Data Standards Body

Technical Working Group

Decision 347 – Maintenance Iteration 19

Contact: Mark Verstege, Hemang Rathod, Nils Berge

Publish Date: 24 June 2024

Decision Approved By Chair: 28 June 2024

Context

This decision relates to the issues consulted on in Maintenance Iteration 19 of the Data Standards. This maintenance iteration incorporates Information Security, CX, Banking, Energy and CDR Register standards. The details for this iteration can be found at: DSB Maintenance Iteration 19 Agenda & Minutes.

Additionally, processes and an overview of the maintenance operating model can be found at: https://github.com/ConsumerDataStandardsAustralia/standards-maintenance.

Decision To Be Made

Changes related to the standards arising from the issues consulted in the maintenance iteration.

Feedback Provided

Below is a list of the issues addressed in this iteration. Each issue has a link to the issue thread containing the public consultation relating to the issue:

Iss. #	Sector	Issue	Decision	Change Type	Obligation Date	Notes
638	All	Maintenance Iteration 19 Holistic Feedback	No Change	N/A	N/A	*Detail in following section*
643	Security	Update TLS cipher suite requirements to address DHEat Attacks and Raccoon Attack vulnerabilities	**Change Recommended**	**Non-Breaking Change**	N/A	Stage 1 change: Allow DHs to stop supporting vulnerable TLS ciphers.
415	Security	Disambiguation of the claims for a response from the introspection endpoint	**Change Recommended**	**Non-Breaking Change**	N/A	Clarify infosec standards with regards to token introspection response for active tokens.
633	CX	Collection Consents - Authorisation Amendment	**Change Recommended**	**Non-Breaking Change**	N/A	Clarify CX and infosec standards with regards to consent amendment.
640	Energy	Retirement date for Get Generic Plan Detail v2 and Get Energy Account Detail v3	**Change Recommended**	**Non-Breaking Change**	N/A	Change retirement date of deprecated versions of noted APIs.
615	Admin	Plan Obligation Milestones for 2025	**Change Recommended**	**Non-Breaking Change**	N/A	Update standards with obligation milestones for 2025.
362	Security	Security Profile: Request Object - Inconsistency in example for sharing_duration and cdr_arrangement_id	No Change	N/A	N/A	No change required because standards align with upstream specification.

Iss. #	Sector	Issue	Decision	Change Type	Obligation Date	Notes
573	CX/Security	Clarification on handling of standard claims in request object	Defer	N/A	N/A	Deferred to MI20.

Decisions For Approval

Issue 638 - Maintenance Iteration 19 Holistic Feedback

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/638

Change Impact
No Change

Decision
No changes identified.

Background
This is the regular Maintenance Iteration Holistic Feedback Change Request that is created at the beginning of each maintenance iteration to capture trivial changes to the standards that do not warrant a dedicated Change Request.

Issue 643 - Update TLS cipher suite requirements to address DHEat Attacks and Raccoon Attack vulnerabilities

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/643

Change Impact
Non-Breaking Change

Decision
The decision is to immediately deprecate the use of vulnerable TLS ciphers by replacing:

Ciphers
Only the following cipher suites SHALL be permitted in accordance with section 8.5 of [FAPI-1.0-Advanced]:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

With:

Ciphers
Only the following cipher suites **SHALL** be permitted in accordance with section 8.5 of [FAPI-1.0-Advanced]:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The following cipher suites **SHOULD NOT** be supported:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Background

A recent vulnerability in the supported TLS ciphers has been identified by the FAPI Working Group. These ciphers, TLS_DHE_RSA_***, which are currently recommended by FAPI are also permitted by the Consumer Data Standards. Details of the vulnerabilities are available here.

This change request was raised late in the maintenance iteration and discussed in the last call given due to the security implications.

The DSB proposed a two-stage approach to address the vulnerabilities:

Stage 1: Deprecate the use of vulnerable ciphers:
This stage proposes immediate deprecation of the vulnerable ciphers by recommending that they SHOULD NOT be supported. This shall leave it to the discretion of the Data Holders how quickly they adopt this recommendation. This is noted in the decision above.

Stage 2: Adopt BCP 195 rather than explicitly listing required ciphers
This stage changes the supported ciphers section to remove reference to explicit ciphers, and instead, refer to BCP 195. There are some relevant TLS considerations in the FAPI profile, so it is proposed that the standard is changed to clearly adopt section 8.5 of FAPI 1 Advanced, and then further constrain it by only permitting ciphers recommend in the current BCP 195.

Participants on the call provided support for stage 1 to be included in this iteration as it would give data holders immediate ability to deprecate support for the ciphers. All participants on the call also noted that they, via their own security practices, already decommissioned support for the vulnerable ciphers.

Only Stage 1 is recommended for this decision. It represents a non-breaking change that can be introduced with immediate effect. Stage 2 changes will be consulted on and applied in the next MI.

Issue 633 - Collection Consents - Authorisation Amendment

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/633

Change Impact
Non-Breaking Change

Decision
The decision is to update the CX and Security Profile standards to clarify that the ADRs must provide the relevant `cdr_arrangement_id` for consent amendments. The specific changes are noted below:

1. **Change Amending Authorisation Standards from:**

Area	CX Standard
Authorisation: Amending consent	The following standards apply when a Data Holder invites a CDR consumer to amend a current authorisation as per rule 4.22A and the ADR has supplied a *cdr_arrangement_id*:

To:

Area	CX Standard
Authorisation: Amending consent	The following standards apply when a Data Holder invites a CDR consumer to amend a current authorisation as per rule 4.22A and in accordance with Specifying an existing arrangement:

2. **Add the following addition to the Consent Standards table:**

Area	CX Standard
Consent: Amendment of Collection Consents and Authorisations	When notifying a Data Holder of an amended collection consent as per rules 4.18C or 4.20S, Data Recipients **MUST** supply the relevant CDR Arrangement ID to the Data Holder according to Specifying an existing arrangement. Providing the CDR Arrangement ID is necessary to trigger the Data Holder authorisation flow simplifications outlined in the Amending Authorisation Standards. Failure to supply the CDR Arrangement ID will result in the full authorisation flow and a disconnected data sharing arrangement history on consumer dashboards.

3. **Replace following in "Specifying an existing arrangement" subsection in the Request Object section of information security standards**

From:

Specifying an existing arrangement

Provided a Data Holder supports PAR, they **MUST** also support the `cdr_arrangement_id` claim provided in the Request Object sent to the PAR End Point. The Data Recipient Software Product **MAY** provide the `cdr_arrangement_id` claim in the Request Object sent to the PAR End Point.

If a Data Recipient Software Product provides the `cdr_arrangement_id` claim in the request object to the Data Holder's PAR End Point, the Data Holder **MUST** revoke any existing tokens related to the arrangement once the new consent is successfully established and a new set of tokens has been provided to the Data Recipient Software Product.

To:

Specifying an existing arrangement

To facilitate the amending of an existing arrangement, the following statements apply:

- Data Holders **MUST** support the *cdr_arrangement_id* claim provided in the Request Object.
- The Data Recipient Software Product **MUST** provide the *cdr_arrangement_id* claim in the Request Object if requesting to amend a current authorisation in accordance with Consent: Amendment of Collection Consents and Authorisations.
- Data Holders **MUST** treat the request under the Amending Authorisation Standards if the *cdr_arrangement_id* claim is provided.

If a Data Recipient Software Product provides the *cdr_arrangement_id* claim in the request object to the Data Holder's PAR endpoint, the Data Holder **MUST** revoke any existing tokens related to the arrangement once the new consent is successfully established and a new set of tokens has been provided to the Data Recipient Software Product.

Background

The current standards are not clear in stating that ADRs must provide the relevant `cdr_arrangement_id` in order for the authorisation amendment to operate as intended.

The consequence of failing to provide the relevant `cdr_arrangement_id` is that data sharing arrangements will be disconnected on consumer dashboards. Further, the simplified amending authorisation flow is only triggered when the `cdr_arrangement_id` is provided by the ADR.

This change request was raised to amend the standards to clarify that if an ADR invites a consumer to amend a collection consent, then they must provide the relevant `cdr_arrangement_id` to the data holder for the corresponding authorisation to be amended as per the rules.

Four options were discussed during the MI. The participants agreed on adopting option 4 which is noted in the decision above. This will result in non-breaking change whilst providing clarity in both the CX and security standards that the `cdr_arrangement_id` is required for authorisation amendments.

Issue 362 - Security Profile: Request Object - Inconsistency in example for sharing_duration and cdr_arrangement_id

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/362

Change Impact
No Change

Decision
The decision is to not proceed with the proposed changes to the Standards or guidance.

Background
This change request was raised highlighting inconsistency in the non-normative example in the standards depicting how the `sharing_duration` and `cdr_arrangement_id` claims are represented within the request object.

Analysis concluded that the non-normative example is consistent and aligned with upstream OIDC specification. As a result, no change is necessary, which participants agreed with.

Issue 415 - Disambiguation of the claims for a response from the introspection endpoint

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/415

Change Impact
Non-Breaking Change

Decision
The decision is to amend the Introspection Endpoint sub-section in Security Endpoints from:

> A Token Introspection End Point Response SHALL include, at least, the following fields:
> - active: Boolean indicator of whether or not the presented token is currently active.
> - exp: A JSON number representing the number of seconds from 1970-01-01T00:00:00Z to the UTC expiry time.
> - scope: A JSON string containing a space-separated list of scopes associated with this token.
> - cdr_arrangement_id: A unique identifier of the CDR arrangement related to the authorisation.

To:

For currently active tokens, a Token Introspection End Point Response **SHALL** include, at least, the following fields:

- *active*: Boolean indicator of whether or not the presented token is currently active.
- *exp*: A JSON number representing the number of seconds from 1970-01-01T00:00:00Z to the UTC expiry time.
- *scope*: A JSON string containing a space-separated list of scopes associated with this token.
- *cdr_arrangement_id*: A unique identifier of the CDR arrangement related to the authorisation.

Background

When responding to token introspection requests, DHs need to align with the upstream Oauth 2.0 Token Introspection standards for inactive tokens. This is not clear in the current standards and is clarified in a guidance article.

This change request was raised to update the standards language ensuring the expected DH behaviour is clear and in alignment with the guidance.

There were no objections to the above proposed change, which is non-breaking.

Issue 640 - Retirement date for Get Generic Plan Detail v2 and Get Energy Account Detail v3

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/640

Change Impact

Non-Breaking Change

Decision

The decision is to change the retirement date for Get Generic Plan Detail v2 and Get Energy Account Detail v3 endpoints to March 3rd 2025.

Background

The version for Get Generic Plan Detail and Get Energy Account Detail endpoints were incremented to v2 and v3 respectively due to changes resulting from the last MI. The retirement date for the deprecated versions was set to 12 months after the obligation date for the new version.

This change request was raised to change the retirement date to March 3rd 2025, reducing the duration DHs will have to maintain support for the deprecated API versions to 3 months.

Participants supported this change.

Issue 615 - Plan Obligation Milestones for 2025

Link to issue:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/615

Change Impact

Non-Breaking Change

Decision

To remove dates prior to 2024 (these will remain available in archived versions of the Standards), and to add the following dates for 2025:

Obligation Milestone	Milestone Date
Y25 #1	17 March 2025 (2025-03-17)
Y25 #2	12 May 2025 (2025-05-12)
Y25 #3	14 July 2025 (2025-07-14)
Y25 #4	08 September 2025 (2025-09-08)
Y25 #5	10 November 2025 (2025-11-10)

Background

The Milestone Dates in the Obligation Dates Schedule currently only extend to **Y24 #5**: 2024-11-11. To provide the CDR participants with forward notice of when obligations *may* apply in future, a schedule of obligation dates for 2025 was proposed, to extend upon the existing obligation schedule. As a result, this gives participants forward notice for resource planning. Participants agreed that milestone dates for 2025 be published in advance, to allow any upcoming changes to be assigned to them.

Documentation and schema changes

The following change requests are for minor changes to correct formatting and spelling issues:

Issue #	Change Type	Change Description
#377 - Review FDO table	Documentation change	Remove Future Dated Obligations associated with dates prior to 2024 as they have passed and are no longer relevant.
#394 - Fix typo 'registeration'	Documentation change	Fix typo 'registeration' in the NBL Candidate Standards.
#395 - Enhancements to Banking documentation	Documentation change	The development of the Candidate Standards for Banking Decision Proposal 306 and Non-Bank Lending included minor styling enhancements to improve readability and interpretation. In addition to applying further minor enhancements related to issue #527 - Fix spelling, grammar and punctuation errors across the API specification across all three related specifications, this change applies the presentational styling changes in the two Candidate Standards to the Binding Banking Standards to provide visual consistency only. No change in the meaning of the Candidates or Binding Standards is intended.
#396 - Improve clarity of the PerformanceMetricsV3 structure	Documentation change	The Standards build process doesn't show the content of deeply nested arrays in some parts of the documentation. This change reduces the depth of the nested objects to

Issue #	Change Type	Change Description
		allow each level to be displayed more clearly. This change is enabled by reorganising the schema by using references, without changing the overall property structure and is therefore considered a non-breaking documentation change. This change is cosmetic to improve the presentation of the standards for readers.
#400 - Enable generic links to schemas	Standards publishing	The Standards build process generates anchor links to key elements in the documentation. Where schemas are defined, the anchors include the version of the schema. Where guidance articles refer to a schema in a general sense (not related to a specific version) links from the guidance will break when the version changes. This change will provide anchors in the documentation without versions, so general guidance can remain relevant over a longer period; increasing value and reducing maintenance. This change improves the presentation of the standards and allows readers to link to unique document locations.
#402 - Update Consumer Data Right link	Documentation change	The *Consumer Data Right* link in the introductory section of the Standards currently refers to the ACCC but redirects to the cdr.gov.au website. This change updates the *href* and removes the *title* to reflect the correct target page.

Implementation considerations

When possible, consideration and preference to non-breaking change has been prioritised with community consultation. Where breaking changes have been recommended, future dated obligations have been proposed in consultation with participants during the course of the Maintenance Iteration to ensure sufficient lead time for implementation.

Implementation considerations for each change request have been considered and detailed within each change request summary.