Data Standards Body

Consumer Experience and Technical Working Groups

Noting Paper 326: Authentication Uplift Context

Contact: Mark Verstege

Publish Date: 13 October 2023

1. Table of Contents

2. Introduction

This noting paper relates to the Consumer Data Right (CDR) authentication standards and how they might be uplifted. As per Rule 8.11(1)(c)(i), the Data Standards Chair has an obligation for the *"authentication of CDR consumers to a standard which meets, in the opinion of the Chair, best practice security requirements"*.

This noting paper accompanies **Decision Proposal 327: Authentication Uplift Phase 1**. It is intended to introduce authentication concepts and propose uplift to authentication in the CDR for the phases beyond Phase 1.

Decision Proposal 327: Authentication Uplift Phase 1 proposes changes to be considered within the first phase of authentication uplift pertaining to *online* customers, including:

- the support of stronger customer authentication methods,
- higher levels of authentication assurance,
- strengthening existing OTP authentication, and
- supporting App2App redirection flows for a better consumer experience.

This noting paper doesn't propose any Standards changes, its purpose is to present questions for feedback that will help inform the development of relevant future Standards in subsequent authentication uplift phases.

Summary of key concepts in this noting paper

This noting paper proposes the following for consideration:

- Strong authentication controls for CDR,
- The incorporation of risk-based assurance levels for the selection of Credential Levels,
- Support for multiple authentication factors, including progressive step up authentication,
- Supporting decoupled authentication supported by Client Initiated Backchannel Authentication,
- Adopting FIDO Credentials/Passkeys,
- Adopting streamlined re-authentication using login hints for improved consumer experience,
- Introducing Business Single Sign-On for non-individual consumers and partnerships, and
- Interoperability with trusted digital identity providers in line with the exposure draft Digital ID bill, and the Trusted Digital Identity Framework

2.1. The role of authentication in the CDR

CDR authentication standards as currently defined, enable authorised access to consumer data held by Data holders. Data recipients redirect end users to Data Holders. These end users may either be individual consumers or a nominated representative that acts on behalf of a non-individual consumer.

Authentication serves as a repeatable process to prove the end-user is the same person who previously established a digital identity. How the end user is challenged to gain access may differ. Commonly this is either through possession of a secret (like a password that the user knows), a verified device (like a smartphone that the user owns), or an identifiable physical attribute of the user (like a fingerprint biometric). The end user must satisfy the authentication challenge by successfully presenting the credential required, thus demonstrating they have access to the associated digital identity that was registered.

In the CDR today, the Data Standards support only "one-time passwords" (OTPs) that may be delivered to the end user in a variety of methods. Some delivery methods such as email or SMS are less secure than, for example, a soft-token application enrolled on the end user's registered device or a hard token device fob that both provide a cryptographically secure method for OTP generation.

It was a deliberate choice to exclude passwords as an authentication method at the inception of the Consumer Data Standards. To avoid phishing attacks, and the issues prevalent with screen scraping, this control was introduced to improve security.

It is also important to recognise that authentication is not the only aspect of securing a digital identity and authority to access information held by a Data Holder for a consumer. Whilst the requirements differ between sectors, typically there is some form of identification required to enrol a digital identity and the verification of any identification information provided. At establishment of the digital identity credential this creates a binding between the identity information and access to the identity and any products and services connected to the digital identity.

2.2. The need for strong authentication controls

Authentication is a primary security control used by Data Holders to establish assurances that the person seeking to gain access to consumer data is the intended customer with the right to access that data.

The breadth of CDR data that can be accessed spans multiple sectors including Banking and Energy, as well as Telecommunications and Non-Bank Lending earmarked in future.

Attacks on authentication controls are increasingly more sophisticated

In early 2023, the Australian Bureau of Statistics released its report into Personal Fraud[1] for the 2021-22 financial year including 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 the referenced year alone, and was the same rate found for the previous year (2020-21). Stolen personal information was primarily used to obtain money from bank accounts

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

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.

As Australians also grapple with the increasing frequency of data breaches and identity fraud, recent reporting on Phone Porting scams highlights the sensitivities with single factor authentication when OTPs are delivered by SMS.

In the UK, authorised push payment fraud has increased with £485.2 million lost to APP scams in 2022 from impersonation attacks — for example a fraudster impersonating bank staff to get someone to transfer funds out of their bank account and into that of a fraudster — continuing to account for £109.8m in losses.

Further to this, Artificial Intelligence-fuelled threats[2] that are just only now becoming cost-effective for criminals to employ at scale which further place OTP and memorised secrets used as a single authentication factor in jeopardy. Emerging AI threats include:

- AI detection of a consumer's password or other details by listening to them using their keyboard via their computer's mic (yet another reason not to use passwords); and

- A variant of the "Hello Mum" SMS scam, known as "vishing"[3] where an AI Chatbot literally speaks to the victim using the voice of the relative / friend they are impersonating.

Authentication controls must be enforced consistently and appropriately across all participants of the CDR ecosystem to counteract these risks and reduce the likelihood of harm to Australian consumers.

Action Initiation will introduce higher risk actions that need stronger protections

As the CDR expands to support Action Initiation, strong customer authentication will also be necessary to provide appropriate protections for higher risk actions like making payments or changing energy retailers. In Europe, the Payment Service Directive 2 (PSD2) mandates strong customer authentication.

At the same time, better authentication standards will help improve the consumer experience by offering device-native authentication options that are appropriate for the channel and situation the consumer is interacting in.

[2] A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards, https://arxiv.org/abs/2308.01074
[3] CAPEC-656: Voice Phishing, https://capec.mitre.org/data/definitions/656.html

2.3. National and international considerations

As a member state of the OECD, Australia is an adherent to several recommendations in relations to authentication (OECD/LEGAL/0353 "**Recommendation of the Council on Electronic Authentication**" published 2007) and digital identity (OECD/LEGAL/0491 "**Recommendation of the Council on the Governance of Digital Identity**" published 2023).

Key recommendations for authentication uplift include:

- *Adherents design and implement digital identity systems that respond to the needs of users and service providers.*

- [Should be designed using] *technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.*

- [Having regard that] *authentication mechanisms need to be continually upgraded to keep ahead of new forms of fraud (e.g., attackers steal credentials and use them to perpetrate fraud or other crimes). It is therefore desirable for authentication methods to be implemented with the ability to leverage more robust authentication technologies in the future. The growing use of multi-factor authentication, as well as the use of biometrics (e.g., iris scanning or finger printing), is an example of this trend .*

Domestically, the Australian Cyber Security Centre (ACSC)'s Information Security Manual (ISM) recommends several authentication hardening practices including implementing multi-factor authentication for system access.

2.4. Offline Customers

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

Decision Proposal 327: Authentication Uplift Phase 1 describes the issues and implications in supporting offline customers whilst stating that "a security risk-assessment for offline customers is being considered to assess best practice security for that modality".

2.5. Terminology

Unless otherwise specified, the definitions within NIST.SP.800-63-4.ipd Digital Identity Guidelines (refer to Appendix A) are otherwise assumed.

Term	Meaning
Authenticator	Means something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. Defined by NIST.SP.800-63-4.ipd Digital Identity Guidelines (refer to Appendix A).
Authenticator Assurance Level	A measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in NIST SP 800-63-3 in terms of three levels: AAL1 (Some confidence), AAL2 (High confidence), AAL3 (Very high confidence).
Authentication device	Means the device on which the user will authenticate and authorise the request. Defined by OpenID Connect Connect Client-Initiated Backchannel Authentication Flow – Core 1.0 (refer to Terminology).
Authentication factor	A group of authentication methods based on something the user knows (knowledge), something the user has (possession), or something the user is (inherence).
Authentication method	Is a type of authentication challenge commonly represented in OpenID Connect by way of an "amr" or Authentication Method Reference such as a face biometric, pin code, or OTP. Referred to in RFC8176 Authentication Method Reference Values. Defined by NIST.SP.800-63-4.ipd Digital Identity Guidelines (refer to Appendix A) as an "Authenticator Type".
Consumption device	Means the device which helps the user consume the service provided by the Relying Party. Defined by OpenID Connect Connect Client-Initiated Backchannel Authentication Flow – Core 1.0 (refer to Terminology).
Credential Binding	Credential binding is the binding between an identity and the authenticator that is used to confirm the identity used to access a service or system.
Credential Level	A group of authentication methods assigned to a level of security and risk by TDIF. The TDIF defines three Credential Levels (CL1, CL2, CL3) which define the allowable authentication methods to meet certain levels of security.

Term	Meaning
Identity Proofing	Identity proofing is the process of providing evidence of identity claims or attributes (e.g., identity documents, credentials or history) to establish confidence in an identity. The TDIF defines identity proofing by proofing levels. Identity Proofing Levels categorise data transactional and financial risk by the degree of confidence that a person's claimed identity is their real identity, as defined in TSIF 05 Role Requirements: IP1 and IP1+ (basic confidence), IP2 and IP2+ (standard confidence), and IP3 (strong confidence). NIST defines identity proofing by assurance levels. Identity Assurance Levels are categories that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in NIST SP 800-63-3: IAL 1 (Some confidence), IAL 2 (High confidence), IAL 3 (Very high confidence).
Levels of Assurance	Defined by OECD/LEGAL/0491 as *"the extent to which a service provider can be confident in the claimed identity of a user and is determined by the practices employed by the digital identity solution provider in the issuing of a given digital identity solution".* For authentication, levels of assurance are defined by • TDIF as Credential Levels. • NIST as Authenticator Assurance Levels

3. Authentication controls are determined using assessment against risk-based assurance levels

3.1. Overview

When accessing or applying for a service, you generally need to provide proof of who you are. The level of proof is correlated to the level of risk in incorrectly verifying you or providing access to the service to the wrong person.

Figure 1 Proving who you are, is just as important as the level of authentication required to access the service

Many systems allow an individual to claim, or assert, different identity information such as a name, date of birth, email address and phone number. Verification of such identity information is measured by the degree of confidence that a person's claimed identity is their real identity.

Frameworks including NIST's Digital Identity Guidelines[4] and TDIF Role Requirements[5] incorporate a risk-based framework for selecting appropriate identity and authentication assurance levels.

[4] Section 6, NIST SP 800-63-3: Digital Identity Guidelines
[5] Section 3.2 Digital Transformation Agency–TDIF 05 Role Requirements

Whilst strong authentication controls can limit who accesses a service, there is also a correlated need to verify who the individual is, based on the identity information the individual provides and the extent to which that information is verified.

These frameworks connect the requirements for identity proofing with the authentication levels necessary for system access based on a measurement of impact across a number of dimensions including financial loss, personal, and organisation harm. When risks like data loss or harm are assessed to be low, the service owner may request minimal verification of an individual's true identity against the identity information asserted by the individual. Conversely, when the risks are higher, it is more important to bind strong authentication controls and verification of identity information.

In order to effectively use TDIF in a risk-based way, implementers are required to decide which identity-proofing (**IP**) level to use. The selection of this level depends on the level of risk. The IP levels are as follows:

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**.

Table 1 Intended usage risk taken from Identity Proofing Levels (Table 1), Digital Transformation Agency: TDIF 05 Role Requirements

The IP level required is determined by a set of stated objectives when controlling risk. These are:

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
***Identity Proofing* objectives**[2]	Claimed identity meets: • Uniqueness	Claimed identity meets: • Uniqueness • Legitimacy • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control
Uniqueness Objective						
***Identifier* chosen by the *Individual* is unique**	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
A check undertaken by the *IdP* to establish that the *Individual* is the sole claimant of the *Identity*[3]	-	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*

Table 2 Identity proofing objectives as defined by Identity Proofing Levels (Table 1), Digital Transformation Agency: TDIF 05 Role Requirements

Once the level of risk has been determined, and the corresponding IP level selected, this decision then translates into the corresponding Credential Levels (CLs) permitted by TDIF.

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

Table 3 Credential Level bindings taken from Identity Proofing Levels (Table 1), Digital Transformation Agency: TDIF 05 Role Requirements

Further to this, Credential Levels provide a list of permitted credential types, or authentication methods, as follows:

CL1	ONE OF: • Memorised Secret • 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	
CL2	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
CL3	• 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

Table 4 Authentication methods as defined by Digital Transformation Agency: TDIF 05 Role Requirements.
SF = Single Factor, MF = Multi-Factor, Memorised Secret = Password. The greyed methods denote the Data Standards currently exclude passwords from being used as an allowed memorised secret.

Currently the Data Standards only allow a Single-Factor OTP which meets CL1. The TDIF permits CL1 authentication factors for only very low risk and low risk transactions (IP1 and IP1 Plus).

TDIF itself is informed by the NIST identity guidance, expanding the identity proofing levels with intermediate proofing levels (IP1+, IP2+) and an additional high assurance level (IP4) that binds identity proofing and authentication via proof of life (liveness) verification where only the highest level of authentication is permitted.

NIST takes a more traditional risk management approach and determines authentication assurance levels based on assessment against a set of impact categories:

	Assurance Level		
Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

Table 5 Section 6, NIST Maximum Potential Impacts for Each Assurance Level

After assessing risk against each of the impact categories, this determines an overall risk rating which in turn determines an Identity Assurance Level. This decision then translates into the corresponding Authentication Assurance Level:

	AAL1	AAL2	AAL3
IAL1: Without personal data	Allowed	Allowed	Allowed
IAL1: With personal data	**NO**	Allowed	Allowed
IAL2	**NO**	Allowed	Allowed
IAL3	**NO**	Allowed	Allowed

Table 6 Section 6.4 NIST Acceptable Combinations of IAL and AAL

NIST provides a straightforward evaluation framework to determine the appropriate NIST Authentication Assurance Level based on assessment against impact categories:

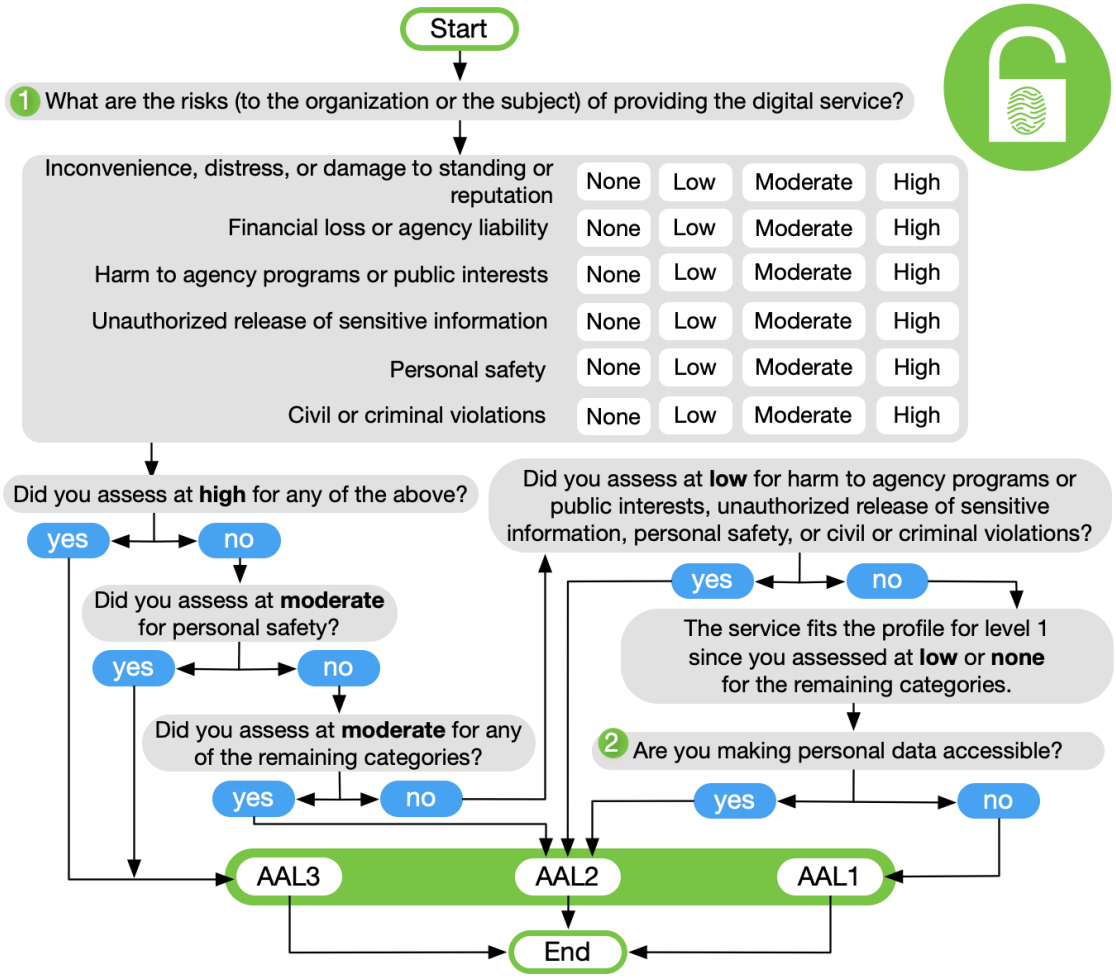


Figure 2 NIST SP 800-63-3 Section 6.2 Selecting AAL

Both frameworks provide a method of risk assessment which assists in the determination of acceptable authentication levels. Both frameworks support a principle-based assessment of risk which decides what authentication controls are allowed. A similar approach could be adopted in the Data Standards for deciding the required Credential Level which either allows Data Holders to individually conduct risk assessments and Credential Level decisions for their organisations or have binding Credential Level assessments set out in the Data Standards for data clusters and actions as is currently the case.

3.2. Why is a risk-based assessment methodology important?

Recent reports to the Chair, including the 2022 Independent Health Check Report, have strongly recommended improving authentication controls within the context of a risk-based decision-making framework. Authentication controls are a tangible response to risk. By defining a risk assessment framework that assists in identifying appropriate authentication controls it can be employed in a scalable way for all participants.

The Chair intends to consult on a decision making framework for assurance levels in future consultations.

3.3. Best practice

Many frameworks exist for identifying security risks and managing them. Some like NIST and TDIF look at impact categories and data sensitivity whilst others like MITRE, NIST and OWASP are focused on threat modelling and mitigations. All of these frameworks have merits, and it typically makes sense to combine a variety of tactics to manage the security landscape. Common frameworks and techniques include:

- **NIST** assurance levels define appropriate identity proofing and authentication requirements based on impact categories supplemented by an easy to follow decision making framework that considers data sensitivity, data loss, financial and reputational impacts;
- **TDIF** maps Identity Proofing levels to approved Credential Level bindings[6] with an emphasis on the identity proofing requirements;
- **OWASP** is best known for tracking a Top Ten list of critical security risks that are re-evaluated annually. OWASP also maintains the OWASP-TMP Treat Modelling methodology which in the assessment of threats and a countermeasure assessment process that includes modelling the security and information flow landscape. This threat modelling methodology includes a formal documentation process that is supported with relevant OWASP published tools.
- **STRIDE** is a widely used threat modelling approach initially developed by Microsoft that focuses on threat classification that aides in identifying any flaws in the security architecture of a system so they can be corrected.

[6] Section 3.2 Table 1: Identity Proofing Levels, TDIF 05: Role Requirements

- **MITRE ATT&CK** framework provides a comprehensive catalogue of known threats and mitigations. It is often a useful resource to augment a chosen threat modelling framework.
- **FAPI 2.0** has been developed from the ground up around a core attacker model to determine necessary security mechanisms. The Attacker Model identifies primary threats which the FAPI 2.0 Security Profile then seeks to mitigate.

3.4. Considerations when adopting an assessment methodology

Combining fit-for-purpose techniques would provide a robust and objective assessment framework for CDR security profile controls and for participants to employ in their CDR system design. Practically speaking, the NIST framework offers a good starting point because it is focused on data sensitivity and selection of authentication controls. The impact categories could be further tailored to the CDR which would then provide a classification framework for selecting appropriate authentication controls.

Threat Modelling whilst essential, could augment the authentication assessment framework, to consider the holistic threats to the CDR and the broader security control mitigations.

When considering an assessment methodology appropriate to the CDR, it is important to recognise the different levels of maturity to digital security across CDR sectors along with CDR policy objectives—such as eligibility criteria permitting data sharing for offline customers in Energy—may not neatly align to strong security practices.

As identified in the Independent Information Security Review Recommendation 12:

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

The review further states:

> *"While there are industries which lack in digital maturity and therefore may struggle to immediately meet such a requirement, these industries should be encouraged to uplift their security rather than lowering the security of the Data Standards to make allowance."*

Opportunities to uplift authentication in future sections of this paper are considered in the context of the Chair defining a risk-based authentication assessment framework that guides the selection of authentication controls.

4. Authentication Factors

4.1. Balancing flexibility, consistency, and prescription with authentication methods

Due to the economy-wide nature of the CDR, a consistent and familiar consumer experience is important both within sector verticals and across the economy-wide distribution of Data Holders. Consistency benefits consumers by ensuring a safe and secure environment is offered for data sharing regardless of Data Holder. At the same time, conformity of experience will help consumers to better trust the experiences presented within the CDR. A key recommendation from the Independent Information Security Review was alignment with NIST authentication assurance levels. For the Consumer Data Standards, this alignment is facilitated through the adoption of TDIF Credential Levels which are a nationally defined and recognised set of credential requirements as part of the Government's digital identity reform.

The corollary is that industry has typically offered authentication experiences as a point of competitive differentiation which has led to different implementations and different approaches depending on the digital maturity of individual organisations, the sector they operate within, and the business strategy and investment decisions of each organisation.

Evolving the authentication standards to adopt stronger customer authentication methods requires a balance between prescription and constraint versus free discretion of each Data Holder to adopt a preferred approach.

In the United Kingdom, the Financial Conduct Authority mandated strong customer authentication in line with PSD2[7] for open banking. However, the choice of authentication methods was left to the discretion of the banks which meant there was fragmentation in experience and, at times, increased friction and burden on consumers.

4.1.1. Constraining supported authenticator channels and delivery methods

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

NIST also requires[8] that authenticators make sure the user's telephone number is associated with a specific physical device that has been pre-registered for authenticator use when SMS (or voice) 2FA is used. NIST further recommends that verifiers watch for events such as "device [swapping], SIM change, number porting, or other abnormal behaviour before using the PSTN[9] to deliver an out-of-band authentication secret" because these activities could indicate a compromised channel.

---

[7] See Part 7 of the Payment Services Regulation (2017) (UK)
[8] See section 5.1.3.3, "NIST SP 800-63 Digital Identity Guidelines: Authentication & Lifecycle Management"
[9] PSTN stands for Public Switched Telephone Network, a network of telephone systems

In the CDR today, the Data Standards support only "one-time passwords" (OTPs) that may be delivered to the end user in a variety of methods. Some delivery methods such as email or SMS is greater than other authentication channels. Given this reason, even when used in a multi-factor setting the Australian Cyber Security Centre (ACSC)'s Information Security Manual (ISM) recommends "...authentication factors that involve something a user has should be used with something users know"[10].

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

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

However, unlike the banking sector, energy sector customers are considered eligible consumers even if they do not have online access to their account with their energy retailer. Without online access, these customers are unlikely to have an enrolled digital identity they use to login to their energy retailer to manage their customer relationship.

As such, there appears to be a conflict between international security best practice, the CDR rules for offline customers, and the digital maturity of some sectors designated in the CDR such as Energy. Best practice guidance is clear that SMS should be avoided as an authentication channel and email should not be used. Contrary to this, the CDR rules consider offline customers to be eligible consumers in the Energy sector. Offline customers would not have an enrolled digital identity and there are limited mechanisms to verify the consumer is the user attempting to access their data.

Enabling requirements to digitally register such offline customers before they can access their CDR data is one option, but it may also result in different consequences. One example is if an online account is required for energy switching under CDR Action Initiation. A customer seeking to churn from one energy retailer to another may be required to digitally register with their existing retailer just to churn away which could result in higher friction. Changes to the CDR rules would also be required to facilitate the online activation of 'offline customers'. This is not to say that is not a valid pathway, but it would mean the Chair cannot presently define binding data standards for online registration.

There is also the question of investment in uplifting security. Whilst banking represents an industry with strong investment in authentication, that is not always the case for the energy sector where retailers are typically a smaller size with less funding.

Practically speaking, strong customer authentication measures could be put in place for consumers that have online access independent of industry but this still leaves a significant cohort of consumers who do not have online access with limited options where strong customer authentication cannot apply.

[10] ACSC Information Security Manual; https://www.cyber.gov.au/sites/default/files/2023-06/Information%20Security%20Manual%20%28June%202023%29.pdf

Broader support for authentication factors beyond OTP is proposed in Decision Proposal 327: Authentication Uplift Phase 1.

4.2. Multi-factor authentication

Multi-factor authentication (MFA) is when a user is required to present a combination of two or more authentication factors in order to access a service or system. According to the Commonwealth Bank, "MFA reduces the risk of unauthorised access because even if an attacker has one factor – like a password – they can't complete the authentication process without the second factor". Microsoft claims that using MFA would stop 99.9% of account compromises from password-related attacks such as credential stuffing, password spraying, and brute-force.

Multi-factor authentication requires the user to provide verification for two or more factors of authentication.

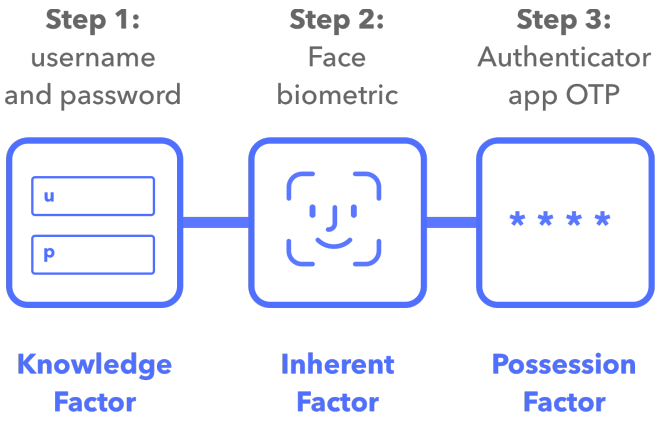


Figure 3 When two or more authentication factors are required to access a resource it is known as multi-factor authentication

Table 7 highlights the common categorisation of authentication factors according to OWASP.

Factor	Examples
Something You Know	Passwords, PIN codes and security questions.
Something You Have	Hardware or software tokens, certificates, email, SMS and phone calls.
Something You Are	Fingerprints, facial recognition, iris scans and handprint scans.
Location	Source IP ranges and geolocation.

Table 7 OWASP examples of authentication factors, Multi-Factor Authentication Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html)

Some authentication providers also consider a fifth factor based on the user's behaviour often referred to as Behavioural Biometrics or Behavioural Authentication. Behavioural Biometrics considers how the user interacts with their device and monitors the patterns of a person's unique movement characteristics representing a "behavioural fingerprint".

Factor	Examples
Something You Do	Keystroke movement, device movement, touchscreen pressure.

Table 8 Behavioural biometrics are increasingly considered as an emerging authentication factor

When the user is required to verify two factors, this is commonly referred to as Two-Factor Authentication (2FA) but it is still a specialisation of MFA.

Increasingly, MFA is becoming a requirement to protect consumer data and counteract the increase in phishing risks and data hacks.

1. The NIST guidelines now require the use of multi-factor authentication for securing any personal information available online.

   Any PII or other personal information — whether self-asserted or validated — requires multi-factor authentication. Therefore, agencies SHALL select a minimum of AAL2 when self- asserted PII or other personal information is made available online.

2. The Australian Cyber Security Centre (ACSC)'s Information Security Manual (ISM) recommends multi-factor authentication, with passphrases as a last resort if that is not possible:

   a. *Multi-factor authentication is used to authenticate unprivileged users of systems (ISM-0974)*
   b. *Multi-factor authentication is used to authenticate users accessing important data repositories (ISM-1505)*

3. The EU's Payment Services Directorate (PSD2) mandates Strong Customer Authentication, involving at least two authenticator factors (Article 97 and Article 4 (30))

   "Member States shall ensure that a payment service provider applies strong customer authentication.

   'Strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data."

MFA is becoming the de facto minimum requirement for authentication. Enabling Data Holders to enforce MFA would not only align to prevailing best practice guidance it would further align to the security practices employed by many Data Holders in non-CDR channels.

4.3. Step-up authentication

Step-up authentication is a balance between security and consumer friction that adapts authentication assurance to the risk level of the data being requested, or action being initiated. Step-up authentication allows users to perform certain actions or access certain data with a lower level of assurance but requires the user to 'step up' their assurance level to perform other more risky actions. An example might be transferring funds over $200 to domestic bank account, updating your contact details with your bank, or opening a new term deposit account.

Step-up authentication is a way to present contextual, time-limited authentication challenges based on risk-based criteria including:

- the time since last successful authentication,
- What previous authentication methods have been verified, and
- The sensitivity of the action being initiated and location of the user accessing the system.

Step-up authentication allows for security controls that can adapt authentication requirements to the importance of the resource being accessed, and the risk level if it were to be exposed.

A risk profile might also assess[11]:

- *IP reputation: Is someone attempting to login from an IP address associated with previous dubious requests?*
- *Impossible travel: Frequency of requests from different geo-locations*
- *Known device: Whether the device is recognised or not*

In banking and online commerce, a common example of step-up authentication is the payment step where the payment amount is above a certain threshold, to a new payee or an overseas destination. In this instance, the service provider would present an additional challenge (e.g., a PIN code or SMS OTP) that the customer must verify before the payment initiation is accepted.

Adaptive authentication controls provide Data Holders with better security options but may come with comprises to consumer usability. The balance between increased security and ease-of-use is an important consideration. Principles, and even consumer experience standards, that help govern when and how step-up authentication can be employed could help balance the needs of security and usability[12].

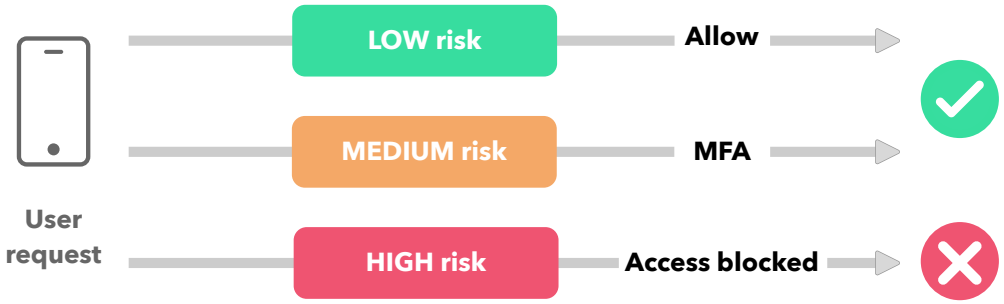
Supporting adaptive authentication is a departure from the existing authentication requirements which require consumer authentication *only at the point of authorisation*. Moving to a risk-based authentication framework would allow Data Holders to present

[11] https://auth0.com/blog/what-is-step-up-authentication-when-to-use-it/
[12] https://www.notion.so/d61cds/Decoupled-Research-Report-Q2-2023-R3-38ac4e3ef4954b1f85d25a6f17835d26?pvs=4#77f6d35446f049e7b9f527534af1ca66

authentication challenges *after* successful consent establishment, during the lifespan of a valid authorisation.

4.4. Adaptive authentication

Step-up authentication is a static assessment of risk. Adaptive authentication, sometimes referred to as risk-based authentication, is similar to step-up authentication but it is dynamic instead of static. Authentication policies define risk-based criteria which trigger additional authentication challenged, depending on a user's risk profile and the sensitivity of the resource being accessed.



Many times, this means adaptive authentication provides a "silent" layer of security to consider vectors of risk. For example, a risk policy might assess, amongst other things:

- IP reputation: Is someone attempting to login from an IP address associated with previous malicious or fraudulent requests,
- Impossible travel: Are temporally close requests coming from different geo-locations that would be unfeasible to make (e.g., two requests coming from different sides of the world within seconds of each other),
- Known device: Whether the device is previously recognised or not,
- Location: Is the user making the request from a location they normally would,
- Time: Is the user making the request at an unusual time compared to their previous request history

4.5. FIDO Credentials / Passkeys

Passkeys are cryptographic credentials stored securely on a user's device that avoid the need for password credentials. Passkeys are more secure than passwords because they consist of a public/private key pair with the public key bring provided to the website or service you log in to, and the private key being securely stored on the user's device. Passkeys are developed using Fast IDentity Online 2 (FIDO 2) protocols. Whilst smartphone manufacturers are now embedding FIDO 2 capability into their devices (e.g., Apple iOS devices and Google Android devices), users can also user their own physical FIDO 2 key (e.g., Yubico).

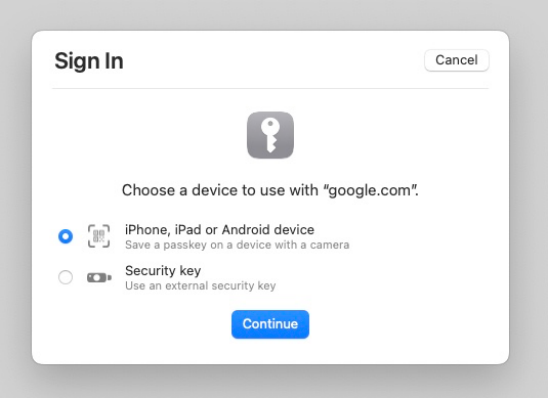


Figure 4 Example Passkey challenges for authentication. Source: Tom's Guide

Supporting FIDO credentials would not only change the authentication challenge, but it would also change the need for a Customer ID selection step thus streamlining the authentication flow where a FIDO credential has already been registered.

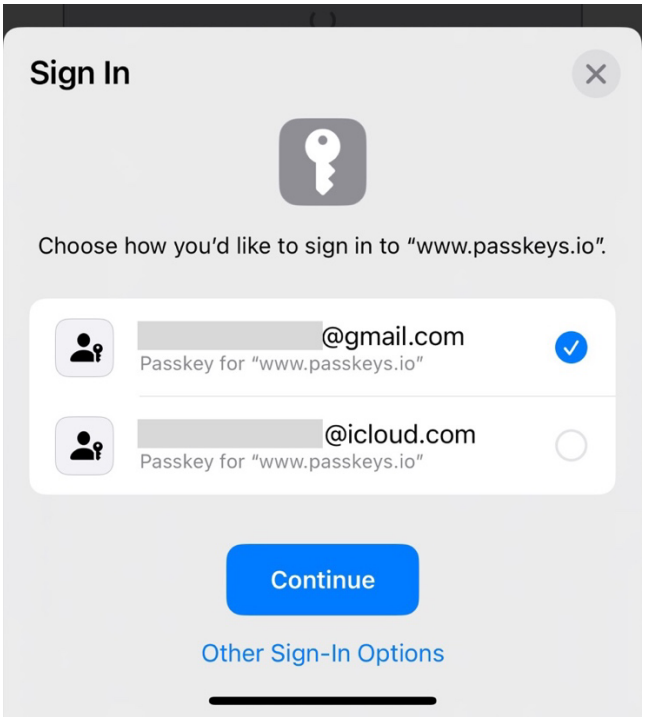


Figure 5 Sign in using an existing Passkey registration

Given the presentation of passkeys may vary widely, it is anticipated that CX guidelines and data language standards would be proposed to ensure there is familiarity for consumers.

Consultation questions

1. Are there any accessibility considerations with supporting step-up authentication controls?
2. Are there any sector-specific considerations to support step-up authentication controls?
3. How might the Data Standards accommodate enrolment for FIDO credentials, including any consumer experience considerations?
4. How might the standards accommodate the loss or recovery of a FIDO credential?

5. Interaction Flows

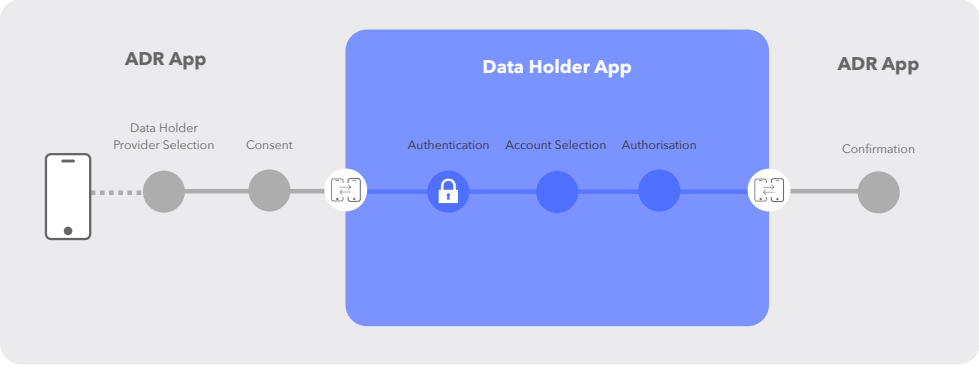
Interaction flows are the ways in which a consumer interacts with establishing authorisation. This can include how the consumer is "handed off" between the ADR and Data Holder along with the channel the consumer is interacting with. Different interaction flows may move the consumer between multiple channels where this aids the consumer experience. An example of such channel switching is an in-store checkout experience where the consumer interacts with a point-of-sale terminal to scan goods and is then prompted to make payment using the retailer's smartphone application. How the two channels are linked can vary but typically include the sharing of a shared set of information or key to bind the two channels.

Interaction flows also consider *how* the consumer is moved between channels. This may include a push-based mechanism, such as the UK's App2App redirection model, where the redirect is to a registered app URL on the user's smartphone that seamlessly switches them from the ADR app to the Data Holder app. It may also be a pull-based interaction flow like a kiosk scenario. In the UK, the open banking standards support a variety of interaction flows including decoupling the authentication challenge from the rest of the authorisation flow use agreed consumer identifiers.

The Data Standards permit a single Interaction flow at present which commonly referred to as the "Redirect with OTP" flow. This flow permits a consumer to originate through an app or web experience with the ADR before being redirected to the Data Holder's web flow. This flow provides for a universally consistent experience to connect ADR and Data Holder so the consumer can establish data sharing arrangements. Whilst useable, it is not always the most ideal interaction flow under all circumstances. In the United Kingdom for example, the Open Banking standards permit other flows like:

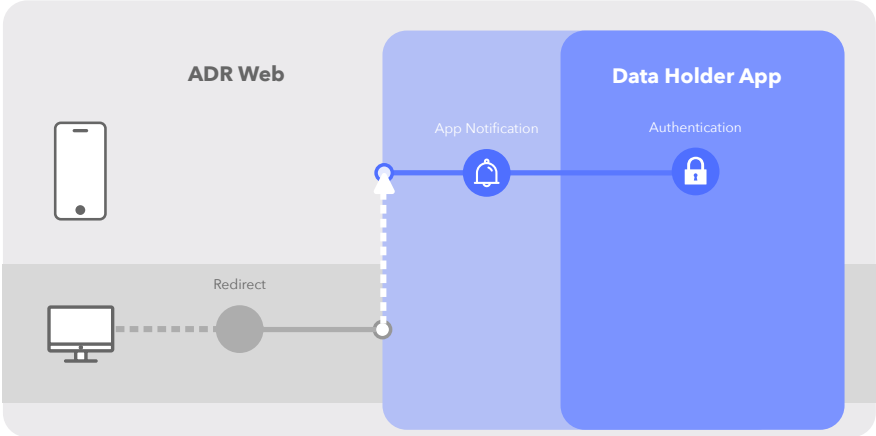
(a) **same device-coupled flows**

a. **app-to-app (App2App)** when there is a supporting Data Holder application installed the user is shifted between two apps on the consumer's trusted device

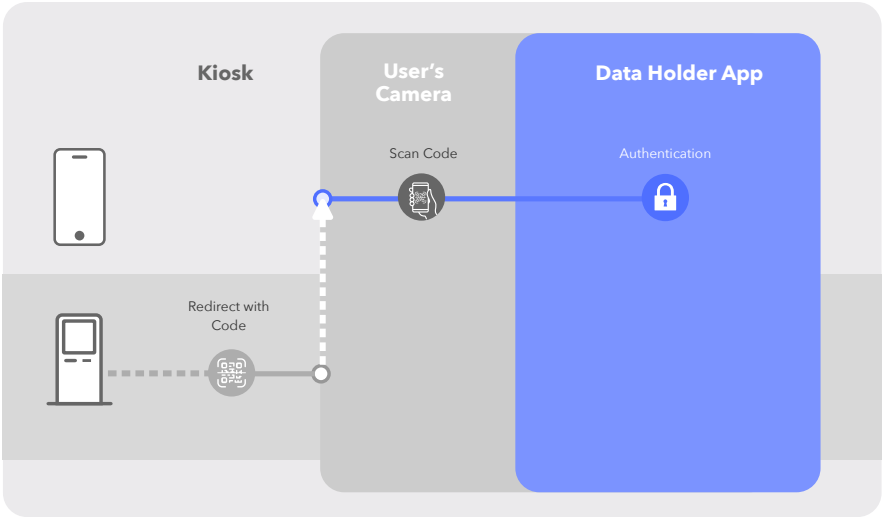


(b) **decoupled flows** where the user can establish authorisation on a separate authentication device to the consumption device. From a consumer perspective, these can be separated as follows:

a. **consumer-owned device flows** where the user commences consent establishment on a consumption device like a desktop browser and completes the authentication and authorisation stages on their authentication device like their smartphone often by way of a push notification.



b. **public / kiosk flows** where the user can establish authorisation by interacting with a public kiosk (e.g., a point-of-sale checkout terminal or their accountant's computer) that allows them to continue the consent journey on their own trusted device often by way of a client (ADR) presented binding code like a QR code.



With both consumer-owned and kiosk flows, both push-based and pull-based approaches could be considered.

[Decision Proposal 327: Authentication Uplift Phase 1] considers the introduction of X2App interaction flows in Phase 1 which will improve the consumer experience for same-device journeys.

5.1. Improved consumer experiences with same-device interaction flows

Coupled interaction flows are where the consumption device and the authentication device are the same. In other words, the consent flow is carried out on a single device. This is how the existing Redirect with OTP flow works. Whilst the device is the same, the consumer may move between an app and a web view to complete parts of the process depending on how the hand off occurs between the ADR and Data Holder.

The Data Standards support Web2App and App2App interactions flows but they don't currently support flows that direct the consumers to their Data Holder app.

Supporting these flows would extend the Data Standards for same-device interaction flows whilst offering significant security, usability and consumer experience improvements.

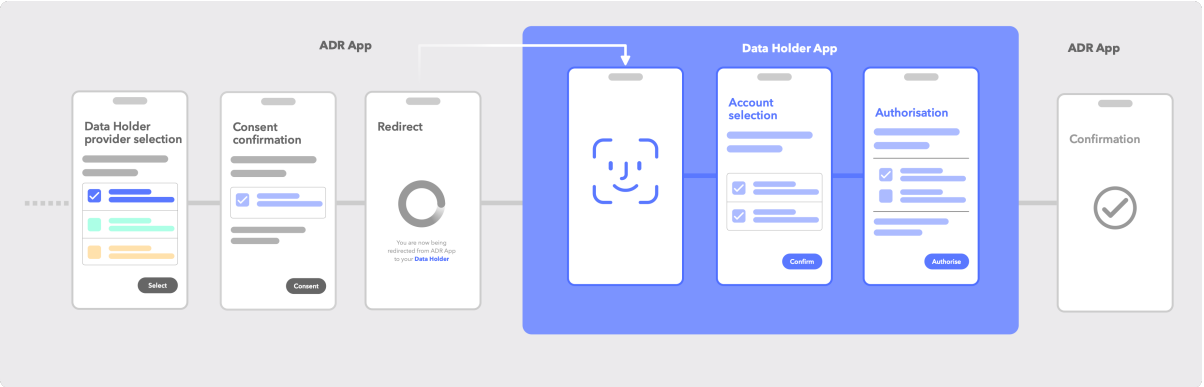


Figure 6 App to app (App2App) redirect seamlessly laucnhes the Data Holder's app using a deep-linking process.

An important consideration with the Web2App and App2App interaction flows is whether they are required by the Data Standards (for example, if the Data Holder has an available app that is installed on the consumer's consumption device). Supporting these interaction flows would mean through a method of deep linking the consumer would be authenticated through their Data Holder app using the same credentials and authentication methods (for example, a biometric) they normally use when directly accessing their accounts using the app.

A high-level interaction flow might look like:

1. During the consent flow, the Consumer selects their chosen Data Holder at the Data Holder provider selection step within the ADR app.
2. A redirection invokes the chosen Data Holder app on the same device where the Consumer authenticates with the Data Holder app.
3. The Consumer is presented with an authentication challenge from the Data Holder app in accordance with the allowed authentication methods and standards.
4. If the Data Holder offers multiple customer profiles, the Consumer is asked to select which profile they are interacting as.
5. The Consumer is taken straight to the screen (deep-linked) where they can select their accounts and confirm their authorisation.

6. The Consumer is redirected straight back to the ADR app on the same device.

Facilitating x2App flows is technically fairly straightforward and is widely supported by iOS and Android devices. Using a feature called "app-claimed" http URLs — also known as "deep linking" ('Universal links' on iOS or 'App Links' on Android) — recommended in BCP 212 – OAuth 2.0 for Native Apps it provides a secure and widely supported mechanism for mobile apps to automatically launch the user to a defined location within an installed app. For this mechanism to work, both the Data Holder app needs to claim their registered authorisation URL and the ADR app needs to claim their registered redirect URL.

Supporting x2App interaction flows is dependent upon support for alternative authentications methods beyond OTP. Typically, apps are secured using a password, PIN code or biometric and the Data Standards would need to accommodate equivalent authentication measures.

5.2. Enabling authorisation flows across devices with decoupled interaction flows

This work package addresses Recommendation 13: Alternative Authentication Flows of the Independent Information Security Review.

Decoupled interaction flows are where the consumer starts the consent flow on one device, such as a desktop computer, but completes the authorisation on a second device, such as a smartphone. These sort of interaction flows allow the consumer to move from the initiating device to the device they use for authentication. The benefit of these flows is that they support a variety of scenarios where a consumer is dealing with an untrusted or public device they don't want to enter security credential into, or they have enrolled a trusted device for a passwordless authentication which improves their experience when logging into a variety of devices.

How the decoupled flow is initiated falls into two broad categories:

- **push-based mechanisms** where the consuming device pushes a request for authentication to the authentication device; and
- **pull-based mechanisms** where the consumption device presents a binding message that the consumer then scans using their authentication device. In this scenario, the consumption device can also offer the consumer the option to continue the consent flow on the consumption device, like their desktop as a fallback.

5.2.1. Push-based decoupled interaction flows

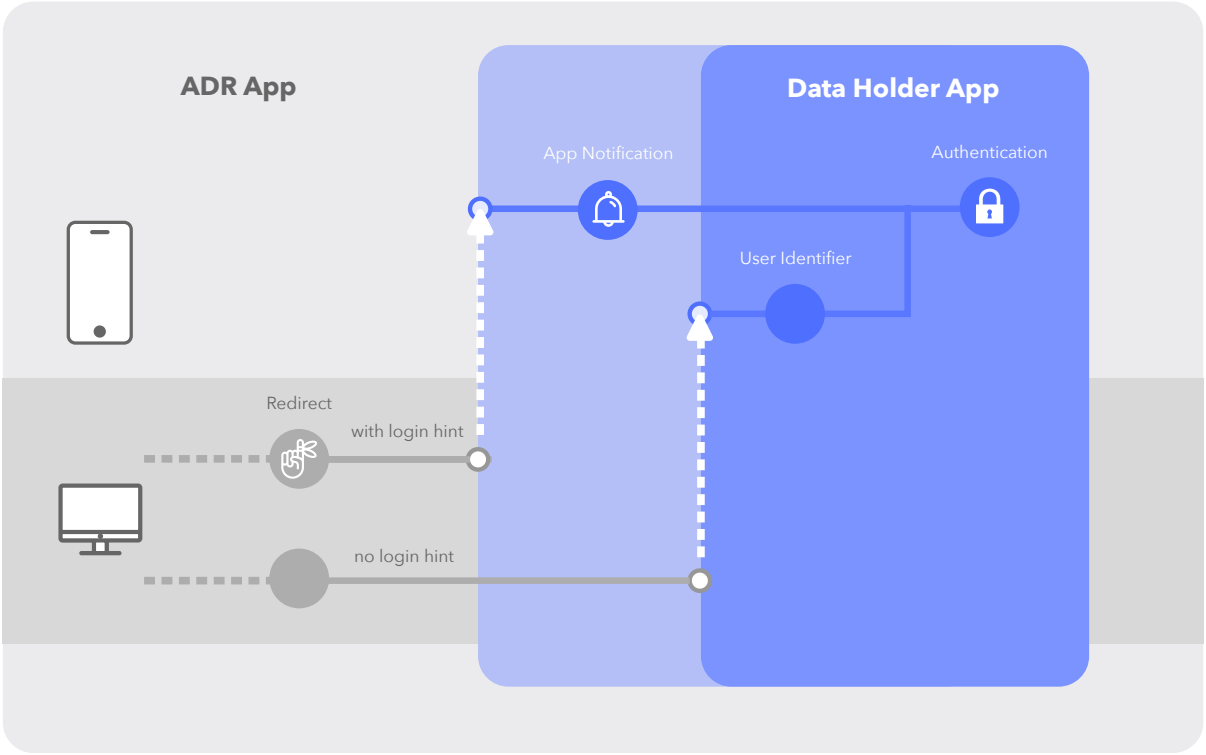


Figure 7 High level flow diagram representing opportunities to streamline authentication when the consumer has previously established consent. Fallback to user identifier entry is also represented.

These interaction flows allow the hand off from the consumption device via a mechanism that “pushes” the user onto their authentication device. The consumer must then successfully authenticate based on the challenge the Data Holder presents such as a biometric which may include a binding challenge code.

A commonplace example of push-based authentication is the presentation of a random secret on the consumption device that the consumer must correctly input on their authentication device *after* an initial authentication challenge like a biometric. TDIF role requirement CSP-04-02-03g provides guidelines for the supported options allowing directional transfer of the secret across consumption and authentication devices. The key approach is to bind the consumption and authentication device through a shared secret.

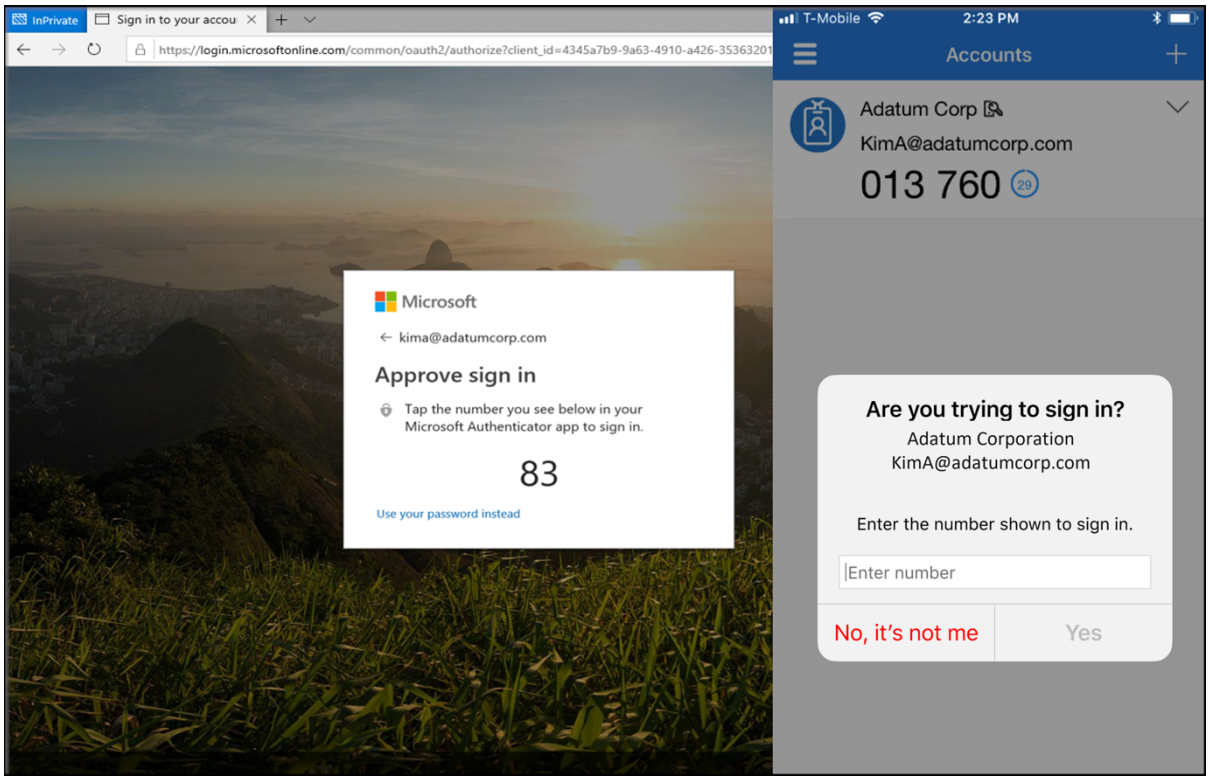


Figure 8 A Microsoft example of push to approve with biometric and challenge code. Authorisation confirmation can be presented after a successful authentication challenge. Source: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-au

FAPI supports decoupled authentication using the Client Initiated Backchannel Authentication (CIBA) specification, of which there is a FAPI variant. This specification supports different "flavours" of initiation. They are:

1. **"push mode"** which is explicitly not allowed by FAPI-CIBA[13];
2. **"poll mode"** where the client calls an endpoint hosted by the Data Holder to retrieve the outcome of the authentication result;
3. **"ping mode"** where the Data Holder posts a unique identifier of the authentication session to the client (the client has registered a callback URL for the ping as part of their client registration setup), and the client then retrieves the authentication result from the Data Holder.

These mechanisms establish a technical approach that supports the consumption device waiting for a message back from the authentication device.

5.2.2. Pull-based decoupled interaction flows

These interaction flows present a binding code that the consumer scans with their authentication device to bind the two channels. Once the authentication device has the authentication context it requests successful authentication from the consumer to complete the authorisation flow.

[13] Refer to ref 5.2.2 (3); https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_CIBA.md

The below options are not mutually exclusive. None or all options may be preferred and supported.

Scanning ADR generated codes

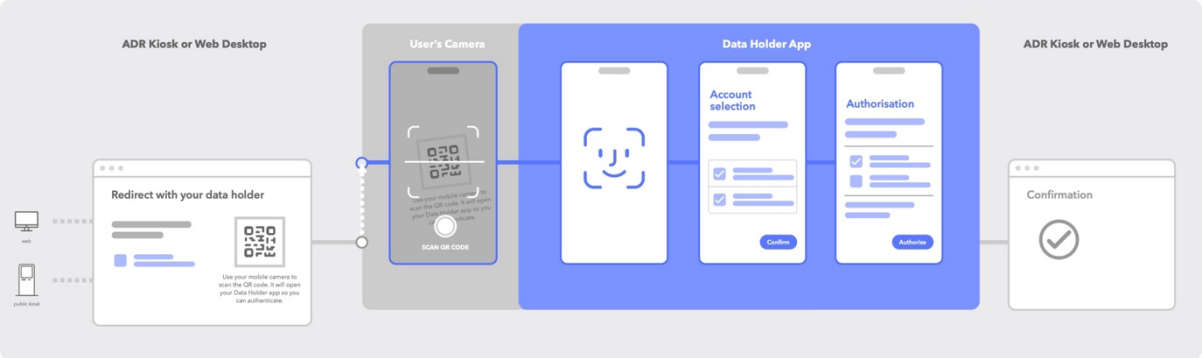


Figure 9 Decoupled flow where the ADR presents a binding code that allows the authentication device to links to the consumption device

This could be a Near-Field Communication (NFC) or Quick-Response (QR) code.

For this flow to work, it is assumed that knowledge of the consumer's chosen Data Holder is required so that the code can be generated with the appropriate login hint for the Data Holder and consumer. Alternatively, it may be an embedded location for the Data Holder to call back to obtain information of the authorisation.

This flow is useful where the consumption device doesn't allow selection of the Data Holder or doesn't allow the consumer to continue the flow without a trusted device in their position. An example of this is a supermarket checkout that has details about the goods in the cart and the price but does not know the funding source the consumer wishes to pay with. The consumer can then use their banking app to complete the authorisation and purchase.

Scanning Data Holder generated codes

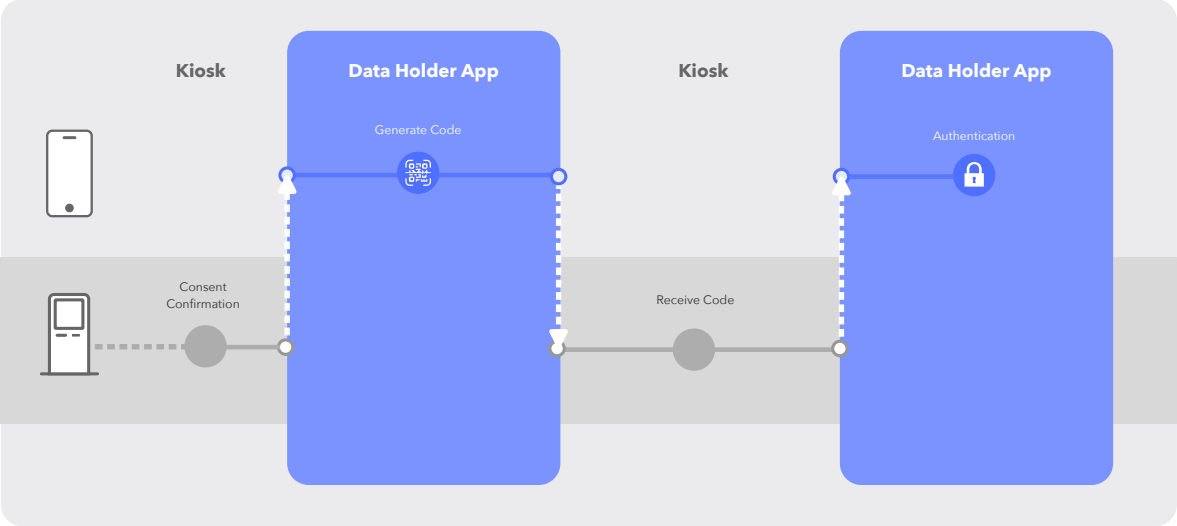


Figure 10 Decoupled flow where the Data Holder generates a binding code that the ADR can use to connect the consent flow together

This could be an NFR, QR or an alphanumerical code.

For this flow, the ADR continues to a standard redirect flow on the consumption device. It is then the Data Holder which presents a QR code generated by the Data Holder for the consumer to scan. In this way, the ADR isn't involved in the QR code generation.

5.3. Streamlined re-authentication using login hints

With all interaction flows including decoupled flows, there is a further opportunity to streamline the consumer's experience for re-authentication scenarios.

OpenID Connect allows the oAuth client to offer a "login hint" to the authorisation server that serves an identifier for the end-user that is authenticating with the authorisation server. This hint is used by the authorisation server to determine the end user and present the authentication challenge for the end user without requiring the user to input a user identifier like a username or Customer ID.

OpenID Connect supports a shared identifier, known as a "login hint", that uniquely identifies the user (like an email address, phone number or subject identifier), or an ID Token previously issued by the authorisation server to client. By extension, CIBA supports an additional hint type known as "login hint token" which is a JWT[14] token containing information identifying the end-user for whom authentication is being requested.

CIBA does not recommend the use of widely known user identifies like phone number of email address as the login_hint in the authentication request because "an attacker could start unsolicited authentication sessions on large numbers of authentication devices, causing distress and potentially enabling fraud"[15].

Since the Data Standards do not support user identifiers being input on the ADR side, all authentication processes are conducted within the Data Holder's domain. As such, considering login hints that are widely known is less of an issue provided they are signed as a JWT-based hint because the Data Standards would not permit the user to manually enter a user identifier on the ADR side. This would only hold true provided the ADR didn't previously collect that user identifier as part of a registration process that occurred on the ADR side (e.g. signing up for an account with the ADR and providing the email address).

If valid concerns remain, then a login hint should only ever be used where the hint is provided by the Data Holder after a successful authorisation. This could be a new "nonce" or bound identifier used only for the purposes of re-authentication.

Further, CIBA recommends implementations consider Subject Identifiers for Security Event Tokens to define appropriate subject identifiers.

These considerations will be presented in future Decision Proposals with options presented for feedback.

When a login hint is available, it improves the experience for the consumer by removing unnecessary friction from the authentication flow as represented in Figure 11. In this scenario, the decoupled interaction flow presents an ADR passing an authorisation request

[14] JWT stands for JSON Web Token. JSON stands for JavaScript Object Notation.
[15] https://openid.net/specs/openid-financial-api-ciba.html#authentication-sessions-started-without-a-users-knowledge-or-consent

with a secure login hint claim that is supported by the Data Holder. Upon receiving the login hint, it allows the Data Holder to push an authentication request to the consumer's authentication device to authenticate them, and then, authorise the CDR request.

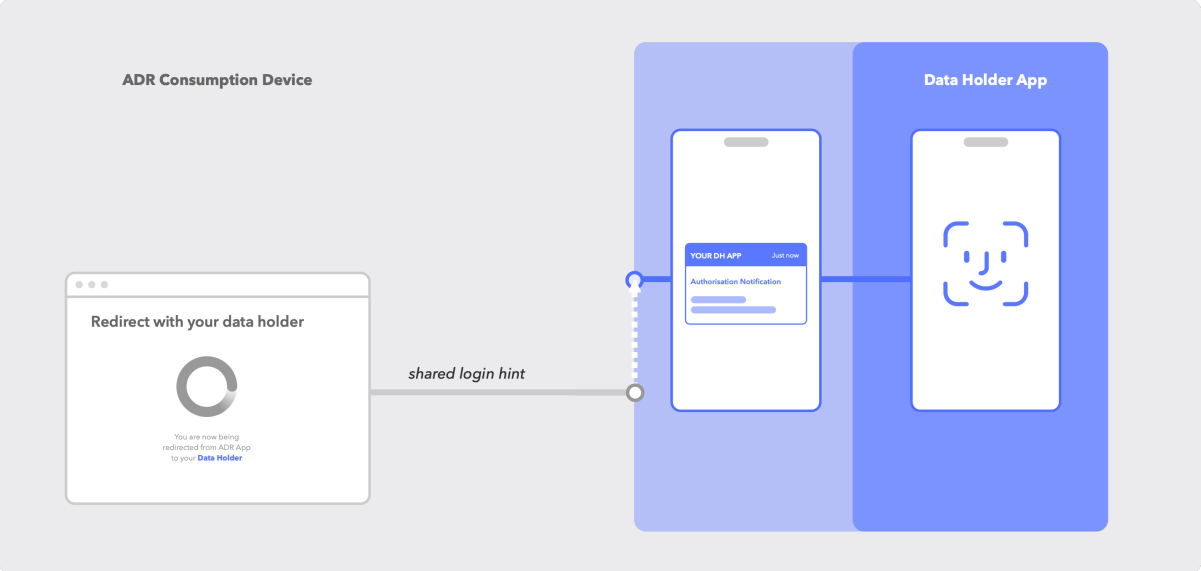


Figure 11 A decoupled authentication flow that uses a login hint to streamline authentication without the need for the user to provide a user identifier.

When a prior login hint is not available, the consumer experience would fallback to existing redirection flows. In the case of decoupled interaction flows, the user identifier would be entered on the consumption device on the Data Holder side after the ADR has redirected to the Data Holder's domain. This may be a supported pattern for decoupled authentication where the user controls both the consumption and the authentication device. However, this is unlikely to be recommended for kiosk scenarios where the consumer does not have control of the consumption device. Entering a user identifier on the consumption device would also be against security best practice, and would unlikely meet consumer expectations. Pull-based decoupled interaction flows represent a better option for kiosk-based scenarios.

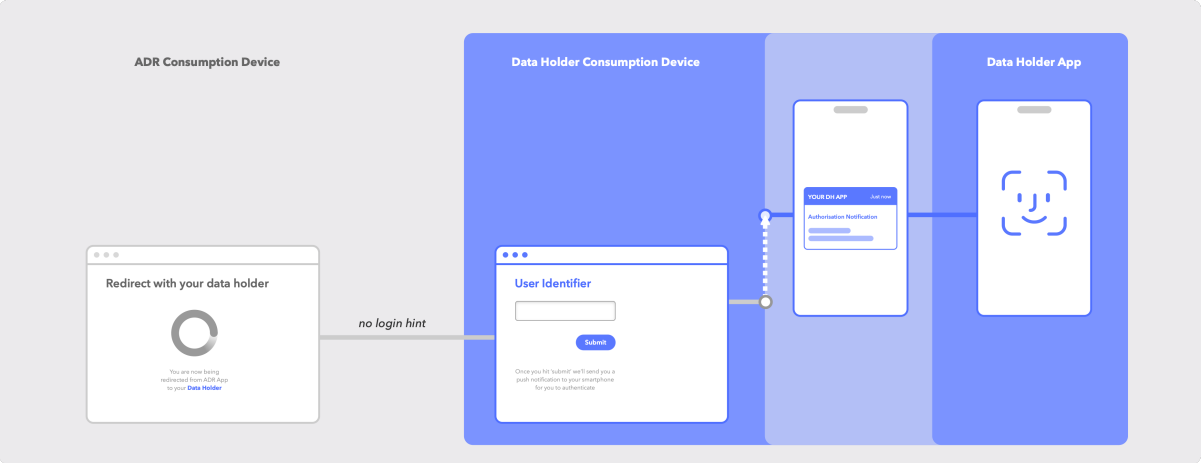


Figure 12 A decoupled authentication flow where no prior login hint has been established

Consultation questions

5. Are there any other interaction flows that the Data Standards should consider supporting?
6. Should the Data Standards consider requiring or recommending certain interaction flows in specific use cases?

6. Federated identity including business SSO

6.1. Digital ID / Trusted third-party federated identity login

Federated identity is a "process that allows the conveyance of identity and authentication information across a set of networked systems"[16]. It allows a user to log in using an identity provider that is independent of the resource server. A common example is using a social login like Google or Facebook to access web services of separate organisations like Spotify or Instagram without the need to create a login and password with the web service provider. How, or if, the CDR considers federated identity standards would likely be limited to accredited TDIF Identity Service Providers.

The government's Digital ID initiative establishes a framework for trusted identity providers to act as an Australian citizen's single login across a variety of services. myGovID for example provides a single login to citizens to verify their ID across a range a range of government services without having to verify identity documents with each government service individually. The Digital ID initiative supports both government identities like myGovID as well as commercial identity providers including Australia Post Digital ID and ConnectID.

Recognising trusted identity providers in the CDR could offer many consumer benefits including reducing risks of data theft, improved convenience and a better experience. Rather than Data Holders individually providing a digital identity and separate authentication process, the authentication of the consumer would be delegated to one of the trusted identity providers. When the consumer has previously connected their trusted Digital ID with their Data Holder, this presents a safe and secure way for the Data Holder to authorise consumer data sharing without necessarily being the identity provider. This approach could also expand to consumer authentication with ADRs so the consumer has a single login to access the services of their ADR and Data Holder. This adds further benefits by reducing the number of steps in the consent flow because it could streamline the authentication process during consent either ameliorating the need for re-authentication with the Data Holder, or only requiring a step-up authentication challenge at authorisation with the Data Holder.

6.2. Business Single-Sign On (SSO)

Similar to TDIF accredited identity providers, Data Holders sometimes offer corporate customers to connect their enterprise access management systems to their Data Holder

[16] NIST Digital Identity Guidelines Appendix A – Definitions and Abbreviations. https://pages.nist.gov/800-63-3/sp800-63-3.html#def-and-acr

applications. With this approach, the business consumer in effect brings their own trusted identity provider – typically their workforce identity and access management system – allowing the business to better control access to external systems outside their own corporate network. This makes managing access policies easier and allows their workforce to use their workforce ID to access third-party systems. It also makes it easier for businesses to seamlessly handle user deprovisioning and access rights using centralised enterprise identity management policies.

Change Request 542: SSO as an alternate authentication method proposes changes to authentication standards to enable single-sign of for business consumers.

If SSO is allowed by the Data Standards, it would be expected that this could be defined as a permitted authentication flow with accompanying CX standards and guidelines, whilst allowing Data Holders to align to their current practices provided they meet the required security thresholds.

6.3. Delegated authority authorisation

Delegated authority management provides mechanisms for a user to delegate their permissions and authority to one or more delegated users. A commonplace example is role-based access controls where different rights or permissions are granted to different user roles (e.g., a business owner setting up their bookkeeper with permissions to collect bank feeds and reconcile accounts in their accounting software). Delegated authority can allow users to manage fine-grained relationship-based access control.

The CDR rules currently support a category of delegated authority referred to as nominated representatives which allows non-individual consumers to grant permissions to the named persons who can act on behalf of the non-individual consumer.

But there are many other examples of delegated authority that occur in our lives, especially for individual consumers, that could also benefit from standards that support delegation of authority in the CDR.

Family delegation: Consumers could extend their authority to family or household members to act on their behalf. This could be a guardian managing the banking choices of a minor, a flatmate being allowed to access energy data, or a partner being able to update household contact details for utilities.

Professional delegation: Consumers could delegate professional classes of peoples to establish data sharing on their behalf whilst remaining in control of their data sharing consents. The CDR rules permit the disclosure of data to Trusted Advisors which could be the spoke of this style of delegation.

Powers of attorney and guardianships: Consumers could manage authorisation for their delegates to have authority to represent them on digital services and applications.

Instead of the consumer performing the authentication and authorisation steps themselves using the ADR services that are controlled and managed by the delegated user, consumers could benefit from greater control and security if they could delegate their authority with permissions they can fully manage. In the example of Trusted Advisor use today, a consumer would complete the data sharing consent, authentication and authorisation

processes at the guidance of their Trusted Advisor so their CDR data could then be collected by the Trusted Advisor. The consumer loses some control in this scenario because there is no way for them to limit the extent of CDR data that is collected and possibly used by the Trusted Advisor other than limiting which data clusters and accounts that are selected.

An alternative approach might be allowing consumers to nominate named persons that are given delegated authority, possibly temporarily. This access could be constrained using fine-grained permission management that limits, amongst other things, the historical time period of data that is collected, the actions that can be performed, or types of accounts that can be accessed. These permissions could then be granted to the delegated user by giving them a temporary authentication code, or by onboarding them with a login credential that is bound to the permissions the consumer has given them. In this way, the delegate can only ever access the CDR data in the way the consumer wants it to be accessed.

Furthermore, minimum authentication requirements could be tied to the authenticating end user, not just the consumer. Because the consumer remains in control of their data using their Data Holder authorisation dashboard, they can manage usage and revoke access to delegates at any point in time.

The consumer could even pre-establish certain permissions templates for classes of users (e.g., a doctor or accountant).

Consultation questions

7. How might the Data Standards consider interoperability with the federation of trusted digital identity providers for individual consumers?
   Such mechanisms may allow a consumer to authenticate using a common identity provider. An example of this is a consumer authenticating with a MyGovID which allows them to access a variety of government services including the ATO, Centrelink and Medicare

8. How might the Data Standards enable individual and non-individual consumers delegated authority to people such as their Trusted Advisors, powers of attorney, or secondary users?
   Presently, a consumer must authenticate themselves to allow their Trusted Advisor to collect data. Delegated authority mechanism may allow the consumer to allocate access credentials to their delegated authority. These access credentials may be time bound, constrained to certain accounts, data sets or even data ranges. In such scenarios the consumer would remain in control of the Data Holder CDR dashboard to revoke or amend the authorisation at any time whilst permitting the delegated authority to manage data collection on their ADR dashboard.

9. Other than supporting SSO within a Data Holder's domain, should the Data Standards consider Identity Service Providers that are not TDIF accredited, and if so,

why?

10. What role, if any, should NIST's Federation and Assurance guidelines play in informing federated identity standards?

11. What role, if any, should OpenID Connect Federation 1.0 play in informing federated identity standards?

12. Are there any other normative standards, guidelines or security approaches that should be considered if SSO and federated identity were supported by the Data Standards?

6.4. ADR Authentication: protecting data held by data recipients

Authentication controls for ADRs, and by extension accredited and non-accredited persons, are not considered in the related decision proposal. Whilst there may be very valid reasons to consider authentication standards for how consumers and their trusted advisors access consumer data on an ongoing basis, this would require significant changes to the processes of ADRs today.

The Chair has a requirement under the CDR rules to ensure the security of CDR data. This extends to the collection and storage of data by ADRs.

As data is accumulated by ADRs across multiple industries, the centralisation of CDR data for a consumer may present increased data sensitivity and security risks. The accumulation of consumer data may result in threat actors attempting to access this through access 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 ADRs.

Decision Proposal 225 – Data Recipient Security Standards invited feedback on the implementation of authentication controls for ADRs however there has been no decision on the direction of standards being applied to ADRs.

Consultation questions

13. What should be considered if authentication controls are required for ADRs?
14. Should ADRs adopt the same authentication standards that are required Data Holders?

7. Beyond authentication uplift

Holistic security profile uplift

This noting paper and **Decision Proposal 327: Authentication Uplift Phase 1** focus on the uplifting the consumer authentication standards. There are many other dimensions to the security of the CDR when protecting consumer data that will be considered, including migration to FAPI 2.0 support, as part of a holistic Security Profile uplift consultation.

To ensure the Data Standards are fit for purpose, the current Security Profile requires uplift in a number of areas as outlined in **Decision Proposal 182 - InfoSec Uplift for Write**. Key areas include:

- FAPI profile alignment and migration to FAPI 2.0, in turn making is simpler and more cost effective to implement
- Rich authorisation for a more expressive authorisation permissioning language beyond coarse-grained oAuth scopes along with supporting purpose-based consent
- Secure events and notifications between ADRs and Data Holders which may include threat and risk sharing between participants
- Supporting non-repudiation and message signing requirements for CDR receipts and verifiable credentials

Further to this, the Security Profile has undergone enhancements and extensions since version 1.0 of the Data Standards. As changes have been made, the Security Profile has grown in size and complexity to accommodate new rules and sectors. As part of the holistic Security Profile uplift, it is anticipated that a simplification of the security control statements is required. Alongside this, adoption of an RFC format for the Security Profile will be considered to achieve better international alignment in accordance with the many normative references cited in the Security Profile.

Finally, there are a number of outstanding change requests related to security which should be considered as part of a holistic Security Profile uplift.

Identity verification

Authentication is just one dimension to the securing of consumer data. Whilst it protects access to consumer data, it is predicated on the existence of a customer relationship. As the CDR moves into Action Initiation, including origination services, identity verification will be an important consideration. How the CDR, and consequently the Data Standards, solve for these requirements is out of scope of this paper.

Consultation questions

15. Are there other areas where the Security Profile should be extended or reviewed?

Appendix A

8. List of consultation questions

The questions for community feedback in this consultation are consolidated below:

Section 4: Authentication Factors

Consultation questions

1. Are there any accessibility considerations with supporting step-up authentication controls?
2. Are there any sector-specific considerations to support step-up authentication controls?
3. How might the Data Standards accommodate enrolment for FIDO credentials, including any consumer experience considerations?
4. How might the standards accommodate the loss or recovery of a FIDO credential?

Section 5: Interaction Flows

Consultation questions

5. Are there any other interaction flows that the Data Standards should consider supporting?
6. Should the Data Standards consider requiring or recommending certain interaction flows in specific use cases?

Section 6: Federated identity including business SSO

Consultation questions

7. How might the Data Standards consider interoperability with the federation of trusted digital identity providers for individual consumers?
   Such mechanisms may allow a consumer to authenticate using a common identity provider. An example of this is a consumer authenticating with a MyGovID which allows them to access a variety of government services including the ATO, Centrelink and Medicare

8. How might the Data Standards enable individual and non-individual consumers delegated authority to people such as their Trusted Advisors, powers of attorney, or secondary users?
   Presently, a consumer must authenticate themselves to allow their Trusted Advisor to collect data. Delegated authority mechanism may allow the consumer to allocate access credentials to their delegated authority. These access credentials may be

time bound, constrained to certain accounts, data sets or even data ranges. In such scenarios the consumer would remain in control of the Data Holder CDR dashboard to revoke or amend the authorisation at any time whilst permitting the delegated authority to manage data collection on their ADR dashboard.

9. Other than supporting SSO within a Data Holder's domain, should the Data Standards consider Identity Service Providers that are not TDIF accredited, and if so, why?

10. What role, if any, should NIST's Federation and Assurance guidelines play in informing federated identity standards?

11. What role, if any, should OpenID Connect Federation 1.0 play in informing federated identity standards?

12. Are there any other normative standards, guidelines or security approaches that should be considered if SSO and federated identity were supported by the Data Standards?

Section 6.4: ADR Authentication: protecting data held by data recipients

Consultation questions

13. What should be considered if authentication controls are required for ADRs?
14. Should ADRs adopt the same authentication standards that are required Data Holders?

Section 7: Beyond authentication uplift

Consultation questions

15. Are there other areas where the Security Profile should be extended or reviewed?