks that could be considered.

Level Of Assurance Separation

NIST SP 800-63-3 first introduced the separation of LoAs into three distinct categories, to allow agencies to define individual assurance levels that enabled greater flexibility, privacy, and reduced risk to be applied to digital identities and their transactions. The separation was split to address:

- Identity Proofing – Identity Assurance Levels (**IALs**)
- Authentication – Authenticator Assurance Levels (**AALs**)
- Federation (assertion strength within a federated environment) – Federated (Identity Architectures) and Assertions Levels (**FALs**)

Each of these assurance categories can be assessed individually or in combination with one another to meet the desired risk profiles and outcomes expected of an exposed service. By implementing a risk management framework that considers each of these levels individually (where applicable), more robust challenges and security controls can be issued in a decentralised model.

[48] ISO/IEC 29115:2013, Section 6.6 LoA mapping and interoperability

[49] ISO/IEC 29115:2013, Section 6.5 Selecting the appropriate level of assurance

[50] ISO/IEC 29115:2013, Section 10.3 Threats to, and controls for, the authentication phase

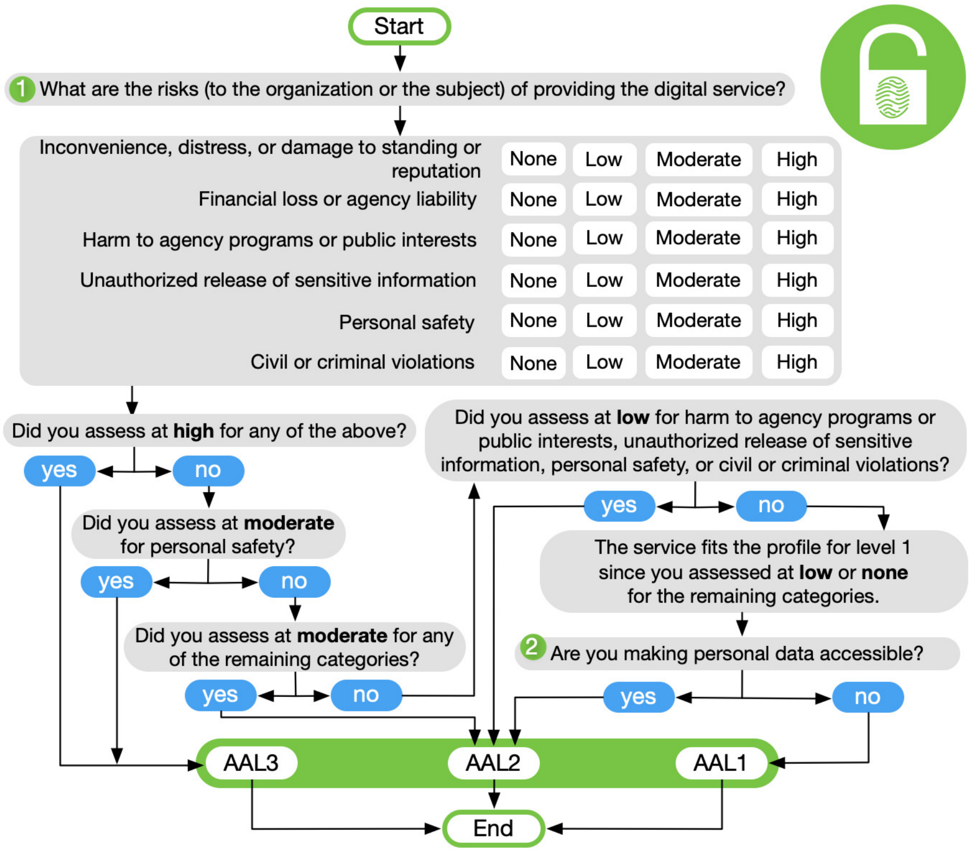
Selection of Assurance Levels

A key inclusion within NIST SP 800-63-3 is the risk-based process flow to select appropriate assurance levels per each assurance category. The authentication assurance levels are defined to be commensurate with the risk to organisations and consumers. When combined with context specific risk frameworks, this model can help enable greater understanding of where high levels of authentication security may be warranted and apply appropriate controls. Unlike, ISO/IEC 29115:2013, only 3 LoAs are defined in this framework. The three levels are:

- **AAL1**: Some assurance that the user controls an authenticator bound to the account and requires either single-factor or MFA
- **AAL2**: High confidence that the user controls authenticator(s) bound to the account and requires proof of possession and control of two distinct authentication factors
- **AAL3**: Very high confidence that the user controls authenticator(s) bound to the account and requires possession and control of two distinct authentication factors, with stricter requirements than AAL2.

The selection of an appropriate AAL to be enforced can be determined by applying a similar AAL decision tree as depicted in Figure 1 below. By applying a risk-based approach that considers various risks and impacts that are relevant to organisational and consumer needs, the minimum AAL can be determined in a methodical and repeatable way.

Figure 1 NIST SP 800-63-3 AAL Decision Tree[51]


Start
1 What are the risks (to the organization or the subject) of providing the digital service?
Inconvenience, distress, or damage to standing or reputation
Financial loss or agency liability
Harm to agency programs or public interests
Unauthorized release of sensitive information
Personal safety
Civil or criminal violations
None
Low
Moderate
High
Did you assess at **high** for any of the above?
yes
no
Did you assess at **moderate** for personal safety?
yes
no
Did you assess at **moderate** for any of the remaining categories?
yes
no
Did you assess at **low** for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
yes
no
The service fits the profile for level 1 since you assessed at **low** or **none** for the remaining categories.
2 Are you making personal data accessible?
yes
no
AAL3
AAL2
AAL1
End

[51] https://pages.nist.gov/800-63-3/sp800-63-3.html#63Sec6-Figure2

Permitted Authenticator Types

Another key inclusion in NIST SP 800-63-3 is a detailed list of permitted authenticator types per AAL and how they can be used to provide the associated AALs including where applicable, the combination of various authenticators that must be enforced to achieve higher levels of assurance.

Future Revision Considerations - NIST SP 800-63-4

Revision 4 of NIST SP 800-63 is currently out for public consultation and largely aligns with the guidelines presented in NIST SP 800-63-3, detailing the same key concepts around AALs and authenticators and risk-based approaches to defining assurance levels. However, of importance to note within the latest revision is the increased focus on reducing risks for consumers, greater fraud protection controls and a forward-looking view of increasing federated access between organisations.

In the context of authentication, two key highlights that may be considered relevant are:

Equity Considerations[52] - The ability to provide accurate and equitable authentication services to consumers that account for specific characteristics and considerations faced by a population that may be vulnerable or disadvantaged. This could be achieved through binding additional authenticators, reducing the need for possible account recovery processes. Within the CDR ecosystems, as increasingly digital services are made available, greater adoption is seen across the Australian public, and further industries are required to participate, the number of consumers will continue to grow, each with their own specific circumstances. It can be expected that without appropriate consideration given to an increasingly larger cohort of potentially vulnerable or disadvantaged consumers, then this may disproportionally alienate or unfairly exclude them from participation in the CDR.

- Greater guidance and outlined processes for Digital Identity Risk Management[53] - Revision 4 outlines 4 key steps to be considered as part of the digital identity risk management process to determine appropriate assurance levels and the need to document relevant information that culminates in a Digital Identity Acceptance Statement[54]. This process supports organisations by providing a methodology that can be considered to assess digital identity risks associated with assurance levels, such as AALs and supplements existing risk management processes that are critical to determining appropriate authentication security controls. The 4 key steps are:
    - Conduct Initial Impact Assessment
    - Select Initial Assurance Levels
    - Tailor and Document Assurance Level Determinations
    - Continuously Evaluate & Improve

eIDAS Regulation (EU) 910/2014

The European Parliament and the Council of the European Union adopted the eIDAS Regulation (EU) 910/2014 in July 2014 to define approved electronic identification schemas and establish rules for trusting service providers between member states. This is a regulatory framework that helps ensure secure electronic transactions can take place between organisations and consumers.

[52] https://pages.nist.gov/800-63-4/sp800-63b.html#sec11

[53] https://pages.nist.gov/800-63-4/sp800-63.html#sec5

[54] https://pages.nist.gov/800-63-4/sp800-63.html#IDacceptStmt

Assurance Levels

eIDAS Regulation (EU) 910/2014 outlines assurance levels as "the degree of confidence in electronic identification means in establishing the identity of a person"[55] to ensure the person claiming to use a particular identity is the owner that was originally assigned to it. Similar to ISO/IEC 29115:2013, these span multiple processes including identity proofing and verification, and authentication. However, unlike ISO standards, only 3 levels are outlined:

- **Low**: Limited degree of confidence in the claimed or asserted identity of a person
- **Substantial**: Substantial degree of confidence in the claimed or asserted identity of a person
- **High**: A higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial

Selection of Assurance Levels

The regulation does not detail a framework or process that mandates certain assurance levels to particular scenarios but instead obligates participants to recognise the assurance levels designated by the online service. This allows members to define their own risk appetite and can expect participants to meet certain assurance levels before they are able to interact securely.

Permitted Authenticator Types

Regulation (EU) 910/2014 strives to maintain a consistent application of requirements on all participants, noting that technical requirements should be technology-neutral and it "should be possible to achieve the necessary security requirements through different technologies". Supplementing the eIDAS Regulation, the Commission Implementing Regulation (EU) 2015/1502[56] was adopted in September 2015 and sought to set out minimum technical specifications and procedures for assurance levels.

Sections 2.2 (Electronic identification means management) and 2.3 (Authentication) of the regulation contain minimum authentication requirements, and when combined with Section 1's (Applicable definitions) definition of 'authentication factors', can be used to determine minimum authentication controls to be implemented. This provides a basic framework to identify appropriate controls relative to the applicable assurance levels.

[55] eIDAS Regulation (EU) 910/2014, Recital 16

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502

Appendix B Leading standards and frameworks relevant to sensitivity analysis and broader risk management practices

This section of the report outlines several industry proven frameworks and standards that speak to sensitivity analysis for the Chair consideration. A high-level summary is provided together with its potential applicability to the CDR. The suitability of implementing any one framework or standard is contingent upon (i) ensuring no conflict arises from existing requirements or guidelines mandated by the Australian Competition and Consumer Commission or the Office of the Australian Information Commissioner, (ii) feasibility and practicality of imposing any additional compliance obligations to CDR Participants, including ADRs, and (iii) available resources to implement it within existing CDR risk management processes.

ISO 27005 – Security Techniques (Information Risk Management)

ISO 27005 provides a qualitative and quantitative approach to documenting the likelihood of risk and consequence scale or impact of risks. The standard is useful to identify potential privacy risks and analyse identified risks to determine the likelihood of a breach. Note that the utility of qualitative scales and the consistency of risk assessments that derive from them will depend on a standardised interpretation. The drawback however is its lack of prescription and the need to define both the scope of a risk management activity and what risk criteria may be applicable.

ISO 29101 - Privacy Architecture Framework

ISO 29101 introduces the Privacy Architecture Framework, a comprehensive document that encompasses the privacy lifecycle and is designed to be integrated into an organisation's overall risk management strategy. In the context of data sensitivity, the framework expounds on the need to preserve privacy controls. Sensitivity classifications of a data attribute should be flowed through to the systems that either process or store the data. These systems should be able to distinguish between the different sensitivities of data that is being stored and used. System owners should then be required to implement processes to mitigate the risk of introducing sensitive personal information or high-risk data into a repository containing non-sensitive personal information or low risk data. While not entirely applicable, the potential output demonstrates the usability and value of sensitivity analysis being conducted at a broader scale.

ISO 29184 – Information Technology (Online Privacy Notices and Consent)

ISO 29184 outlines implementation considerations of two key privacy principles derived from ISO 29100, namely (i) Principle 1 – Consent and Choice, and (ii) Principle 7 - Openness and Transparency. ISO 29184 states that consent notices, especially those involving third parties collecting CDR data should also state the potential risks or harm that the consumer may face, and the likelihood of any risk to them if they consent to sharing their personal information. This is tied to the very essence of the principle of informed consent. In the context of the CDR, and particularly with respect to CDR insights data which carry potentially higher sensitivity classifications through a combination of disparate datasets, this standard recommends that consent notices should also state elements of a consumer's personal information in which insights can be gained.

ACS Framework for Controls and Data Sharing

The Framework and Controls for Data Sharing 2023 provides controls for each phase of the data life cycle, linking the purpose of data sharing (the 'why') to the mode of data sharing (the 'how'). The primary position of this framework is the acknowledgment that not all data is the same, and in many instances, the level of personal information in a dataset cannot be systematically measured, and the inherent sensitivity of the data itself cannot be unambiguously assessed.

As the Chair progresses towards a risk-based approach to developing data standards, and with respect to the need for a data sensitivity analysis, this framework provides a lens into the next step that will be required when managing the security of CDR data. Once the sensitivities of data attributes have been identified, they can be segmented into tiered control environments, each requiring specific security controls as it increases in risk. The recommendations below could be introduced by way of an update to Part 2 (Minimum information security controls) of the CDR Rules:

- High Control Environment - explicit purpose and authority to access and use data, strong governance, and security at each stage of the life cycle, access limitations, and explicit restrictions on release of data and insights, or secondary use of data and insights.
- Moderate Control Environment - general purpose and authority to access and use data (such as an authorising regulatory framework), general restrictions on release of data and insights, or secondary use of data and insights, and strong governance and security at each stage of the life cycle.
- Low Control Environment - no explicit authority to collect and use data, but no known restrictions to use data, appropriate governance, and security at each stage of the life cycle and is generally construed as open data that is generally available in the public domain.

Commonwealth Risk Management Policy and Maturity Model

The purpose of the policy is to embed risk management into the culture and work practices of entities to improve decision making in order to maximise opportunities and better manage uncertainty. The elements of the policy outline its requirements. Entities should tailor their risk management arrangements to suit the nature of their operations and the risks they face. The Policy provides the principles and requirements for managing risk in undertaking the activities of government.

www.pwc.com.au/pic

At PIC, our purpose is to improve the lives of Indigenous peoples and support self-determination through empowering Indigenous led models and solutions. With over 50 staff located in 8 offices across Australia, we offer a full suite of consulting services, regularly collaborating with PwC and its extensive array of specialist business services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au/pic.