RAIDIAM

Standards for the Future

CDR Information Security Recommendations

Incorporating responses to
Data Standards Body consultation:
Decision Proposals 182
https://github.com/ConsumerDataStandardsAustralia/standards/issues/182

Prepared for

Australian Banking Assocation

July 2021

Table of Contents

About the Australian Banking Association

With the active participation of 22 member banks in Australia, the Australian Banking Association (ABA) provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators, and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive, and accessible banking industry.

ABA Lead: *Emma Penzo.*

About RAIDIAM

Raidiam is an identity and access management specialist, providing consultancy, architectural design, and technologies to drive secure data sharing globally. We have published research papers for the UK Government providing thought leadership on Authentication and Accreditation across ecosystems; we have contributed to writing security standards for the OpenID Foundation and Brazil Open Banking; and we have designed, developed and delivered entire open banking ecosystems in the UK and Brazil. We are committed to ensuring that all industries globally have workable frameworks and standards that offer the highest degree of protection for themselves, their customers, and their partners.

Raidiam Authors: *Ralph Bragg, Tim Johnson.*

CONTACT

For any enquiries regarding this publication, please get in touch at:

https://www.ausbanking.org.au/

Australian Banking Association, PO Box H218, Australia Square NSW 1215

+61 2 8298 0417

1 Introduction

This paper contains Australian Banking Association (ABA) recommendations on robust information security for the next major iteration of the Consumer Data Right (CDR) to enable use cases that require write access (incorporating payment initiation and action initiation).

A core tenet of the Consumer Data Right is that consumers have a right to control what data is shared about them and with whom it is shared. Australians must remain in control of their data resources and be able to exchange their data, selectively, for services at their discretion.

"Security and "trust" are therefore key to a successful CDR. Ensuring that the appropriate technical standards for information security are put in place to enable the CDR is vital. These technical standards need to accommodate both an extension in scope for open banking, as well as setting the template for expansion of the CDR to other sectors of the economy. As noted in Scott Farrell's review in December 2019:

"…Open Banking needs to work together with [other sectors] to form a single, broader framework…"[1]

Australia has the regulatory foundation to deliver the most advanced, multi-sector consumer data-sharing economy in the world and so can lead the way in globally recognised implementation. The ABA position is that the success of this ambitious functional scope is predicated on the appropriate Trust framework being put in place well in advance of functional scope development

In this paper, the ABA and Raidiam are proposing a future that works not just for 'Open Banking' but that can work for all consumers in all sectors. It is a future that will position Australia as a global pioneer in the development of a cross-sectoral integrated data economy – driven and enabled by the CDR.

1.1 Concepts

The conceptual framework for the CDR is clearly set out by the Office of the Australian Information Commissioner:

*"The Consumer Data Right (CDR) gives consumers greater control over their own data, including the ability to **securely** share data with a **trusted** third party."*[2]

---

[1] Farrell Report – Foreword, page v. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[2] https://www.oaic.gov.au/consumer-data-right/what-is-the-consumer-data-right/

"Security" and "trust" must therefore be key concepts and considerations in the successful implementation of the CDR. However, defining and then implementing these key elements must also depend on the functional requirements for the data being shared.

At present the CDR prescribes a technology framework for *read-only* data sharing i.e., the viewing of account information. The evolution of the CDR will require an extension of present functionality to include read/write operations[3], i.e., payment initiation and other actions. It is therefore imperative that the Trust elements[4] which presently underpin read only access be upgraded.

1.2 Objectives, Scope and Structure

This paper presents the ABA's recommendations for upgrading the CDR Trust elements. In so doing, it also discusses a number of other options which were considered as part of the review process. A key priority has been to ensure the security and long-term stability of core capabilities that will ultimately drive the success of the entire ecosystem.

Further, this paper provides a clear roadmap for the implementation of the recommended required Security and Trust elements, considering the complexity and assumed timelines for the enablement of read-write data access.

The scope of this paper is necessarily broad, given the scope of the proposed transformations.

We consider it important to start by providing a detailed analysis of the elements of Trust demanded by a comprehensive, functioning data sharing ecosystem. We look at how to implement these elements individually and then how to implement them across an entire ecosystem. We explore how the evolution of an ecosystem to cover new functionality leads to new technology requirements, and we review the options that exist for that technology, drawing on experiences from around the world. Finally, we will make recommendations, taking into account migration proposals and potential timescales required for the implementation of the necessary changes.

Section 2 of the paper provides a less technical 'Summary for Executives' focusing on the scope of the proposed CDR upgrade and various decision-making roles.

Section 3 onward is intended for readers with a technical background who will be responsible for leading the implementation of the Trust solution at their organisations.

---

[3] Also called Action/Initiation within Australian regulations.

[4] Trust is comprised of four elements: Security, Identity, Privacy/Control and Consent/Authorisation. Each will be expanded upon in the following sections.

2 FOR EXECUTIVES: CDR Trust framework upgrade requirements

This section is intended as a non-technical summary for Executives who need to understand the key issues regarding the upgrading of the CDR to support read/write access. Section 3 onwards provides detailed technical information aimed at those with the responsibility to implement the required standards within their organisation.

2.1 Recommendations

This paper makes the following recommendations:

1. **Adopt FAPI 2.0 for future best practice:**
    a. The CDR should move to adoption of the FAPI 2.0 family of specifications as soon as possible, to future-proof the entire ecosystem, future implementations and to promote the benefits of international best practise.
2. **Ensure and Preserve Interoperability:**
    a. CDR should support interoperability with relevant global open standards.
    b. CDR should adopt global open standards as issued and without customisation wherever possible
    c. Where deviations to the standard are deemed necessary:
        i. To request first that they be incorporated in the relevant global standard to continue to ensure interoperability.
        ii. To ensure that any unique local changes follow a robust and transparent change process and are by exception.

To support an efficient adoption of the FAPI 2.0 family, we recommend:

- ***Immediate***: Publication / clarification of timelines around the current requirements to upgrade from FAPI 1.0 (v6) to FAPI 1.0 (FINAL), in order to keep current standards up-to-date and secure.
- ***<3 months***: Consult ecosystem to confirm and publish preference and plan for adoption of the Grant Management API extension and RAR to support fine-grained consent
- ***<6 months***:
    - Review maturity of proposed standards, vendor implementation plans and support, and participant development pipelines
    - Confirm requirement to adopt the FAPI 2.0 family of specifications, within a suitable timescale, via a phased approach
    - Confirm timescales for retirement of the unregistered Australian custom OAuth 2.0 extensions (to support international alignment and harmony).

2.2 Overview

Any data sharing requires Trust. The core Trust questions are “Who”, “What”, and “How”. That is: ***Who*** is taking part in the data sharing, ***What*** data is each participant allowed to see, and ***How*** should that data exchange be secured. These questions are central in every use case: ranging from a normal consumer online service login, through to complex data sharing across an ecosystem.

Whilst the above understanding of Trust appears relatively straightforward its actual delivery becomes significantly more complex when moving from a consumer/service model through to a distributed network that requires consumer consent.

For example, a consumer logging on to see their own credit card transactions requires the consumer and the credit card provider (or ‘Data Holder’ (DH)) to agree and implement methods for confirming the Who, What and How. The consumer and DH must know who each other is, must be given control and visibility of exactly the correct data, and must be sure that the exchange is secure. Consent is implicit within this process, with the consumer self-consenting to seeing their own data.

Across a distributed network in a typical CDR use case, the consumer grants explicit consent to another party (the Accredited Data Recipient (ADR)) to see their transactions data. In this case the DH needs to identify *both* the consumer and the ADR, to validate that the appropriate permissions have been given *and* received, and to ensure that *all parts* of the exchange are secure.

Implementation is further complicated when the use case requires not just explicit consumer consent, but detailed, flexible explicit consent. Providing and using consent to *see* transaction information is conceptually straightforward, requiring account details and perhaps a time period. However, providing and using consent to *do* something (as is the case payments), requires more details and flexibility to specify information such as the receiving account, payment amount, time of payment, recurrence, and currency.

In technology terms, this is known as multi-dimensioned, fine-grained consent. This becomes significant for payments due to the bearing on risk and fraud liabilities.

If Trust is to be achieved across the full breadth of an information ecosystem all parties must agree to standards that deliver the Who, What and How of each and every transaction in a completely reliable way, i.e., clear and well understood Standards for the operation of Trust protocols. In technology terms, Trust can be expressed as covering the elements of Security, Identity, Privacy/Control and Consent/Authorisation.

The CDR has already published standards for Trust which were originally based on the global FAPI 1.0 standard for API Security. However, the CDR included bespoke amendments within its published standards to cover the elements of Privacy/Control and Consent/Authorisation. In addition to being bespoke, these amendments were targeted at the initial use cases required by the CDR which are all Read-only.

The Farrell Report[5] recommends the next evolution of the CDR to introduce read/write functions (suitable for payment initiation and action initiation). This functionality will require further amendments to the CDR Trust standards particularly focused on the elements of Privacy (to increase Consumer control and preserve data minimisation), and Consent (to accommodate fine-grained multi-dimensional use cases). The currently specified bespoke mechanisms are insufficient to meet the needs of Action-Initiation or more purpose driven use cases therefore the ABA recommends these bespoke mechanisms should be replaced in favour of standards and designs that meet all holistic needs of the CDR.

Global standards have continued to evolve in parallel with the objective of providing a core framework to implement Trust across the widest range of use cases across any data sharing Trust Framework. The emerging FAPI 2.0 protocol incorporates a comprehensive set of foundational standards for solving Security, Privacy/Control and Consent/Authorization requirements.

Given the trajectory for the global convergence of standards, decision makers should take the opportunity to align any emerging Trust protocols fully with international standards and in so doing share in the benefits that international partnerships can offer. The ABA considers that the alignment of CDR Trust standards with global models will be critical in minimising ongoing support and maintenance costs, and for securing the widest possible range of commercial vendor support.

FAPI 2.0 is now published as an implementer's draft[6], meaning this iteration is locked, stable, and ready for implementation. Therefore, key vendors supporting banks, future data holders and data recipients of the CDR are likely to adopt the draft standard with 6-9 months. Banks and other CDR participants should then be in a position to implement the data sharing rails, based on a global FAPI 2.0 gold standard, during 2022. This would provide a strong foundation to prepare to launch the first stage of CDR write propositions during 2023.

Restating the position, the ABA strongly supports the proposal to align the Australian CDR standards with the emerging international standard.

---

[5] https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report
[6] https://openid.net/specs/fapi-2_0-baseline.html

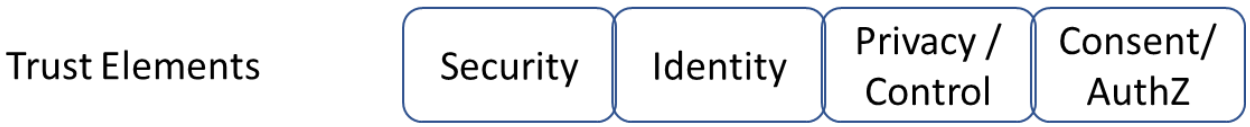
2.3 Principles of Trust

Any data sharing ecosystem requires Trust. This Trust needs to be multilateral (meaning it needs to accommodate many to many interactions) and unequivocal (strong and not breakable), providing surety between all participants for the core questions of "Who, What and How" connections can be made, and data can be shared securely.

The core Trust questions can more formally be expressed in the four elements of Trust:

- **Security**: ***(How) is this line secured?***
  the methods for ensure that any connection is secured, and so that any data transferred is received as it was sent[7], without being seen or manipulated by any external players
- **Identity**: ***Who are you?***[8]
  the methods for defining and identifying the actors in the data sharing ecosystem. For the CDR this includes banks, third parties, and consumers.
- **Privacy/Control:** ***What are you allowed to see/do?***
  the methods for ensuring that the end user has full control to give, see, monitor, change and/or revoke any consents they have granted.
- **Consent/Authorisation:** ***How can I be sure?***
  the methods for providing the required consents, and for ensuring that only the required data is authorised, to the authorised third party, for the authorised amount of time.

We note that conceptually the above elements form a non-overlapping set with distinct solutions required for each sub-system or "method" delivery mechanism. In combination the above elements when properly implemented are sufficient for the delivery of a Trusted ecosystem.



[7] This paper and the standards discussed focus on the security of the TRANSFER of data. A parallel question on how to STORE the data securely is important for the ecosystem to consider; and may be addressed via accreditation or regulation.
[8] Although Identity is a core Trust Element, there are many valid implementations for participants and countries worldwide. Therefore, we will not cover HOW to validate Identity, but only how to transmit that validation.

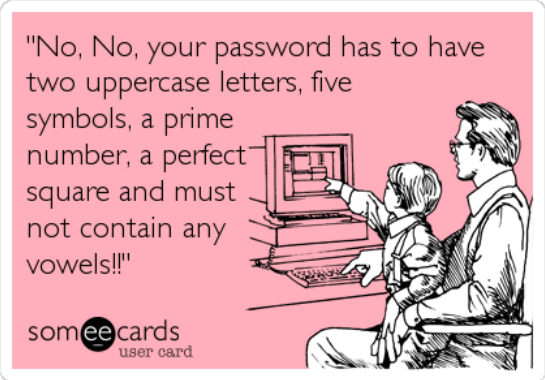
2.4 Trust Implementation Concepts

In the online world, implementation of Trust is a set of technology challenges. Methods for overcoming the challenges of implementing each of the elements of Trust individually have been around for many years. For example, Authentication mechanisms such as user passwords have been around since classical times (think of "Open Sesame") and the SSL protocol for internet browser security was first introduced in 1995.[9]

Source: The Spectator Australia [10]

Online access for banking accelerated as adoption of the internet increased. Banks needed to know who was signing in, to be sure it was them, and then needed to ensure that (only) they saw (only) their data. Errors or restrictions in account access, incorrect account visibility or 'crossed wires' have all been costly in terms of both financials and PR.

Banks implemented increasingly secure methods of identity and authentication over the ensuing decades. Most banks today have augmented the classic username/password combination with additional types of multi-factor authentication.

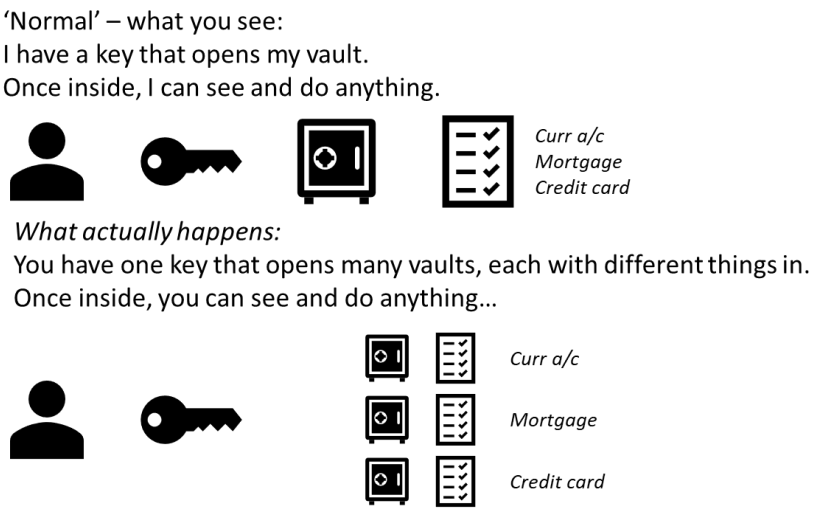


Source: SomeEcards.com[11]

Banking has answered the core Trust questions for the standard use-case of essentially a two-party, direct connection. This is one of the reasons why banks are trusted around the world to protect the data of their customers.

[9] https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL
[10] https://www.spectator.com.au/comic/open-sesame/
[11] https://www.someecards.com/usercards/viewcard/MjAxMy01MjU0MmU2NGRhOTE2Yzdl/

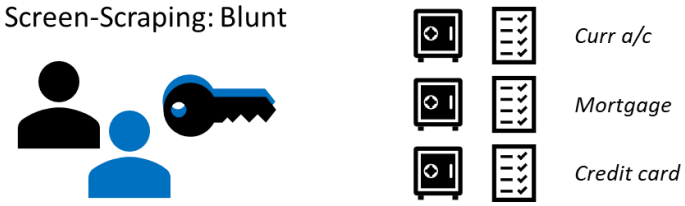
Although banks are trusted, the actual implementation of this Trust flow is already more granular than it appears for users. The Customer experience is simple:



Moving into the era of Open Banking requires data to be shared more generally (but no less securely) by incorporating more parties than just the customer and the bank across an entire ecosystem. Where that ecosystem is distributed, as with the CDR, the requirements for definition and validation of the Trust elements becomes more complex.

In particular, Open Banking (as with the CDR) requires an additional party to be introduced, called a 'Third Party' or TP[12]. This Third Party does not own the data (data owner is the Consumer) and does not need to have all of Data Holders data (data is held at the Bank).

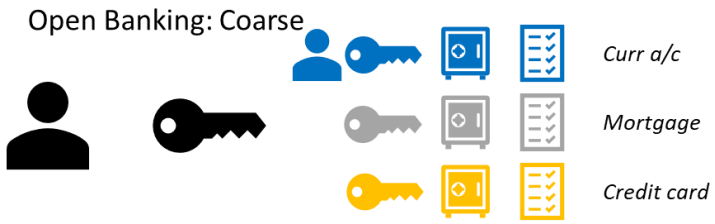
The blunt option here is "screen scraping", where the Consumer gives their key to the TP. This does allow the TP the same levels of access as the Consumer, but is 'all or nothing', is highly insecure, very inflexible, and difficult to see and revoke:



This leads to the requirement for more granular consent. Open Banking ecosystems start by allowing consumers to give TPs different keys for each of the vaults. This means the Consumer can see which key(s) have been issued to which

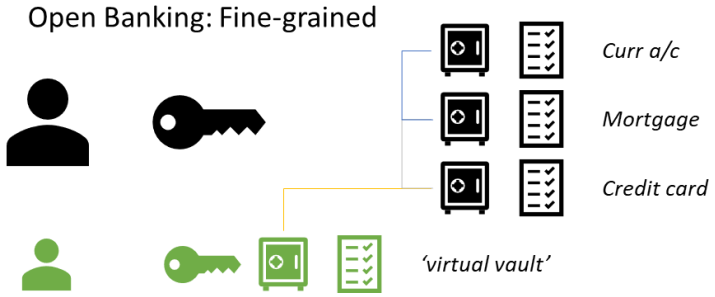
[12] In Australia, the receiving party is currently referred to as an "Accredited Data Recipient" (ADR). However, in the case of write access, the third parties receiving and actioning, will both receive and action data, not just acting as 'data recipients'. For ease of referencing therefore, this paper adopts the language of 'Third Party' (TP) or 'Third Party Provider' (TPP), similar to the existing EU usage.

TP(s), without needing to share their own key. These keys can be time-bound and are easy to revoke but they allow TPs to see[13] ALL DATA within that vault.



This approach may be acceptable for simple use cases, but in real world use cases, the data required by TPs is likely to be held in different vaults, and Consumers may not need or want a TP to see all data within any single vault. For example: a Price Comparison service may require access to the last 3 months of current account debit transactions to confirm utility payments. A mortgage affordability and comparison check will need 12-18 months of all current account transactions to confirm salary, loans, and other financial commitments, as well as needing access the mortgage account to confirm current repayment rates.

To minimise the amount of data shared and to increase control, Consumers should be able to provide just one key to a TP for that TP to obtain just the right amount of data required from just the right places. This can be thought of as a 'virtual vault' that the Consumer chooses what to put in, and who to allow access:



In all of these examples, the Consumer experience should remain as simple as possible, whether granting consent to a 'read-only' virtual vault, or whether granting a specific, fine-grained, multi-dimensioned consent to a 'read-write' virtual vault.

Across an ecosystem, these relationships need to be set up and managed between multiple TPs, Banks, and Consumers. Therefore, the ecosystem needs to define the mechanisms for setting up this access (getting the correct key), as well as creating the key in the first place (cutting the key), using the key (by TPs), and controlling the key (for Consumers). Providing and cutting the key then needs to be as standard as possible to ensure security.

[13] Although 'see' implies read-only, the same principles apply where TPs can 'see' and 'write' data.

2.5 Use Cases and Consent

Consent management becomes increasingly important as the potential datasets and use cases increase. As an account holder, a Consumer expects and needs to see all types of data and have access to all account functions, at all times. However, this universal access is not always required or desirable for a TP. In order to preserve privacy, and to promote data minimisation, Consumers must have fine-grained control of how much data or functionality is shared with which TP, and for how long.

The elements of Trust need to be broken down and implemented consciously to facilitate distributed, consented, secure data sharing that encompasses TPs: new concepts (the Third Party), new processes (Consumer consent) and new technology (TP access keys and Bank consent management) are all needed.

Although implementation of Trust across a distributed ecosystem is a relatively new challenge, it has been delivered successfully in multiple jurisdictions, including Australia, the UK, Brazil, and New Zealand. The UK, Brazil and New Zealand have also already implemented mechanisms to provide control of fine-grained multi-dimensional consent.

SUMMARY TABLE OF CORE CONSENT DIMENSIONS:

	Products	Granularity	Length	Time	Management
e.g.	***Accounts? Cards? Mortgages?***	***Basic? Full?***	***"For [x] days"***	***"Between [Dates]"***	***View Details of consents and resources***
UK	Yes	Yes	Yes	Yes	Yes
NZ	Yes	Yes	Yes	Yes	Yes
Brazil	Yes	Some	Yes	Yes*	Yes
Australia	Yes	Some	Yes	No	No

*available in the API but not enforced at launch

Payments moves beyond the core dimensions of consent required for providing read-only access to transactions. They will require items such as “From”, “To”, “Amount”, “Currency”, “Frequency” and “Date”. To facilitate all use cases, TPs need to be able to specify precise values for any of the dimensions.

Unlike other implementations around the world, the CDR does not have sufficiently granular dimensions, nor does it include the ability to add new dimensions within the current standards. This is what is known as fine-grained consent, and is the biggest omission in the Australian information security standards.

SUMMARY TABLE OF PAYMENTS CONSENT DIMENSIONS:

	Payments	Payments	Extensions	Granularity
e.g.	*Single Immediate Payments?*	*Variable and/or Recurring Payments?*	*Can new dimensions be added?*	*Can more precision be added?*
UK	Yes	Yes	Yes	Yes
NZ	Yes	Yes	Yes	Yes
Brazil	Yes	No	Yes	Yes
Australia	No	NA	NA	NA

The Data Standards Body’s decision proposal DP-183 [14] highlights the limitations of the existing CDR standards to support some specific but common use cases. Data sharing is not ‘done’; although it does work for current data sharing it is not clear or complete.

The proposed solution put forward in DP-183 refers to a principle of ‘Purpose-based consent’. Purpose Based Consents are a way to encode all of the required dimensions and granularity for a specific use case. Unfortunately, this specificity leads to a consequent loss in flexibility. DP-183 highlights read-only use cases which are not currently enabled by the CDR, but the same principles and requirements are even stronger when looking to enable read-write access.

14 https://github.com/ConsumerDataStandardsAustralia/standards/files/6643013/Decision.Proposal.183.-.Purpose.Based.Consent.pdf

Taking the example of the Tax Return, DP-183 specifies a number of dimensions that would be sufficient for a Consumer to consent, and for a Bank to identify and return that data as a one-time request. This is the equivalent of creating a specific printed consent form and is similar to a rigid multi-course 'Set Menu' in a restaurant.

However, that same Consumer would need a new Purpose Based Consent to be defined in order to repeat the request for the following year, and every year after. In essence, 'Tax Return 2021' would require a new printed consent form from 'Tax Return 2020', and may have different items on it that a Consumer would need to be aware of. To extend the restaurant analogy, swapping out one course from a set menu would require a NEW set menu to be defined.

The alternative, multi-dimensional fine-grained consent is more similar to providing a mechanism to select appropriate options for printing out a consent form, which provides full control and visibility to both Consumer and TP. The restaurant equivalent is *a la carte*, where consumers can choose exactly what they want.

There is a danger for the CDR that trying to centralise ALL possible use cases restricts potential innovation by TPs, and in fact reduces the levels of visibility and control that consumers have over their data. It would also commit the DSB to attempting to represent every possible combination and dimension of access into static scope representations.

Although concerns have been raised about the potential impact of multiple consents on Consumers, this can be addressed using customer experience guidelines. Fine grained consent allows for simplification of customer experience if required for some use cases, but also allows all complex use cases, both known and unknown.

Revisiting the analogy from section 2.4, this requires the ecosystem to make a generic key cutting machine, and standardise the functions for how to cut it, rather than trying to define a different key for each individual use case.

2.6 The Need for Standards

Implementation of Trust across a distributed ecosystem requires that all of the elements of Trust are captured and delivered in a standard way, agreed by all participants within that ecosystem. Therefore, core to the delivery of the elements of Trust across any ecosystem is the agreement of standards.

The importance of standards to the success of an ecosystem can be illustrated with two empirical cases. First, the home video ecosystem was only made possible by the agreement of standards for recording, distributing and playing home videos. Second, the browser wars of the late 1990s were partly tempered by web pages adopting W3C standards[15] and so ensuring they were "available on all browsers".

Depth of implementation and complexity of standards depends on the desired use cases and overarching regulatory frameworks. Delivering the required standards to ensure secure, coarse-grained consents is far more straightforward than delivering standards to ensure fine-grained, privacy-preserving, flexible consents.

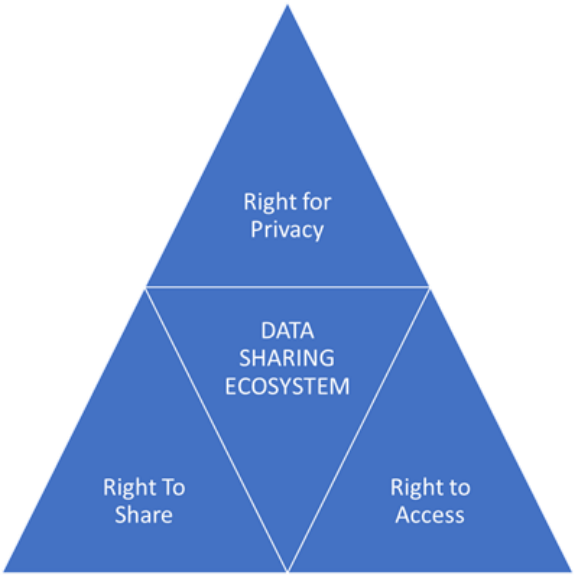
Standards for ecosystem use are best developed collaboratively, and transparently. This brings the widest range of inputs and expertise to bear on solving problems that will occur in any data sharing ecosystem. In the case of standards for data security, they also ensure global familiarity, which drives interoperability, functionality, and validation advantages.

Across the world of open data-sharing ecosystems, we see that the challenges of implementation and standardisation are not unique. Therefore, nor should the solutions be unique.

Objectively, the ideal case should be the use of international, open standards.[16]These provide the lowest cost, widest distribution, and broadest marketplace for solutions to common problems. We note that some global IT vendors do not support the CDR Information Security Standards as they currently exist. This makes it challenging for participants of the ecosystem to comply with the standards through their vendors as these vendors will typically give precedence to complying with global standards.

[15] https://www.w3.org/
[16] Also stated by the Data Standards Body, Consumer Data Standards, v 1.5.1, https://consumerdatastandardsaustralia.github.io/standards/#standards, Outcome principle 2: APIs use open standards

2.7 Open Banking Standards



As described in the previous section, standards are vital for success. However, actually defining and agreeing standards is a balancing act covering three competing rights:

- The Right to Share
- The Right to Access
- The Right for Privacy

Participants in data sharing need standards that cover all three of these. However, the challenge is in balancing the needs of each type of participant in order to deliver a functioning ecosystem.

For Open Banking, standards development has been rapid, recent, and recurring.

2.7.1 Origins and Layers

The first scale implementation, in the UK, took the global open framework for internet authorisation – OAuth2.0 – as a starting point. This was a natural starting point because of the ubiquitous acceptance of OAuth[17]; it is a standard developed and used by Amazon, Microsoft, Google, and Facebook among others.

Identity layer

The next challenge was to decide what specific rules should be applied to the OAuth 2.0 framework. Once again, a global standard was available, OpenID Connect (OIDC). This is an identity layer that sits on top of the OAuth2.0 standard and whose primary purpose is to facilitate identity exchange for users and clients. It also introduced significant and vital security improvements on top of OAuth 2.0 and was widely adopted.

Security layer

However, the OpenID Connect extension to OAuth 2.0, whilst a significant improvement, was still insufficient to secure resources in the financial sector. That required the development of a new security protocol layer on top of OIDC, called the *Financial Grade* API profile (FAPI). The OpenID Foundation is responsible for this standard's development and maintenance through its FAPI Working Group.

[17] https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth

The first version, FAPI 1.0, is available in two variations: the original 'FAPI 1.0 Baseline' which was intended for Read only and 'FAPI 1.0 Advanced' which was intended for Read-Write (although either variation supports both). Under the privacy regimes of Europe and Brazil, consumer payments and consumer data are deemed equally important. Therefore, the international community has mainly coalesced around FAPI 1 Advanced for both read and read-write[18].

2.7.2 Adoption and Intention

Adoption of new standards is never easy, and the UK was no exception. Banks' security representatives felt that FAPI 1.0 Baseline was not secure enough. On the other hand, for the first two years of the UK programme there was insufficient vendor support FAPI 1 Advanced to be adopted as the foundational standard.

This situation led to the UK's Open Banking Implementation Entity (OBIE) developing its own *temporary* security protocol which was a compromise in that it offered more security than FAPI 1 Baseline but was easier to implement than FAPI 1 Advanced[19].

However, ensuring that this 'UK Special' was temporary was a high priority for all participants. The intent was always that the ecosystem's vital core security standards would be maintained and developed in the long term through active guardianship of the most suited global standards body.

As stated by the Technical Design Authority of the UK OBIE in Decision 167: [20]
"moving to a truly global profile with no elements specific to the UK or Open Banking will promote adoption and consequent interoperability. The greater the level of adoption, the better the support from product providers and implementers – 23/08/2018".

2.7.3 Security

A number of other open banking implementations have followed the UK, including Australia's CDR. FAPI 1.0 has been adopted by all of them as the way for participants to ensure the Security element of their Trust.

The UK, New Zealand and Brazil have all adopted 'profiles' of FAPI 1.0 Advanced. These implementations are therefore all broadly technically inter-operable. They are all also formally registered and therefore recognised by the international standards community, which includes a number of global commercial technology vendors.

---

[18] FDX in the USA is an exception to this and is using Baseline as the base.
[19] https://openid.net/2021/03/12/fapi-1-0-part-1-and-part-2-are-now-final-specifications/
[20] https://openbanking.atlassian.net/wiki/spaces/WOR/pages/556335308/167

In contrast, the Australian CDR Information Security standards were developed by *adding additional custom extensions* into the base OAuth 2.0 framework, which were not registered with the IANA Registry. This effectively makes the Australian standards unique, and therefore removes the benefits of interoperability and global commercial vendor support[21].

2.7.4 Identity

The element of Identity is the most difficult to standardise, even within a single country. Where there is a national digital ID, such as the Scandinavian BankID, it is very possible simply to leverage existing schemes. However, implementing national Digital Identity programmes is by itself a challenging undertaking and not one typically implemented simultaneously with an Open Banking programme.

In practice, in Open Banking systems globally, the responsibility for Identifying and Authenticating customers remains with the Data Holder. Apart from some agreed core principles and guidelines, Identity and Authentication typically remains an area where Data Holders can innovate around both the User Experience and the Mechanisms that they use, in order to derive their own versions of 'Friction Right' customer experiences.

2.7.5 Privacy/Control and Consent/AuthZ elements

Moving from read-only to read-write requires a rethink of how to control access to the movement of currency. This calls for fine-grained Consent (to confirm the payment instruction from/to the correct accounts, for the right amounts, at the right time) whilst simultaneously requiring that the consumer needs for Privacy are balanced against the needs for Payment Initiators to have visibility of the status of any new payment resources that are created.

Although FAPI is the base of the Security element, all existing jurisdictions differ when it comes to defining the other elements of Trust (Privacy/Control and Consent/AuthZ).

This is partly down to the regulatory frameworks and partly down to timing: In the UK, Privacy is mandated legally by GDPR, and Consent is mandated under the terms of PSD2. Australia does not have an equivalent to GDPR, meaning that some of the provisions need to be enacted within specific legislation like the CDR.

---

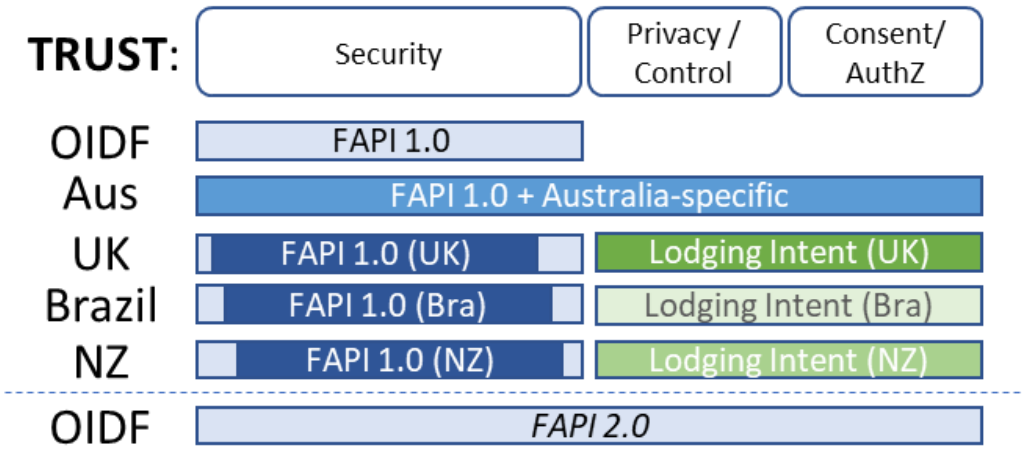
[21] There are defined mechanisms that standards bodies can use to register their custom extensions to promote international interoperability. The IANA Registry contains all of the registered OAuth 2.0 parameters from all of the standards bodies that have felt it necessary to extend the core specifications. Australia has not registered its own custom extensions.

The UK and Australia were early adopters for open banking, meaning broad Consent and Authorization standards were not available at the time of ecosystem build. Australia developed a specific, proprietary method of sharing Arrangement IDs,[22] and the UK used a pattern called 'Lodging Intent' which effectively decouples the details of an authorization from the request for authorization.

New Zealand took a pragmatic approach to re-use existing standards, and so took the UK's output as a starting point. It too followed a pattern to develop a Lodging Intent in order to reach its standard. This means the NZ standard is similar but not inter-operable with the UK (though the barrier to convert is very low).

Brazil copied the EU's GDPR into its own privacy law (LGPD), as well as the key concepts from PSD2. So, it naturally also copied the approach for implementation of open banking, and similarly defined its own Lodging Intent pattern to meet its consent needs. However, Brazil has also introduced other Consent management APIs which further improve upon the UK.

CURRENT GLOBAL TRUST ELEMENT PROFILES



Returning to the previous section's example, the home video ecosystem, we see some clues and similarities to the future development of all of these implementations. Both VHS and Betamax achieved the same aims through the definition and adoption of standards, albeit in different ways[23]. Full international interoperability required a single prevailing standard, and so the VHS and Betamax wars were ultimately costly distractions on this journey.

In a similar vein, the evolution of open banking standards is likely to consolidate to a single technical standard that governs *how* data is secured and shared whilst leaving each region to develop the content of *what* they share as they see fit.

[22] For more details on Arrangement IDs, please see the Technical section 3.2.
[23] https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:42098/SOURCE1

Some UK and Brazil participants have already started to consider their routes to moving to the emergent FAPI 2.0 standard which will be discussed more in later sections.

2.7.6 Impacts of Use Cases

As detailed in section 2.5, the requirements for control and consent depends on the required use cases.

Payment Initiation[24] introduces additional complexity around the concepts of Data (or "Resource") Ownership. In a read-only data model, Resources have a sole Owner. For Payments, some new Resources may be created that aren't necessarily under sole ownership. Indeed, some Resources such as Joint accounts are already jointly owned.

This difference in requirements leads to a challenge of implementation, which the UK ecosystem summarized as follows:[25]

"OAuth 2.0 scopes are coarse-grained, and the set of available scopes are defined at the point of client registration. There is no standard method for specifying and enforcing fine grained scopes (e.g. a scope to specify that account information should only be provided for certain time periods). A ***consent authorisation*** *is used to define the fine-grained scope that is granted by the PSU to the AISP."*

Extending from read-only to read/write functionality requires sufficient granularity and flexibility within the Trust elements to cover all proposed use-cases, without being prescriptive on use-cases.

[24] , or 'Action Initiation' within the CDR
[25] https://openbanking.atlassian.net/wiki/spaces/WOR/pages/658792/001

2.8 CDR Trust Standards

2.8.1 Current and Desired States

The existing Australian CDR 'Security Profile' is based on a global open security standard from the Open ID Foundation (OIDF) called the Financial-grade API (FAPI) profile. However, FAPI 1.0 (as used within Australia, UK, NZ, and Brazil at the time of writing) is ONLY a Security profile, meaning the other elements of the Trust framework (Identity, Privacy/Control and Consent/Authorisation) need to be covered through other approaches.

Australia has implemented a local-only specification to cover these elements, but now needs to extend the functionality from read-only to read-write. This means that the elements need to be extended as well:

Privacy/Control needs to be stronger to restrict the TP's ability to control and to preserve Consumer privacy. Consent/Authorisation needs to be fine-grained to ensure the Consumer remains in control and that the Bank can confirm the correct level of Authorisation for the transaction. Consent also needs to be flexible, dynamic, and multi-dimensional in order to cater for all potential use cases.

Both Scott Farrell in the report of the *Inquiry into Future Directions for the Consumer Data Right* and the Data Standards Body (DSB) have expressed their support for open standards.

Scott Farrell recommended:

"Open international standards should be used as a starting point for Consumer Data Right rules and standards where available and appropriate." [26]

This position is supported by the DSB Outcome principles, which state:

"In order to promote widespread adoption, open standards that are robust and widely used in the industry will be used wherever possible." [27]

2.8.2 Technical Approaches – LIP and FAPI 2.0

The current CDR approach to Privacy/Control and Consent/AuthZ is not sufficiently fine-grained nor is there sufficient visibility and control for all participants necessary to address complex data sharing arrangements nor payments. However, there are existing standards to build on, since apart from Australia, all other reference open banking jurisdictions (UK, Brazil, and NZ) have

[26] https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf Recommendation 8.9
[27] https://consumerdatastandardsaustralia.github.io/standards/ v1.5.1, under 'Principles':

incorporated standards for granular read/write as well as read-only activities from the start.

Standards for the Privacy/Control and Consent/Authorisation elements have typically been sought from two sources:

- leveraging the work created from a previous national open banking programme, which has typically meant following a "Lodging Intent Pattern" (LIP) which is then specific to the relevant jurisdiction, and/or
- leveraging work from international standards bodies with long experience in designing standards to address Consent and Authorization. e.g. the IETF, Kantara or the OIDF.[28]

Lodging Intent

The Lodging Intent Pattern is the approach followed by the UK, NZ, and Brazil to deliver fine-grained consent. However, they each use different implementations of this pattern. Although already adopted globally, there is no 'standard' implementation, and the solutions also mix together some concepts for expediency (which is not best practise, and complicates future extension).

The ABA does not support the Lodging Intent Pattern for Australia as a first preference, due to the existence of a more suitable standard to cover fine-grained multi-dimensional consent. This standard is the OpenID Foundation's FAPI 2.0 protocol. This will be a global open standard, and aims to be the 'right' way of solving for these issues in a way which can be adopted easily and extended in future.

FAPI 2.0

The objectives of the OpenID FAPI working group are to provide standard solutions for Trust elements in a way that is highly extensible and can immediately be adopted as best practise. The development and publication of FAPI 2.0 is fully aligned with those objectives.

The OIDF FAPI Working Group have developed FAPI 2.0 to include support for mandatory standards for the Privacy/Control and Consent/Authorisation elements alongside enhancing the Security element. FAPI 2.0 is designed to be applicable to read/write as well as read-only data sharing activities and already has significant input from members of the Australian CDR community.

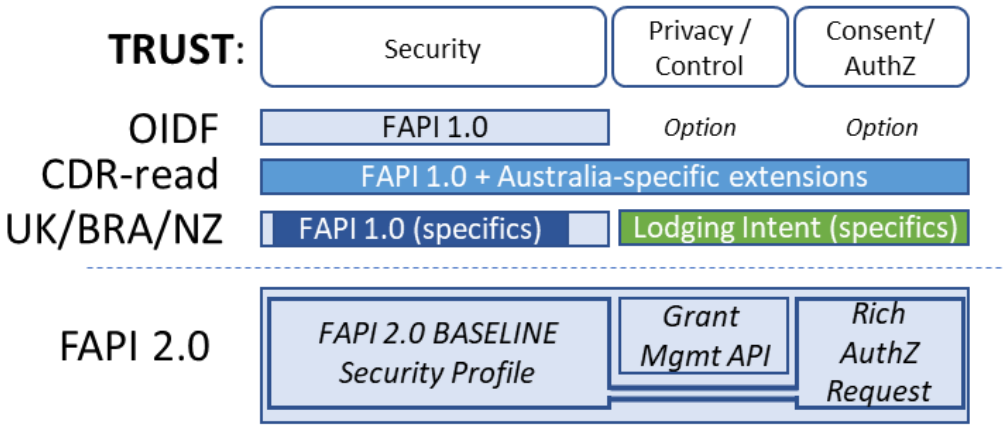
[28] Kantara and the OIDF have extensive experience in developing and maintaining royalty-free and IP-restriction-free standards in this area.

FAPI 2.0 mandates the use of standards that cover Privacy/Control and Consent/Authorisation, for which the proposed key enablers are:

- The "Rich Authorization Requests" (RAR) extension to OAuth2.0 (which is already published in "Internet-Draft" format[29]) for Consent/Authorisation.
- The "Grant Management API" extension to OAuth 2.0 (which is now published for industry review[30]) for Privacy/Control.

The FAPI 2.0 Baseline profile is now published as an Implementer's Draft[31]. This Baseline profile combines Security and AuthZ elements (effectively mandating RAR), although future iterations may split those elements back out to accommodate more advanced usage.

CURRENT AND FUTURE GLOBAL TRUST ELEMENT PROFILES



[29] https://datatracker.ietf.org/doc/html/draft-lodderstedt-oauth-rar-03
[30] https://openid.net/specs/fapi-grant-management-01.html
[31] https://openid.net/specs/fapi-2_0-baseline.html

2.9 CDR Standards for the Future

2.9.1 Security

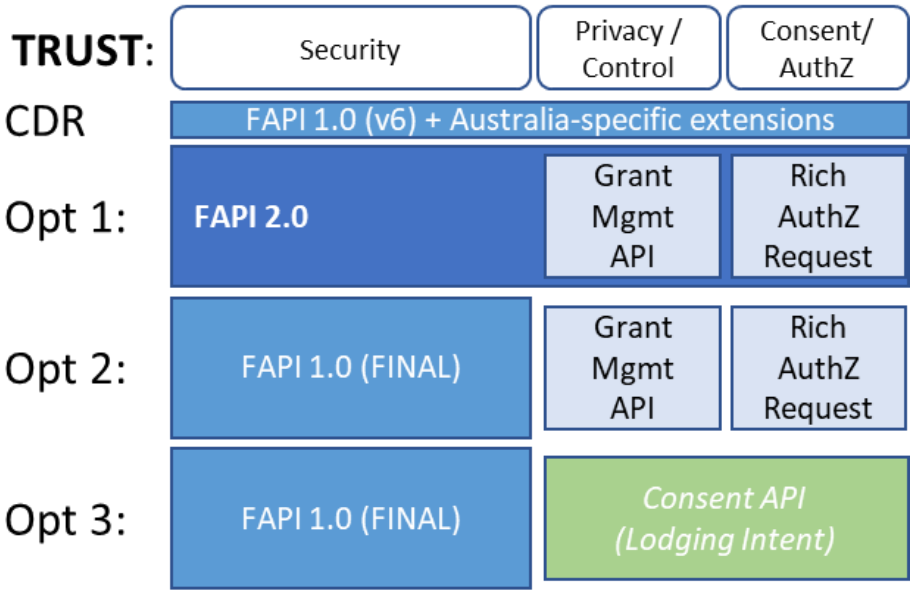
When it comes to the different Trust elements, with Security it is always recommended to move to the latest standard, especially with such an important data sharing programme as that of banking. As FAPI 1.0 Advanced is now FINAL, it is strongly recommended it be adopted by the DSB for implementation as soon as possible by all CDR participants, given existing legislated delivery obligations. The migration to FAPI 1.0 for implementers of the CDR is relatively straightforward, with the migration actions that need to take place already well publicised. [32]

Adoption of FAPI 2.0 in time will enhance the Security elements for the CDR, mainly through simplification. Even more importantly, it will also bring solutions for Privacy/Control and Consent/Authorisation which are inextricably linked and mandated.

2.9.2 Privacy/Control and Consent/AuthZ

The clear choice around Privacy/Control and Consent/Authorisation elements is between LIP (on top of FAPI 1.0), which has a few existing implementations, some emerging consensus, but no global open standard, and the FAPI 2.0 approach which will be a global standard backed by industry, but for which there are no current implementations.

OVERVIEW OF OPTIONS:



[32] https://bitbucket.org/openid/fapi/src/master/FAPI_1.0/changes-between-id2-and-final.md

2.9.3 Options analysis

We have consulted and analysed a number of options which are summarised below. The preference is for **Option 1: Adoption of FAPI 2.0:**

Option	Description / comment	Pros	Cons	ABA Position
Option 1 **Adopt full FAPI 2.0:** including Grant Management and IETF Rich Authorisation Requests (RAR).	The FAPI 2.0 Baseline specification includes a requirement to support IETF RAR and a recommendation to support Grant Management. The ecosystem can deliver all the future requirements for the CDR, as well as reducing implementation complexity by aligning to international standards.	• Delivers on the CDR need to enable read-write • Aligns CDR Trust standards with international standards for interoperability / support • Puts Australia ahead of the long term global moves. • Implemented as part of vendor-supplied security infrastructure • FAPI 2.0 Baseline specs already published (inc RAR). • Ongoing spec support and maintenance provided by an established global body.	• Grant Management is presently undergoing public review (implementers draft is expected to be approved by 6 September 2021). • Implementation timescales of 12-18 months to ensure vendor and bank support.	**Preferred**
Option 2 **Adopt Grant Management and IETF Rich Authorisation Requests** (but stay on FAPI 1.0).	Grant Management and RAR support could be added without requiring participants to formally re-certify or change their security posture to switch off support for features and standards that are used in FAPI.	• Minimises amount of change for Banks, FAPI 2.0 could be enforced at later point • Leverages emerging best practise standards without immediate re-engineering. • Implemented as part of vendor-supplied security infrastructure	• CDR Security Profile already requires updating from FAPI 1.0 'v6' to 'FINAL' • Stepping-stone rather than end-state. FAPI 2.0 security uplift will still be required soon. • Implementation timescales of 9-12 months.	**Secondary**
Option 3 **Use a Lodging Intent:** Implement a Consent API (Lodging Intent Service).	An alternative Consent Management API, proprietary to Australia, could be defined. Potentially leveraging the design patterns already used by Brazil, NZ, and the UK.	• No impact on Banks's vendors, can be implemented outside of OAuth as it is not a formal extension. • Is a proven pattern with examples already in place. • No need to extending existing CDR one-offs.	• Still requires FAPI 1.0 FINAL Uplift. • Does not exist so needs defining for Australia • Further diversion from long term FAPI 2.0 direction • Increases long-term complexity/duality • Implemented outside of the security infrastructure so requires custom build for each participant.	**Not a preferred option.**

3 TECHNICAL Discussion

Implementation of Trust is a technology challenge that has existed for many years. Implementation of Trust across a distributed ecosystem is a relatively new challenge, but one which has been delivered successfully in multiple jurisdictions, including Australia's CDR.

Core to the delivery in any of these jurisdictions has been a base of international, open standards. These provide the lowest cost, widest distribution, and broadest marketplace for solutions to common problems. In the case of standards for data security, they also ensure global familiarity, which drives interoperability, functionality, and validation advantages.

When looking forward to the emerging potential requirements for Action Initiation or 'Purpose Based Consent', the CDR approach to Privacy/Control and Consent/AuthZ is currently considered to be insufficient, lacking both the ability to constrain access in sufficient dimensions and the mechanisms to ensure that all parties have appropriate visibility of resources created by Action Initiation at all times.

However, there are solutions that could be incorporated into the existing 'Security Profile'. Apart from Australia, all other reference open banking jurisdictions included standards for read/write as well as read-only activities from the start. The UK and Brazil were driven by regulation, NZ adopted foundational elements to their standards to future-proof its own voluntary implementation.

These jurisdictions' implementations offer tremendous case studies that can be used to assess what has worked well and what could be improved as Australia looks to catch up with the rest of the world by adopting Action Initiation.

In addition, since some of these reference standards have been created, both the Internet Engineering Task Force and the OpenID Foundation have been developing specifications designed to standardize the mechanisms for using OAuth 2.0 to enable richer use cases whilst simultaneously addressing the requirements for visibility and control necessary for all parties engaging in Open Banking ecosystems.

All of these standards efforts are being created to mitigate deficiencies in OAuth 2.0 that were present in 2018/2019. OAuth was well equipped to authorize simple actions on behalf of resource owners, such as read-access to one's contact list. But when it came to more complex authorization decisions, such as access to certain features of a number of bank accounts, or the authorization of transactions, such as the initiation of a payment, the built-in support did not suffice.

The "scope" parameter, which ought to be used to determine the requested scope of an access token, is defined as a space delimited list of flat string values. This is not sufficient to, for example, list resources and corresponding actions on those resources or to define amount, currency, and other details of a payment transaction. Moreover, the length of the scope value is restricted by the maximum length of the authorization request URL, and the scope value is not protected from modifications by the user, which might cause security issues.

Different patterns to solve that challenge can be observed in the wild. They basically fall into two categories: either complex data structures are passed in the authorization request, or the authorization request refers to authorization data represented in a RESTful HTTP resource. So, the solution space boils down to the typical "pass by value" vs. "pass by reference" design decision. [33]

3.1 Lodging Intent – Pass by Reference

The Lodging Intent pattern is a generic name for a sequence of steps and an authorization process where a fine-grained multi-dimensional Consent Resource is passed by reference to an Authorization Server. This resource is known by different names in different jurisdictions, e.g. "Consent" (Brazil) or "Resource-Request" (UK, NZ). This 'Intent Resource' is created to reliably pass information to the authorization process which is protected from modification without the need to sign it digitally. Typically, the Intent resource also acts a receipt of the Authorization and potentially, though architecturally not ideal, morphs into another resource type that may have its own life cycle.

The following content describing the high-level steps and examples are sourced from the OIDF Lodging Intent Document and the New Zealand Open Banking API Documentation[34]

Note that Lodging Intent is not the ABA recommendation for the following reasons, but it is included here for completeness.

- There is no 'Lodging Intent' defined for Australia, so would be a new build
- The international direction of travel is toward the international FAPI 2.0 family of specifications. Adopting Lodging Intent would be a retrograde step.. and increase long-term complexity/duality
- Implemented outside of participants' security infrastructure. Requires a custom build for each participant, and would happen in addition to the requirements to uplift the core security to FAPI 1.0 FINAL.

[33] https://bitbucket.org/openid/fapi/src/master/Financial_API_Lodging_Intent.md
[34] https://www.apicentre.paymentsnz.co.nz/standards/available-standards/account-information-api-standard/

3.1.1 Lodging Intent Process (overview)

In every jurisdiction that uses this process, a variant of the following diagram can be found.

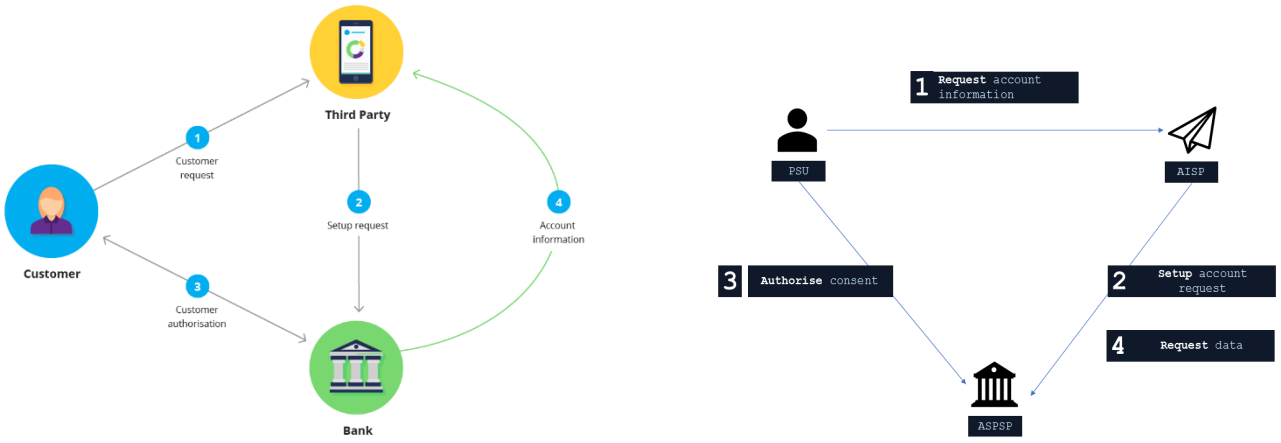


Figure 1 UK Open Banking Lodging Intent

3.1.2 Pre-setup Request (Obtain Access Token for Intent Creation)

The AS might require clients to authenticate and get authorized as a prerequisite to create a lodging intent. The recommended approach is to use the OAuth client credentials grant type to authenticate the client and access tokens to convey the authorization towards the lodging intent resource.

This requires the AS to define a certain scope the client needs to specify when asking for an access token.

The following example shows how to obtain an access token using the example of a payment initiation API. The respective scope value is "`payments_create`".

```
POST /token HTTP/1.1
Host: as.bank.example
Content-Type: application/x-www-form-urlencoded

client_id=3630BF72-E979-477A-A8FF-8A338F07C852&
grant_type=client_credentials&
scope=payments_create
```

3.1.3 Setup Request (Create Lodging Intent)

In the next step, the client uses the access token to create a new lodging intent.

The data sent to the resource endpoint depends on the particular transaction and API type. The representation format is at the discretion of the AS, JSON is the recommendation since it allows to represent even complex structures in a simple and robust way.

In our example, the client sends data describing a certain payment initiation transaction in JSON format:

```
POST /payments HTTP/1.1
Host: api.bank.example
Content-Type: application/json
Authorization: Bearer eyJraWQiOiJOQnlW...

{
  "creditor":"DE563784858585758585585",
  "instructedAmount": {"currency": "EUR", "amount": "123"},
  "remittanceInformationUnstructured": "Ref Number Merchant: 739466380"
}
```

The lodging intent will respond with an id of and/or link to the newly created resource. This reference is used in the next step to link the resource into the authorization process.

```
HTTP/1.1 201 Created
Content-Type: application/json
Location: /payments/36fc67776

{
 "consentId": "36fc67776"
```

3.1.4 Customer Authorisation (Authorization Request)

The client must send the reference to the lodging intent(s) to the authorization server as part of the authorization request. Three mechanisms can be used:

3.1.4.1 Parameterized Scope Values

The intent id can be made a part of the scope value used to ask for permission to access certain resources or perform a transaction. For example, the base scope value could be „payment“ and the resource could be added in the concrete authorization request separated by colons, resulting in an effective scope value “payment:36fc67776“. This is shown in the following example (with URI encoding):

```
GET /authorise?response_type=code&
client_id=3630BF72-E979-477A-A8FF-8A338F07C852&
redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&
scope=payment%3A36fc67776&
state=S8NJ7uqk5fY4EjNvP_G_FtyJu6pUsvH9jsYni9dMAJw&
code_challenge_method=S256&
code_challenge=5c305578f8f19b2dcdb6c3c955c0aa709782590b4642eb890b97e
43917cd0f36 HTTP/1.1
Host: as.bank.example
```

This way the lodging intent adds further details regarding the authorization the client asks for, which fits the purpose of the scope parameter. It also allows the AS to determine whether a user already consented to a certain request by just comparing scope values.

Most resource servers support parameterized scope properties, and this mechanism was adopted for both the Berlin Group and the Brazil Open Banking Ecosystem

3.1.4.2 Additional Request Parameter

Instead of enriching the scope value, one could also refer to the additional data using a new custom URI request parameter, as shown in the following example:

```
GET /authorise?response_type=code&
client_id=3630BF72-E979-477A-A8FF-8A338F07C852&
redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&
scope=payment&
payment_intent=3A36fc67776&
state=S8NJ7uqk5fY4EjNvP_G_FtyJu6pUsvH9jsYni9dMAJw&
code_challenge_method=S256&
code_challenge=5c305578f8f19b2dcdb6c3c955c0aa709782590b4642eb890b97e
43917cd0f36 HTTP/1.1
Host: as.bank.example
```

This approach requires the introduction of an additional request parameter, which is related to the particular scope value. Most likely this means there needs to be a distinct URI query parameter per scope value type (e.g. API type). This approach might be easy to implement but the coupling between scope value and corresponding intent is not as clear as in the method described above.

3.1.4.3 Claim

Deployments using OpenID Connect might also consider using distinct claim values to convey the intent id. The binding between scope values and intent Id is comparable to the additional request parameter approach and always requires OpenID connect to request API authorization.

This mechanism was adopted by the UK Open Banking programme as it was the only mechanism supported by vendors at the time. There is an overwhelming majority of participants in the FAPI WG that of the view that the use of an identity claim to convey a reference to a fine-grained scoping document is not a pattern that the industry wishes to take forward[35]. So much so, that FAPI 2.0, which aims to address Fine-Grained authorization and Consent Management goes so far as to require the use of RAR if 'scope' is insufficient to convey authorization details.

[35] https://bitbucket.org/openid/fapi/issues/416/rar-if-scope-and-claims-param-not

3.2 Australian CDR – Pass by Value(s)

The Australian CDR introduces multiple new OpenID Connect Claims as a mechanism for conveying limited authorization details which is an approach, that appears to have significant opposition from the majority of the OpenID FAPI WG as an appropriate long-term solution. [36]

Claims, as defined by OpenID Connect Core, *"specifies how the Client can obtain Claims about the End-User and the Authentication event*".[37] Both the UK and the CDR potentially misuse this property to convey authorization details, fundamentally information conveyed in the claims parameter has an intended audience of the Client (DR), whereas the Authorization elements included have a Target of the Resource Server by way of a linked Access Token.

No.	Parameter	Description	Target	Standardized?
1	`scope`	lists permissions.	Access Token	Yes
2	`scope`	OIDC Core Section 5.4 defines special scopes to request claims.	ID Token UserInfo Response	Yes
3	`scope`	Some implementations support parameterized scopes / dynamic scopes.	Access Token	No
4	`claims`	requests claims in a fine-graied way.	ID Token UserInfo Response	Yes
5	`claims`	may be able to describe permissions and/or detailed information about an access token in a fine-grained way.	Access Token	No
6	`authorization_details`	describe permissions and/or detailed information about an access token in a fine-grained way.	Access Token	Yes

Figure 2 OAuth 2.0 Parameter to Target Audience Mapping (Courtesy of FAPI WG member Takahiko Kawasaki – Authlete)

The CDR also introduces an additional OAuth parameter '*cdr_arrangement_id*' to be used as a reference to this unique authorization request. Similar in some ways to the OIDF Grant Management standard that is intended to be incorporated with FAPI 2.0[38], the CDR parameter remains *unregistered*[39] as an OAuth property.

Registering an OAuth parameter extension is a straightforward process and would signal to the international community Australia's intention to promote Australian Standards for adoption globally whilst ensuring that key features

[36] https://bitbucket.org/openid/fapi/issues/416/rar-if-scope-and-claims-param-not
[37] https://openid.net/specs/openid-connect-core-1_0.html#Claims
[38] https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Baseline_Profile.md
NOTE: To enable an interoperable solution to consent management it is anticipated that future versions of this specification will reference the FAPI WG's Grant Management API.
[39] https://www.iana.org/assignments/oauth-parameters/oauth-parameters.xhtml

introduced by the CDR are correctly registered on the Internet Assigned Numbers Authority (IANA) registry which would prevent collisions with other standards bodies.

What is different with the Australian CDR's use of Identity 'Claims' is that the extensions did not introduce a flexible mechanism to convey by reference or value, multi-dimensions of consent.

Therefore, despite the customization of core specifications, it is still not possible for customers to control access to their resources based on time, content, or any other dimension. Australia's CDR data sharing rules relies on TPs only accessing data that they have a legitimate reason to access even though the Access Tokens ('keys') that they have been given are significantly and unnecessarily more powerful.

As an example, Data Holders are obliged to share up to 7 years of accounts data on presentation of a TP's key, even though the TP may only have consent from a customer to access last week's transactions. This has potential security and insurance implications for Data Recipients as the keys the have been given cannot be voluntarily constrained which increases the responsibility and burden for protection of those keys significantly. Any compromise of the keys will enable a malicious actor to use the key in whatever lock it will fit, not just the locks that the TP has promised the customer it will, and perhaps importantly, what it will *not* use the key for.

3.3 FAPI 2.0 – Pass by Value

The broad aims of the OpenID Foundation FAPI WG is to:

- Enable applications to utilize the data stored in the financial account,
- Enable applications to interact with the financial account, and
- Enable users to control the security and privacy settings.[40]

FAPI 1.0 has succeeded in enabling ecosystems around the world *securely* to utilize and access data stored in the financial account in a standardized way. However, FAPI 1.0 did not standardize mechanisms to control access to data in a way that would preserve privacy whilst ensuring appropriate visibility for all parties.

FAPI 2.0 aims to address these two significant requirements and it does so by incorporating "OAuth 2.0 Rich Authorization Requests" which is currently in Draft 5, the IETF OAuth WG Standards Track, "OAuth 2.0 Pushed Authorization Requests"[41] which is in Draft 09 and Last Call before being assigned a formal RFC number, and the OpenID Foundation's "Grant Management API"[42]

These three standards provide the following capabilities:

3.3.1 Pushed Authorization Requests (PAR)

- Privacy preserving mechanism for conveying a request for authorization that be of any size.
- Communicated via a 'back-channel' message from an intended Data Recipient to a Data Holder which enables:
    - Requested Access to Data to be 'pre-processed' without impacting the Customer. E.g. A request to make an OSKO payment for 45,000AUD could be immediately rejected if the Banks global policy for an OSKO payment would be breached.
    - This offers tremendous benefits to customers as they could be immediately prompted to select another payment type or use another bank without being redirect to the Bank.

[40] https://openid.net/wg/fapi/charter/
[41] https://datatracker.ietf.org/doc/html/draft-ietf-oauth-par
[42] https://openid.net/specs/fapi-grant-management-01.html

Although still in draft format, pushed Authorization Requests have already been incorporated into the Australian CDR standards and are included as part of FAPI 1 Final.

3.3.2 Rich Authorization Requests (RAR)

The OAuth 2.0 Authorization framework defines the parameter "scope" that allows Data Recipients to specify the permission of an access token. This coarse-grained authorization request works when it is possible to model all elements of an access into a single string e.g. 'post-wall' can be defined as a static authorization that will 'Allow the application to post messages to your social media wall'.

This fixed scope is sufficient to ensure that all parties understand what is being requested and granular enough to be sufficient to execute the operation.

This mechanism is insufficient to specify fine-grained authorization requirements e.*g. 'please give me authorization to make a payment request to '082-902 1234567' for $43.23, the transaction must only have 1 to authorize (because it's a time sensitive purchase) and I want it to be executed using PayID payment rail'*

Or another example in JSON:

```
{
      "type": "payment_initiation",
      "locations": [
         "https://example.com/payments"
      ],
      "instructedAmount": {
         "currency": "AUD",
         "amount": "123.50"
      },
      "creditorName": "Merchant123",
      "paymentRail": "PayId",
      "constraints": "singleImmediate",
      "creditorAccount": {
         "iban": "AU02100100109307118603"
      },
      "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

These requirements become even more fine-grained or multi-dimensional when ecosystems look to develop a replacement for 'Card-On-File' arrangements.

"Please give me authorization to make a payment request to '082-902 1234567' for up to $250, per month, for a maximum of one transaction per month to expire in 12 months"

These requirements do not just exist in the world of payments, many of the data access use cases outlined in decision proposal 183[43] can be better met by adopting Rich Authorisation Requests.

"Please give me access to twelve months of accounts information for all Bank Accounts belonging to the customer, starting from 1st July 2019 to 30 June 2020 (inclusive) and account Balances as of 30 June 2020"

The current approach being suggested by Decision Proposal 183 implies the DSB is willing to attempt to represent every possible combination and dimension of access into static scope representations. The ABA seeks clarity on this supposition and recommends instead that the DSB consider adopting RAR as a generic mechanism for enabling multi-dimensional fine-grained consent to be requested and instead focus efforts onto the standardization of the dimensions of data access that the CDR wishes to enable within an Australian RAR envelope.

3.3.3 Grant Management API

PAR introduces the ability to convey a large consent payload in a privacy preserving way and RAR has introduced a standard that allows the dimensions of the requested authorization to be virtually limitless and be requested in a standardized way. What is missing however is a standard process to manage the lifecycle and obtain the status of a particular consent aka a 'Grant'.

The Grant Management API introduces a new extension to OAuth that provides the following capabilities:

- Provides a unique reference to the underlying authorization, like the CDR sharing identifier: `cdr_arrangement_id`
- Introduces a new Authorization Status, Management and Revocation API to OAuth to enable synchronization and standardized management.

[43] https://github.com/ConsumerDataStandardsAustralia/standards/files/6643013/Decision.Proposal.183.-.Purpose.Based.Consent.pdf

3.3.4 The Complete Picture

Collectively these three standards address all the capabilities required to support a complex data sharing ecosystem. They provide the rails on top of which standards authors can define 'What' data they need to share at any level of granularity and ensure that all participants, in particular the consumer, remain in control. The standards have wide support from industry

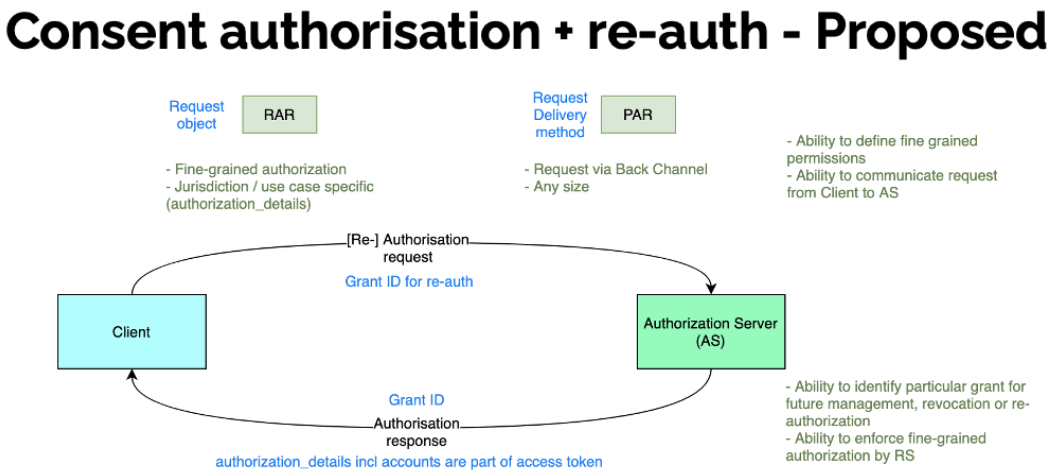


Figure 3 Consent Target State: OIDF Submission to CDR Decision 99 - Concurrent Consent Target State[44]

[44] https://github.com/ConsumerDataStandardsAustralia/standards/issues/99
This proposal received wide industry support from data holders, data recipients and vendors.

3.4 RECOMMENDATIONS and RATIONALE

A mechanism to support fine-grained, multi-dimensional consent is clearly required to evolve the CDR to fully meet its potential. The ABA makes the following recommendations for arriving at that solution:

1. Adopt the FAPI 2.0 family of specifications: Rich Authorization Requests, Pushed Authorization Requests, and the Grant Management API as the framework standards. Build all Consent and Authorization elements of the CDR upon this framework.
2. Improve the existing consent model to ensure that technical access to resources mirrors the expectations of consumers, by providing more appropriate multi-dimensional controlled access to data.
3. Increase engagement with the relevant standards bodies that are responsible for governing the critical foundational standards for the CDR.
4. Ensure that interoperability with global standards is enshrined as a key objective of the Data Standards Body.
5. Adopt an exception process where any departure from international standards is done so after clearly articulating the requirement and identifying where existing standards fall short.

These recommendations will:

1. Reduce potential security issues by adopting standards that are supported by many specialized companies and have been vetted by a wide pool of experts.
2. Increase consumer confidence and uptake of the CDR by ensuring they can share only the necessary amount of data for the purpose that it is being requested.
3. Encourage more vendors to provide services and products that would fit the Australian market by removing any CDR specific features that may otherwise be hard to justify given the relatively small number of potential clients
4. Maximise the potential of the CDR by easing adoption by all participants and by laying the foundational capabilities that enables easier expansion in all potential sectors.
5. Ensure Australian Fintech have the greatest and easiest opportunity to engage with foreign markets

The need to offer consumers better control of their data has been recognised and technically implemented in different ways by different ecosystems around the world.

Australia has already helped drive adoption of some of the elements necessary to solve this challenge already by mandating the adoption of some of the early specifications that solve part of the puzzle however pieces remain to filled.

By continuing this tradition of pioneering better foundations on which to grow and develop the CDR in the areas of consumer consent and privacy, Australia can demonstrate its continued leadership towards adopting best current practice and development of comprehensive national data sharing ecosystem standards that have the potential to become the new reference for other jurisdictions globally.

4 Decision Proposal 182 – ABA Responses

In response to the Consultation Request: [45]

We applaud the approach of the DSB to consider the adoption of a modern, comprehensive standard such as FAPI 2.0, which will upgrade not just the Security aspects, but also cover other Trust elements of Privacy, Consent and Authorisation.

We note that additional feedback request concerning Normative Standards Review (2021) has been raised by the DSB[46] to gather "impacts and implementation considerations" relating to the FAPI 1.0 FINAL standards. In line with the ABA's recommendation to move to FAPI 2.0, we note that these impacts and implementation considerations are no longer an issue when RAR (Rich Authorisation Requests) and Grant Management are supported per FAPI 2.0. This is because the client has a reliable way to get *all* of the details of the authorisation from the Authorisation Server, including scopes and other rich authorisation details.

4.1 Question 1: Existing Gaps

What are the existing gaps or concerns with the information security profile?

We believe it is essential to clarify the nomenclature. What is being termed an 'Information Security profile' is only one part of a Trust Framework that has a number of inextricably linked elements. (See the ABA InfoSec Positioning paper for further background).

The Security element is based on FAPI 1.0, so the only potential gap is that the CDR as published originally referred to the Implementer's Draft of FAPI 1.0.

The FINAL version of FAPI 1.0 was published on March 12, 2021. [47] The FINAL version contains a number of improvements when compared to the Implementers Draft. These gaps, and migration suggestions are already detailed online. [48]

However, there are significant gaps in the Privacy/Control and Authorisation/ Consent elements of the Trust Framework that are detailed in Q2., and which have been identified through the use of the formal Attacker Model described in Q7. [49]

---

[45] https://github.com/ConsumerDataStandardsAustralia/standards/files/6470911/Decision.Proposal.182.-.InfoSec.Uplift.For.Write.pdf

[46] https://github.com/ConsumerDataStandardsAustralia/standards/issues/203

[47] https://openid.net/specs/openid-financial-api-part-2-1_0.html,

[48] https://bitbucket.org/openid/fapi/src/master/FAPI_1.0/changes-between-id2-and-final.md

[49] https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Attacker_Model.md

4.2 Question 2: Gaps limiting extension

What gaps or concerns with the information security profile would prevent voluntary extension to write operations by a data holder?

The current information security profile does not include a flexible Rich Authorisation creation and management capability that is sufficient to address all the needs of the Consumer Data Right envisaged with Action-Initiation, or to address all of the complex multi-dimensional use cases for data sharing identified in Decision Proposal 183.

Without addressing and incorporating a flexible, consistent, and extensible approach to complex authorisation management at a fundamental level in the Trust Framework, the potential and vision of the CDR may struggle to be realised.

In our opinion the following items need to be introduced to the 'Security Profile' in order to support Write Operations more completely:

- A standard means of requesting Rich Authorisation, multi-dimensional access to resources or tightly scoped 'Action-Initiation' events based on the IETF Rich Authorisation Standard (RAR).
- A mechanism through which all parties can determine the status of their Consents, the content of their consents and the life cycle of their 'Action-Initiated' events. This will ensure the necessary visibility of all resources for all parties at all times. It should be based on the OpenID Foundation's Grant Management API
- A standardised process for action-initiation which ensures all parties have clearly defined ownership and access to resources that may be created by Action-Initiation – recognising that Data Recipients may need 'Receipts' of their Action-Initiated events.
- Appropriate technical conformance and certification requirements for all parties. This will ensure that the surety and safety of consumers' resources are guaranteed as much as is feasibly possible, in recognition of the potential increased risk profile that Action-Initiation may bring.
- Ensure that the Customer experience is still usable. Payments will require stronger authentication, with customers needing to provide informed consent without adding significant friction to the payment journey.

4.3 Question 3: Adoption of FAPI 1.0

What aspects of version 1.0 of the FAPI Advanced Security profile, if any, should be prioritised for adoption by the CDR?

As an International open standard, adoption of that standard requires adoption of all aspects of that standard. Therefore, all aspects of this profile will be required for any adoption. Any 'cherry picking' of specific aspects would potentially undermine the benefits of using the international open standards stated in both DSB and Treasury objectives and would require management of Creation of a Formal threat model, Conformance tooling, Certification, and ongoing maintenance of the same.

In addition to the technical benefits that incorporating the final iteration of the standard will bring, the following current concerns will be mitigated:

- It will become increasingly challenging for Data Holders, implementers, and their vendors to maintain support for retired and forked versions of standards.
- It may become increasingly challenging for Data Recipients to implement against CDR APIs if Data Recipients rely on public versions of libraries that enforce conformance to more up to date profiles.

Whilst the technical changes between FAPI 1 ID2 'Draft 6' upon which the CDR information security profile is based and the FAPI 1 Advanced Final profile are minimal, there are some breaking changes. Data Recipients will first need to implement support for these changes before Data Holders can migrate to FAPI 1 Final.

Data Recipients that uplift their implementations to support the requirements for FAPI 1 Final should be backwards compatible with Data Holders using FAPI 1 ID2. This was an important consideration of the FAPI WG when the final publication was defined.

The OpenID Foundation has provided a detailed analysis of the differences between the specifications and provides a high-level set of actions that Data Recipients and Data Holders should perform and in what order. The ABA recommends that the DBS publishes its own analysis and incorporates the work already published by the OpenID Foundation as a part of any migration.[50]

The ABA notes that the formal certification process for FAPI 1 Final was only made available on the 23rd of June 2021 [51]. At the time of drafting there were only three vendors certified for FAPI 1 Final and only one for the Australian CDR (based on FAPI 1 Advanced Final). Sufficient adoption and support by the vendor community will be necessary to ensure that Australian Data Holders continue to be well supported.

---

[50] https://bitbucket.org/openid/fapi/src/master/FAPI_1.0/changes-between-id2-and-final.md
[51] https://openid.net/2021/06/23/openid-financial-grade-api-fapi-conformance-tests-released-for-final-fapi-1-0-parts-1-and-2-specifications/

The ABA requests that the DSB signals any intent to uplift to FAPI 1 Final as early as possible so that appropriate conversations with supporting technology partners can take place.

For the benefit of the nascent ecosystem, the ABA recommends that *Data Recipients* are given a minimum of 12 months to incorporate support for the necessary changes ahead of Data Holders being permitted to enforce FAPI 1 Final Specifications. The ABA recommends that support for FAPI 1 ID2 Draft 6 should be completely phased out by the Data Holder community within 24 months.

4.4 Question 4: Transition to FAPI 2.0

What priority should be given to transitioning to FAPI 2.0?

FAPI 2.0 incorporates a comprehensive set of foundational standards for developing any data sharing Trust Framework. FAPI 2.0 includes Security, Privacy/Control and Consent/Authorisation standards. Support for these standards is not only required but is in many cases also made mandatory.

A 'Transition to FAPI 2.0' is therefore a major change in terms of approach to ecosystem data sharing, not just a simple transition. However, this change would be a significant step for international alignment, as well as enhancing capabilities for the CDR.

FAPI 2.0 is now available as an Implementer's Draft[52], meaning this iteration is locked and stable. This draft significantly reduces complexity for implementers by reducing the permitted OAuth 2.0 features to those that will ensure that the objectives and threats outlined in the accompanied attacker model can mitigated. FAPI 2.0 baseline now mandates a number of security features, including Pushed Authorization Requests (PAR) and Proof Key for Code Exchange (PKCE).

In addition, FAPI 2.0 baseline mandates the use of Rich Authorization Requests to meet the needs for complex and multi-dimensional consent. It also highlights the proposed inclusion of the FAPI WG Grant Management API. The Grant Management API is already published as a recommended Implementers Draft[53] with voting due before September 2021..

The ABA views FAPI 2.0 and its included standards as the best technical solution for delivering a successful implementation of the next stage of the CDR, as well as setting the foundation for future sector expansion ambitions. As an international framework, FAPI 2.0 can be Profiled if required to meet local specific requirements.

Every priority should be given to promoting a transition to FAPI 2.0, and to providing the implementers (Banks and commercial Vendors to banks) sufficient time to carry out these implementations properly.

The ABA requests that the ecosystem be given 18 to 24 months from the publication standards. This will ensure sufficient vendor adoption and product capability deployment by Data Holders which can be performed in parallel to any use case discussions and development.

[52] https://openid.net/specs/fapi-2_0-baseline.html
[53] https://openid.net/specs/fapi-grant-management-02.html

4.5 Question 5: Risk Reduction Considerations

What additional patterns or normative standards should be considered for adoption to reduce the risk of write operations?

The main requirement to reduce the risk of write operations is to lay the foundations to enable Consumers and Data Recipients to have appropriate control and visibility over the use of their Financial Resources (Data and Currency).

Therefore, the ABA recommends that the processes and procedures adopted by Data Holders to protect Consumers' data (and to protect their payments services), remain within the Data Holders domain, in the competitive space and under existing security, compliance and legislative frameworks. This should involve the usual authentication flows that consumers are already familiar with from their Banks.

Any moves to mandate these items centrally, such as a specific, separate channel for the CDR, risks accidentally restricting innovation and appropriate competition. Especially in the areas of Fraud Prevention and Transaction Risk Analysis, over-standardising the Customer Security User Experience could introduce risks to consumers, and may run counter to the overall objectives of the Consumer Data Right.

Data Holders are well versed in managing risks when operating payment services and the ABA recommends that this responsibility continues to remain entirely with the Data Holders domain.

In addition, the ABA recommends that as part of any adoption of Action-Initiation, Data Holders are empowered to offer to their customers more appropriate security user experiences that better enable payments offerings. This would include being permitted to support other more intuitive and friction-right web authentication journeys, including App2App[54] and decoupled flows.

Being permitted to make use of improvements in secure mobile hardware and modern API security standards (which in turn enable more secure and significantly more attractive user experiences to be offered) ensures that any payments services created through the CDR can compare with the exceptionally user-friendly experiences on offer from both Apple Pay and Samsung Pay.

User experience innovation is critical in ensuring that customers grow to see the any Action-Initiation events enabled by the CDR as a genuine alternative to those on offer from Big Tech. Equally, as mobile API driven payments begin to flourish, Banks need to be free to adapt to a rapidly changing threat landscape.

[54] https://standards.openbanking.org.uk/customer-experience-guidelines/appendices/deep-linking-for-app-to-app-redirection/v3-1-6/

4.6 Question 6: Maximising International Interoperability

What additional changes, if any, that should be considered for maximising international interoperability?

The ABA recommends that the following areas of potential improvement be considered to maximising international interoperability and reducing costly fragmentation costs.

Standards:

International interoperability will be maximised through the appropriate use of unadulterated international open standards. If local extensions are defined, ensuring that the local extensions are registered with the appropriate international bodies would significantly improve international interoperability.

The current extension mechanisms defined by the CDR for Consent and Authorisation are not formally registered outside of Australia. Doing this would signal Australia's intention to promote the CDR outside of its own borders.

International Engagement:

Longer term, the ABA recommends that the DSB considers a more formal engagement with the international technology standards bodies that govern the future development of the standards on which so much of the CDR relies. In addition to ensuring international interoperability, engaging with technology standards development bodies (including the Internet Engineering Task Force and the OpenID Foundation) would ensure that Australian consumers' needs are incorporated, and that Australian standards development can be assisted by a global pool of industry specialists.

Standards Development Processes:

The ABA would also recommend the DSB consider formal adoption of World Trade Organisation (WTO) - Technical Barriers to Trade (TBT) Treaty rules which govern the processes to be followed by international standardisation organisations. A consistent, published, and auditable technical governance process could potentially make the Australian CDR standards more attractive as a base from which other countries could develop their own national programmes.

Conformance and Certification:

A significant enabler of interoperability (international or domestic) is the development and use of conformance and certification testing processes and procedures. A standard by itself does not create an interoperable ecosystem: that requires the creation, adoption and then execution of a conformance and certification process. These processes mean that implementers can demonstrate that they have correctly interpreted the specifications and that the inclusion of their services into an API will not have an adverse effect on existing members or the ecosystem as a whole.

4.7 Question 7 – Additional Efficacy Steps

What steps could be taken by the DSB to assure the efficacy of the information security profile?

Irrespective of the final design of the Trust Framework and Information Security Profile, the ABA recommends that the security requirements be formally documented in a way that enables all communication pathways to be critically analysed, assessed for vulnerabilities, and then used to develop an appropriate standard that addresses identified areas of concern.

The FAPI 2.0 Attacker Model[55] is an example specification that outlines the assumptions, potential threat actors and goals and objectives of the underlying profile that are made *before* a standard is designed.

Any specification should aim to document the attacker models and outline the security, privacy, and non-repudiation requirements to enable systematic proofs of the security of the underlying Security Profile to be created.

Without the formal objectives of the security profile being articulated and the potential threats documented it is not possible to know if the published Security Profile is effective at meeting the requirements of the CDR.

Irrespective of the final implementation of the Information Security Profile, all parties will need to adopt and use it correctly to assure efficacy of the ecosystem. The ABA recommends mandated conformance and certification for all parties to the chosen profile and encourages the public development of the certification tools and processes to facilitate industry involvement in assessing the effectiveness of the conformance processes against any published Attacker Model.

[55] https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Attacker_Model.md

5 APPENDICES

5.1 Extension to Write - UK case study

Australia's CDR implementation originally focussed on delivery of read-only data sharing. This focus was partly due to the regulatory framework, and partly due to perceived risks and potential unknown costs of implementation of read/write access.[56] However, extension to read/write functionality was always planned.[57]

Looking to the UK experience: to deliver the level of control and consent required for read-only data access, the UK, being governed by the overarching GDPR and having strong principles of privacy, data minimisation and consumer advocacy ensured that the very first designs supported multi-dimensional fine-grained consent.[58]

Highlighting the need for this fundamental component of any complex data sharing ecosystem was literally the first priority for the Open Banking Technical Design Authority, captured as Decision 001. [59] This need was addressed by engaging with industry and seeking the views of subject matter experts, standards bodies, and specialist companies globally, and ensured that a solid, extensible pattern was adopted for read-only access.

As a consequence, the UK had a solid pattern to extend the 'scope' of data sharing for any purpose, across any data set including payments. Crucially, this was implemented in a way that works *within* existing standards and so did not require customizations of base specifications.[60] Having support from the global industry significantly de-risked the delivery for all participating institutions.

---

[56] https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf (Farrell Report, Dec 2017, p105 "Design Choices to minimise implementation Costs")

[57] https://treasury.gov.au/sites/default/files/2021-02/cdrinquiry-final.pdf (Farrell, Feb 2021 "Future Directions for the CDR", page x and Chapter 5).

[58] https://openbanking.atlassian.net/wiki/spaces/DZ/pages/4010944/Account+and+Transaction+API+Specification+-+v1.0.0

[59] Decision 001 Open Banking Implementation Entity Technical Design Authority https://openbanking.atlassian.net/wiki/spaces/WOR/pages/1918910/Rationale+for+Open+Banking+API+structure+and+OAuth+OIDC+technology+choices

[60] Rational For Standards Based Fine Grained Lodging Intent Pattern OBIE TDA Decision 001 https://openbanking.atlassian.net/wiki/spaces/WOR/pages/1918910/Rationale+for+Open+Banking+API+structure+and+OAuth+OIDC+technology+choices

5.2 Implementing Payment Initiation

In addition to laying the core foundations for granularity of data access, the European Implementations of Open Banking were required under PSD2 to implement Payment Initiation early on, which also heavily influenced the design of the Consent model.

For example, for a generic payment to be successful, *both* parties (payer and payee) must have full visibility and confidence in the end-to-end payment lifecycle. In practical terms, this can involve merchant and customer waiting for an EFTPOS machine to transact the payment, then printing out *two* payment receipts: one for the Merchant and one for the customer.

Open Banking Payments are no different: both participants require long lived access to the details and life cycle of the payment as it is authorized, initiated, cleared and settled, and both parties require durable access to a receipt record.

As noted earlier, the Lodging Intent Pattern offered a solution to this problem where the 'Consent Record' for a payment was used both to convey authorization status, and to act as a receipt record for the payment. This technically simple model has been improved architecturally to cover additional real-world use cases such as ticket reservations for concerts. It is now possible within Open Banking to separate out the Payment Authorization request from the actual Payment. This process will be familiar to anyone who has used a Visa or MasterCard Credit Card to hire a car or check in to a hotel.

5.3 WTO Principles for International Standards

The World Trade Organization (WTO) deals with the global rules of trade between nations. Its main function is to ensure that trade flows as smoothly, predictably, and freely as possible.

The "Six Principles" were agreed upon by the TBT Committee in 2000 with a view to guiding Members in the development of international standards[61].

1. Transparency (prompt, regular and complete publication),
2. Openness (of membership),
3. Impartiality and Consensus (access, input, pricing),
4. Effectiveness and Relevance (market led, promote innovation),
5. Coherence (avoid duplication/co-ordinate with others),
6. Development Dimension (facilitate developing countries' participation).

In practise, this translates to shared intellectual property, published under a Creative Commons license, promoting shared ownership and Integrity of standards.

5.4 Objectives of CDR

CDR was introduced first to the banking industry in July 2020. It aims to give consumers greater say over the access and use of their personal information by businesses and may allow consumers to access specified data held about them by insurers, and to authorise the secure disclosure of that data to third parties.

A Treasury consultation into the “Inquiry into Future Directions for the CDR” released in February 2021 focused on banking and InsurTech Australia says there are parallels and trends which are common to general and life insurance[62].

5.5 About the Open ID Foundation

Open ID Foundation – set up in 2007 to solve the problems of Identity at the heart of the Internet – standardisation of internet identity layer and security standards.

Safe, neutral space for the development of standards. A group of common interest, competitors, promoting inter-operable standards globally.

---

[61] https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm
[62] https://www.asiainsurancereview.com/News/View-NewsLetter-Article/id/76541/type/eDaily/Australia-InsurTech-association-backs-Consumer-Data-Right-regime-to-insurance-sector