Data Standards Body

Technical Working Group

Decision 182 – Information Security Uplift For Write

Contact: Mark Verstege
Publish Date: 19th August 2021
Decision Approved By Chairman: 25th August 2021

Context

Strengthening the foundations of the CDR
The Information Security profile of the Consumer Data Standards provides the foundations for secure data sharing. Its building blocks are the Financial-grade API (FAPI) family of specifications.

The CDR has many immediate needs coming to the fore that have required a review of the current Information Security standards. These include community change requests, rules requirements, consumer research, advancement or uplift to international standards, and security best practice. With the OpenID Foundation (OIDF) finalising FAPI 1.0 there is a direct need to consider the review and uplift of the Information Security profile. In addition, the Inquiry into Future Directions for the Consumer Data Right Final Report (Future Directions report) includes several key recommendations to information security and international interoperability. Whilst these recommendations have not yet been taken up by the Australian Government - and importantly this decision **does not** seek to presuppose which recommendations will be adopted - they provide important guidance in direction setting and long-term outcomes for the standards development of the CDR.

To cater for these needs and future direction, the DSB sought feedback on key aspects to enhance and evolve the security profile. As the CDR expands to sectors beyond banking key considerations for the Information Security profile include:

- Maintaining alignment to changes in the FAPI normative standards and security best practices the Consumer Data Standards relies upon. Consequently,
- Increasing vendor support and lowering overall costs of ownership for data recipients and data holders.
- Enabling interoperability across Australia's digital economy as well as globally.
- Uplifting authentication standards to offer improved experience, choice, convenience, and security as well as alignment to consumers' existing digital experiences.
- Improving the technical reliability and resilience of the consent flow and authorisation processes to minimise consumer impacts.
- Supporting the CDR's expansion beyond data sharing towards action initiation and cross-sector use cases
- Enhancing support for Data Holders to voluntarily extend beyond basic read access into write access models.
- Providing a framework for purpose-based consent and, at the heart of CDR's consent model, a more descriptive authorisation model to better meet the Data Minimisation Principle of the CDR and better support ADRs offering valuable goods and services within the CDR. In turn,

- Defining a richer authorisation permissions model that is more extensible beyond the needs of basic data sharing within the banking sector to support complex use cases including action initiation across all sectors.

The importance of ongoing maintenance and alignment to international standards
As with all normative standards the Consumer Data Standards relies upon, these change over time. Maintaining and uplifting the Consumer Data Standards in line with the changes to the normative standards is important to maintain vendor support, lower cost of ownership for participants and ensure the security of the Consumer Data Standards is kept strong and current.

In line with the recommendations in the Future Directions report, maintenance of the Consumer Data Standards requires ongoing alignment and uplift to international standards where they are applicable to the CDR. This process will require a continual process of review and transition where needed to retain secure foundations for Australia's digital economy. This ongoing effort presents a complex problem across a diverse many-to-many ecosystem that involves a growing number of sectors in the Australian economy, not to mention opportunities for international interoperability.

The security context for the CDR does not stand still but continues to evolve. As the security standards that support the CDR change, the long-term cost of ownership across the CDR is lowered by maintaining currency with industry support that provides a bias towards configuration-over-customisation. If the Consumer Data Standards does not maintain currency the cost of ownership will increase over the long term as vendor support reduces for legacy specifications, not to mention an increased security risk for all participants.

The Consumer Data Standards Information Security profile currently leverages Financial-Grade API (FAPI) Implementer's Draft v06 (ID2 Draft 06). Since the finalisation of version 1.0 of the Consumer Data Standards, the FAPI 1.0 standards have also been finalised. This has introduced a small set of significant changes that impact existing implementations.

During this time, the OIDF—which governs the FAPI specifications—has developed the second version of their FAPI profile (FAPI 2.0). FAPI 2.0 applies key lessons from the implementation of FAPI 1.0 globally and makes improvements to security whilst as the same time simplifying the complexity and cost of implementation.

Increasing interoperability and lowering the cost of adoption and maintenance
As many countries look to adopt regulated Consumer Data Right regimes, similar challenges are faced and similar solutions are likely to be developed. Leveraging international standards has the benefits of stronger vendor adoption which lowers the cost of implementation to Australian organisations.

Adopting the lessons from other countries whilst allowing Australia, in many cases leading the global design of economy-wide Consumer Data Rights, facilitates better standards that will prove to be more interoperable across international borders.

Through the alignment to international standards, this directly increases the CDR's global interoperability and opens the Australian economy to investment whilst allowing growth opportunities into adjacent international markets.

The requirements of the CDR should be quantifiable and testable
Despite the benefits of maintaining alignment to key international standards, at times there are requirements within the CDR which require changes on top of these standards due to the CDR's policy and rules requirements.

This can be supported through the development of attacker models and authentication risk frameworks to provide an objective, testable framework to makes changes that improve convenience, consumer experience and security for the Australian economy and the needs, technology competencies and capabilities of Australians and local regulations that apply within Australia.

Having an information security profile that is testable can offer greater certainty to all participants whilst establishing a certification path for participants and vendors alike that ultimately increases implementation confidence.

Transitioning a complex ecosystem must be phased
The uplift of standards is not as simple as adopting those changes overnight. In a complex many-to-many ecosystem such as the CDR, uniform implementation of the data standards is fundamental to its operation. Consequently, a transition plan between the current Information Security profile and the target state is critical to maintain operations.

To that end, this decision record makes recommendations regarding further consultations to address *how* the transition to defined target states should occur.

Decision To Be Made

Determine the desired target state for the Information Security profile, high-level transition pathway and future consultations required to achieve the desired target state of the Information Security profile for the Consumer Data Standards.

Feedback Received

The Data Standards Chair welcomes the feedback of all participants in response to this Decision Proposal. The feedback provided strong consensus for a preferred target state for the Information Security profile that is in line with the DSB's intentions of providing a safe and secure environment for consumers' data rights.

Feedback was in response to seven questions. The feedback is summarised against each question below.

Question 1 – What are the existing gaps or concerns with the information security profile?

- Most respondents supported uplifting to the final FAPI 1.0 profile as the primary gap including components of the FAPI 1.0 profile such as Proof-Key For Code Exchange (PKCE) and JWT Secured Authorization Response Mode (JARM).
- Whilst some recommended JARM, others noted that there has been a shift away from adopting JARM and instead moving to align towards FAPI 2.0 would be a better investment for the CDR
- Some feedback supported retaining the Information Security profile and only make changes where critical security defects are identified.

Question 2 – What gaps or concerns with the information security profile would prevent voluntary extension to write operations by a data holder?

1. Feedback was slightly more diverse compared to Question 2 however it was predominantly recommendations to support standards defined within the FAPI 1.0 profile or draft FAPI 2.0 profile including Rich Authorization Requests (RAR). Some feedback was outside the scope of the data standards such as considerations around liability frameworks.
2. Some feedback indicated that the CDR consent model should be improved to support two-to-sign / joint account provisions. Noting that the v3 rules change the joint account arrangements, any two-to-sign consent changes would be dependent upon the requirements laid out in the rules.

Question 3 – What aspects of version 1.0 of the FAPI Advanced Security profile, if any, should be prioritised for adoption by the CDR?

1. All feedback supported the adoption of FAPI 1.0.
2. The banking industry proposed a timeframe of 24 months to fully support FAPI 1.0 comprised of 12 months for ADR obligations then a further 12 months for data holders (banks).

Question 4 – What priority should be given to transitioning to FAPI 2.0?

1. The banking industry supported adopting FAPI 2.0 as a precursor for action initiation.
2. The banking industry did not support the UK's Lodged Intent model.
3. Adoption of FAPI 2.0 should be considered against vendor supportability.

Question 5 – What additional patterns or normative standards should be considered for adoption to reduce the risk of write operations?

1. Participants supported enhancing authentication:
    a. Additional authentication methods
    b. Decoupled authentication (sometimes referred to as App 2 App) using Client Initiated Backchannel Authentication (CIBA)

    c. Two-factor authentication
2. Banks supported CIBA but they did not support other authentication options such as 3DSecure.

Question 6 – What additional changes, if any, that should be considered for maximising international operability?

1. Alignment to FAPI 1.0 was consistently recommended to assist with international interoperability.
2. Some banks and vendors advocated including Security Event Tokens, OpenID Shared Signals and Events Framework, and OpenID Continuous Access Evaluation Profile to facilitate securely notifying third parties when key events for consent or initiated actions occur.
3. There was consistent feedback that the DSB interact with international bodies such as the OpenID Foundation.
4. Some respondents noted adoption of OpenID Connect for Identity Assurance 1.0 as a potential framework for Identity Assurance and/or KYC requirements
5. The banking industry requested conformance and certification testing processes (see Question 7).

Question 7 – What steps could be taken by the DSB to assure the efficacy of the information security profile?

1. Feedback consistently requested the DSB provide conformance testing tools and a certification program that allows participants and vendors certify against a comprehensive test suite.
2. The majority of feedback supported the development of a CDR Attacker Model and a minimum authentication requirements / risk-based authentication framework was consistently supported, with the OpenID Foundation FAPI Attacker Model referenced as an example.
3. Some feedback recommended changes to the publication process of the Information Security standards for readability.
4. Many respondents suggested enhanced authentication functionality echoing the feedback received to Question 5

General feedback

The feedback from the banking sector was universally supportive of moving to adopt FAPI 2.0.

The schedule outlined by the banking sector may not achieve the policy objectives presented in the Future Directions report in the desired timeframes. This would require the banking sector, as the first operational sector in the CDR, to prioritise and support uplift faster to achieve the agreed target state.

Current Recommendation

This decision document recommends a set of key target states and specific future decision proposals to address targeted problem spaces based on the feedback received.

Recommendation 1: Adopt FAPI 1.0 Advanced Profile

It is recommended that the data standards adopt FAPI 1.0 Baseline and Advanced Profile as the first transition stage.

This recommendation requires a targeted decision proposal consultation on the gap analysis and transition from FAPI ID2 Draft 06 to FAPI 1.0.

This recommendation is considered a mandatory transition state to the other recommendations. It is recommended that FAPI 1.0 profile adoption should be prioritised before Energy obligations. This ensures alignment across the banking and energy sectors on a common Information Security profile.

Adoption should be in line with the requirements of the CDR and any appropriate security controls currently defined.

The banking industry proposed a timeframe of 24 months to transition the CDR to FAPI 1.0. This timeframe may not be achievable in the broader context of new sectors onboarding into the CDR and the desired timeframes around many of the recommendations laid out in the Future Directions report if they were to be taken up. To achieve FAPI 1.0 as a critical transition state, the banking sector must be capable of uplifting in a timeframe that gives certainty for the energy sector and cross-sectoral ADRs.

The benefit of aligning all sectors to FAPI 1.0 within the implementation timeframes of the energy sector will allow the energy sector to define to a stable benchmark with strong vendor support.

Key Future Directions Recommendations

- Recommendation 8.9 – Using open international standards where available
- Recommendation 8.10 – When diverging from open international standards

Recommendation 2: Adopt the FAPI 2.0 Profile

It is recommended that the data standards adopt FAPI 2.0 Baseline Security Profile and family of standards as the baseline target state to the CDR's Information Security profile.

This recommendation is the target state *after* transition to FAPI 1.0. This recommendation is a mandatory target state prior to the introduction of Action Initiation within the CDR provided data holders and vendors can achieve the required timeframes before the obligation dates for introducing Action Initiation within the CDR.

Adoption should be in line with the requirements of the CDR and any appropriate security controls currently defined.

In meeting the implementation objectives laid out in the Future Directions report, transition to FAPI 2.0 may need to be made within a 24-month timeframe across Accredited Data Recipients (ADRs) and DHs to facilitate the introduction of Action Initiation and stronger customer authentication. Adopting FAPI 2.0 is strongly supported by the banking industry.

This includes the family of standards defined in the FAPI 2.0 profile including, but not limited to:

- **Rich Authorization Requests (RAR):** to support a rich CDR consent and permissioning model between third parties and data holders for data sharing, purpose-based consent, and action initiation.
- **Pushed Authorization Requests (PAR):** For lodging authorisation requests in a secure method in the back channel.
- **Proof-Key For Code Exchange (PKCE):** Enhances security whilst reducing implementation complexity for third parties
- **FAPI Client Initiated Backchannel Authentication (FAPI-CIBA):** To support decoupled authentication and two-factor authentication
- **Grant Management API (GM-API):** For the management of authorisation permissions

Beyond FAPI 2.0, data standards to be consulted upon include:

- **Shared Signals and Events Framework (SS&E), OpenID Continuous Access Evaluation Profile (CAEP) , and OpenID Security Event Tokens (SET):** to facilitate secure communication of state changes, events and notifications to third-parties
- **OpenID Connect for Identity Assurance 1.0 (IDA):** to support verified claims and identity assurance and/or KYC requirements in use cases such as account switching, origination and identification

Key Future Directions Recommendations

- Recommendation 5.21 – Identity verification assessments
- Recommendation 8.9 – Using open international standards where available
- Recommendation 8.10 – When diverging from open international standards

Recommendation 3: Attacker Model, Security Controls, Authentication and Identity Proofing Risk Framework

It is recommended that a threat and attacker model be developed for the Consumer Data Standards, including a risk-based assessment framework for determining security controls and authentication methods, identity proofing requirements, and consequently strengthen the control environment with appropriate risk-based controls.

Feedback strongly supported the development of an attacker model to identify the risks the Information Security model seeks to address, and the controls required to manage those risks. This attacker model can leverage the FAPI 2 attacker model as a baseline developed by the OIDF.

The Data Standards Chair notes that the Future Directions report includes several key recommendations to enhance security, flexibility, and choice for consumers. These recommendations seek to adopt a risk-based approach to assessing which authentications methods be supported and when they are appropriate. In considering which authentication methods are suitable, the convenience and consumer experience of different authentication mechanisms should be considered against the actions being instructed and the risks both within a given sector and across the CDR. This recommendation supports and complement the Future Direction report's recommendations.

A risk-based authentication framework should look at when and how second factors of authentication are required and opportunities to support decoupled authentication (otherwise referred to as app2app).

In conjunction broadening authentication standards, the risk framework should consider the identity proofing requirements when initiating different actions.

Key Future Directions Recommendations

- Recommendation 1.1 – Balanced approach to safety, efficiency and effectiveness
- Recommendation 4.14 – Authentication requirements by data holders
- Recommendation 4.15 – More explicit requirements for accredited persons to authenticate customers
- Recommendation 5.11 – Authentication requirements for payment initiation
- Recommendation 8.1 – Support for development of authentication solutions interoperable with the Consumer Data Right
- Recommendation 8.2 – Minimum assurance standard for authentication to apply to data holders and accredited data recipients
- Recommendation 8.3– Minimum assurance standard for authentication to include a risk taxonomy and matrix
- Recommendation 8.10 – When diverging from open international standards

Recommendation 4: A Rich Consent Taxonomy For Action Initiation

It is recommended that an extensible CDR consent model be defined which provides an extensible base for fine-grained action initiation and data sharing that is sector agnostic.

Consultation should consider the existing needs of the CDR in determining how the current data sharing consent requirements can be defined within a FAPI 2.0 Rich Authorisation Request (RAR) structure. Extensions to the CDR consent model should be considered based on specific needs arising from additional sectors, purpose-based consent, and possible extension to action initiation.

Key Future Directions Recommendations

- Recommendation 1.1 – Balanced approach to safety, efficiency and effectiveness
- Recommendation 4.10 – Consent to send instruction and consent to initiate action
- Recommendation 4.12 – Ongoing consent arrangements
- Recommendation 4.16 – Authorisation to take a specific action
- Recommendation 4.17 – Data holders to require explicit consumer authorisation to accept instructions
- Recommendation 5.12 – Fine-grained payment initiation authorisation
- Recommendation 6.19 – Consumer Data Right dictionary
- Recommendation 6.20 – Industry recommended and endorsed consents
- Recommendation 7.11 – Protections for action initiation instructions to be considered in the privacy and security assessments

Implementation Considerations

Cross-sectoral considerations

With the Energy sector nearing standards finalisation and the Treasury looking at an economy-wide view, uplifting to FAPI 1.0 will provide immediate implementation certainty for sectors beyond banking. Data Recipients need a common Information Security profile to develop solutions across sectors. Commencing with the uplift of the standards to support FAPI 1.0 will achieve near-term consistency and certainty.

A pathway towards FAPI 2.0 will impact sectors beyond just banking. A well-defined pathway towards FAPI 2.0 will need to consider the phasing requirements across several sectors. Prioritising this uplift with the support of the banking sector will enable the successful adoption ahead of the CDR's expansion into Action Initiation. Ensuring that ADRs can implement FAPI 2.0 client requirements such as PKCE without Data Holders prohibiting this will allow for interoperability during transition towards a FAPI 2.0 target state.

Banking sector

Transitioning the banking sector, including active ADRs, will need to consider migration path that minimises any breaking changes.

CDR Register standards

In considering the alignment to FAPI 1.0 and FAPI 2.0 profiles, there are likely impacts to the CDR Register, dynamic client registration and general functions of the CDR Register acting as the trust authority for the CDR. These considerations will need to be consulted on as part of phasing.

Vendor support

To successfully uplift to FAPI 2.0 within the potential timeframes for action initiation as well as the inclusion of energy and the telecommunications sector, vendor support for the standards defined within the FPAI 2.0 profile need to be considered, or where a lack of vendor support is present, alternative mechanisms to achieve the policy requirements of the CDR.

Conformance testing

No recommendation is provided regarding conformance testing. Feedback from many respondents strongly supported the DSB taking an active role in developing a comprehensive conformance and certification (test) suite. Whilst the DSB recognises the need for conformance tools, this responsibility is currently shared with the ACCC. Further discussions are required to progress any recommendations.

Participant capability

Providing mechanisms for participants to comprehensively describe their capability has already been identified as a change to be made to the data standards. With the transitioning of the ecosystem in a phased approach along with any moves towards more choice and expressive consent models, it is likely that a discovery mechanism will facilitate better interoperability and resilience for the entire ecosystem. Consideration will need to be given to what key functionality requires discovery and how that discovery and negotiation between third-party client and data holder will be facilitated.

Appendix – International Working Groups

A consistent piece of feedback in this consultation was that the DSB, on behalf of the Data Standards Chair, should be involved in international working groups such as the OpenID Foundation's FAPI working group.

It is important to note that the DSB, on behalf of the Data Standards Chair, is an active participant in the Global Open Financial Technical Standards (GOFTS) Working Group. GOFTS seeks to advance shared technical standards amongst countries that adopt consumer data standards.

The DSB, on behalf of the Data Standards Chair, is a member of the OpenID Foundation and subscribed to participate in the following working groups:

a. **Financial-grade API (FAPI) WG**
b. **eKYC & IDA WG**
c. **Enhanced Authentication Profile (EAP) WG**
d. **HEART WG**
e. **International Government Assurance Profile (iGov) WG**
f. **Shared Signal & Events WG**

The DSB will continue to review involvement in these working groups and assess involvement in other OIDF working groups.

Appendix – Future Direction Report Recommendations

The DSB considered many broader CDR drivers and strategic requirements in this decision document. The Future Directions report provided a source of strategic recommendations which were considered in the context of other clear and immediate needs to continue to maintain the Information Security profile of the Consumer Data Standards. This document does not seek to presuppose those recommendations, however where possible, alignment to the recommendations was considered.

Recommendation 1.1 – Balanced approach to safety, efficiency and effectiveness

Recommendation 1.1 – Balanced approach to safety, efficiency and effectiveness

The Consumer Data Right should be developed to be safe, efficient and effective. A balanced approach is needed to realise meaningful benefits to consumers and grow participation in the data ecosystem.

Recommendation 4.10 – Consent to send instruction and consent to initiate action

Recommendation 4.10 – Consent to send instruction and consent to initiate action

Accredited persons should be required to obtain access and usage consents to initiate actions for consumers. These consents should be voluntary, express, informed, specific as to purpose, time-limited and easily withdrawn.

Recommendation 4.12 – Ongoing consent arrangements

Recommendation 4.12 – Ongoing consent arrangements

Consumers should be able to provide consents to accredited persons to initiate actions on their behalf on an ongoing basis, within the consent's time limit. Additional safeguards should also be considered for inclusion in the Rules.

Recommendation 4.14 – Authentication requirements by data holders

Recommendation 4.14 – Authentication requirements by data holders

Data holders should be obliged to authenticate consumers prior to requesting action initiation authorisations.

Authentication requirements should be reviewed by the Data Standards Body to ensure they reflect the risks associated with action initiation.

Recommendation 4.15 – More explicit requirements for accredited persons to authenticate customers

Recommendation 4.15 – More explicit requirements for accredited persons to authenticate customers

The Consumer Data Right should include explicit requirements for accredited persons offering action initiation enabled services to authenticate customers in circumstances where there is an ongoing provision of service to that customer. These requirements should be based on international standards on authentication processes.

Recommendation 4.16 – Authorisation to take a specific action

Recommendation 4.16 – Authorisation to take a specific action

Whether the taking of a particular action should require a specific authorisation to be given to a data holder should depend upon the nature of the action requested and other factors, such as the value of the transaction and existing practices and processes in the sector. These requirements should be enabled in the Rules and specified through the Standards.

Recommendation 4.17 – Data holders to require explicit consumer authorisation to accept instructions

Recommendation 4.17 – Data holders to require explicit consumer authorisation to accept instructions

Data holders should only progress actions initiated by accredited persons when they have received the consumer's explicit authorisation to do so. The Data Standards Body should investigate the benefits of enabling fine-grained authorisation for specific action classes, with recommendations being driven by consumer experience and security considerations.

Recommendation 5.11 – Authentication requirements for payment initiation

Recommendation 5.11 – Authentication requirements for payment initiation

Authentication requirements for authorised deposit-taking institutions and accredited persons engaged in payment initiation should be determined based on an assessment of the risks inherent to payment initiation, as well as the need for consistency in the consumer experience.

Recommendation 5.12 – Fine-grained payment initiation authorisation

Recommendation 5.12 – Fine-grained payment initiation authorisation

Consumers should be able to provide some level of specificity to their banks when authorising them to accept payment initiation instructions from an accredited person through the Consumer Data Right. The level of specificity required should be determined in the Rules and Standards.

Recommendation 5.21 – Identity verification assessments

Recommendation 5.21 – Identity verification assessments

The Consumer Data Right should support consumer-directed sharing of Know Your Customer outcomes to the extent to which reliance is allowed on that outcome, in the event that proposed amendments to the reliance provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* are passed by Parliament.

Recommendation 6.19 – Consumer Data Right dictionary

Recommendation 6.19 – Consumer Data Right dictionary

The Data Standards Body should include as part of the Consumer Experience Standards, a non-exhaustive dictionary outlining, in plain English, definitions of common terms used in Consumer Data Right consents. For usage consents, this should include common understandings of purposes.

Recommendation 6.20 – Industry recommended and endorsed consents

Recommendation 6.20 – Industry recommended and endorsed consents

Industry and consumer groups should be encouraged to develop and endorse standard wording for Consumer Data Right consents for specific purposes, and accredited persons should be permitted to display these endorsements in their consent processes through icons, descriptions, links or other appropriate methods.

Recommendation 7.11 – Protections for action initiation instructions to be considered in the privacy and security assessments

Recommendation 7.11 – Protections for action initiation instructions to be considered in the privacy and security assessments

The privacy impact assessment and information security assessment should consider appropriate protections, proportionate to the risks involved for action initiation authorisation, consent and instruction data and, if warranted, identify protections that need to be put in place.

Information security protections for action initiation authorisation, consent and instruction data should be proportionate to the risks presented by misuse of this data.

The assessments should occur before the legislation is settled to determine what should be captured in the primary legislation, the Rules or Standards.

Recommendation 8.1 – Support for development of authentication solutions interoperable with the Consumer Data Right

Recommendation 8.1 – Support for development of authentication solutions interoperable with the Consumer Data Right

The Consumer Data Right should continue to be developed in a manner that encourages the use of interoperable authentication solutions, based on compatible international standards.

Recommendation 8.2 – Minimum assurance standard for authentication to apply to data holders and accredited data recipients

Recommendation 8.2 – Minimum assurance standard for authentication to apply to data holders and accredited data recipients

The Data Standards Body should develop a minimum assurance standard for authentication applicable to both data holders and accredited data recipients. The standard should support interoperability and flexibility for participants, provided minimum assurance standards and consumer experience standards are met.

The standard should include provision of safe harbours for existing authentication requirements for current data sets and functions.

Recommendation 8.3– Minimum assurance standard for authentication to include a risk taxonomy and matrix

Recommendation 8.3– Minimum assurance standard for authentication to include a risk taxonomy and matrix

As part of the minimum assurance standard for authentication the Data Standards Body should develop a risk taxonomy and risk matrix against which assurance levels for particular data sets and Consumer Data Right functions in each sector can be determined with a degree of consistency. This taxonomy and matrix should form part of the minimum assurance standard used to inform the level of assurance required, noting that other considerations will also factor. It should consider the nature of data, likelihood of harm to consumers if data is misused and other key factors that the Data Standards Body considers appropriate. This should be developed in consultation with industry and consumers.

Recommendation 8.9 – Using open international standards where available

Recommendation 8.9 – Using open international standards where available

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

Recommendation 8.10 – When diverging from open international standards

Recommendation 8.10 – When diverging from open international standards

Where divergences from open international standards are proposed, the reason for this should be clearly articulated during consultation, giving stakeholders a chance to comment on whether alignment or divergence would be the most appropriate course.