Data Standards Body

Technical Working Group

Decision 161 – Banking Maintenance Iteration 6

Contact: Mark Verstege

Publish Date: 26th April 2021

Decision Approved By Chairman: 29th April 2021

Context

This decision relates to the issues scheduled for review in maintenance iteration 6 of the Banking sector standards. The details for this iteration, including 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 addressed 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:

Issue #	Issue	Change Status	Obligation Date
#360	Client Authentication improvements for Admin API	Change recommended	Non-breaking
#368	Define deprecation date for PRD v2	Change recommended	Non-breaking
#372	Define deprecation date for Get Metrics v1	Change recommended	Non-breaking
#264	Clarification to NFR public traffic threshold for other ADI's with multiple brands	No Change	Not applicable
#338	CORS - Add CDR specific headers to access-control-expose-headers in response header	No Change	Not applicable
#358	Endpoint registry (obligation) for data holders	No Change	Not applicable
#367	Specify how participants can maintain synchronisation of consents after outages	No Change	Not applicable
#374	MTLS and Client authentication requirements for PAR endpoint	No Change	Not applicable

In addition, the following documentation fixes were consulted on during the iteration:

- **#369: Remove historical audience claim requirements for Data Recipients calling Data Holders defined in the Client Authentication section**
  https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/369
- **#345: Review property requirements in Get Metrics schemas**
  https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/345

Decisions For Approval

Client Authentication improvements for Admin API

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/360

Change Impact

Non-breaking

Decision

The decision based on consultation is to allow Data Holders to authenticate the CDR Register's client credentials at their Authorisation Server using private key JWT client authentication. Self-signed JWT client authentication will continue to be supported by the CDR Register and Data Holders may continue to support this method of authenticating the CDR Register if preferred.

Background

This change allows Data Holders to choose between authenticating the CDR Register's client credentials at the admin endpoint being called or enrol the CDR Register as an oAuth client that is authenticated at the Data Holder's authorisation server in exchange for an access token to call the admin endpoint.

When the CDR Register calls the Data Holder's admin endpoints, such as Get Metrics, the CDR Register will do so according to the registered method of client authentication supported by that Data Holder. This is facilitated through the capturing of additional metadata held by the CDR Register in relation to each Data Holder's implementation.

Define deprecation date for PRD v2

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/368

Change Impact

Non-breaking

Decision

PRD v3 endpoint obligations commenced on February 28th 2021. Based on community feedback it was decided that the retirement data for PRD v2 endpoints is set to May 31st 2021 to give ADRs sufficient time to transition to calling version 3 of the PRD endpoints.

Clarification to NFR public traffic threshold for other ADI's with multiple brands

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/264

Change Impact

No change

Decision

The decision is that NFRs will not be changed. Where a Data Holder presents several distribution brand as separate Data Holder implementations, the NFRs apply to each separate brand, not cumulatively. Where a Data Holder presents distribution brands under the one Data Holder implementation in accordance with the data standard's CDR Federation definitions, a single set of NFRs applies to all brands.

Further specific guidance has been provided in Noting Paper 169 – White Label Conventions that addresses the considerations and expectations for brand representation within the CDR.

CORS - Add CDR specific headers to access-control-expose-headers in response header

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/338

Change Impact

No change

Decision

The decision is that no change is required to further support CORS. The purpose of the section of the Consumer Data Standards pertaining to CORS is not to restate the external CORS standard in full in the CDR standards. Rather, this obligation has been clarified in the following convention.

Endpoint registry (obligation) for data holders

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/358

Change Impact

No change

Decision

No active decision is taken in regard to this change request. The input is considered under an open Decision Proposal 158 - Participant capability discovery.

Specify how participants can maintain synchronisation of consents after outages

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/367

Change Impact

No change

Decision

The decision is that no change is required.

Context

The CDR Register standards considered the situation where consumers withdraw consent via the Data Holder Dashboard however the ADR is unavailable to receive the withdrawal request. Because there are no availability standards applied to ADRs, Data Holders cannot reasonably determine when an ADR will become available.

Data Holders are required by the rules to notify the ADR when the consumer withdraws consent via the Data holder dashboard, however, they are not expected to implement an exhaustive retry mechanism. The responsibility for availability and timeliness of the ADR solution is the responsibility of the ADR. Further to this, the DH doesn't have visibility of ADR maintenance windows and outages.

Upon restoration of service, it is expected that an ADR would validate all active consents to determine whether (a) they have expired, and if still current (b) whether they have been withdrawn by calling the Data Holder token or token introspection endpoint. If consent is no longer valid, the request will return an error response communicating to the ADR's software product that the refresh token is no longer valid. The ADR would update the consent status and ADR consumer dashboard accordingly.

Define deprecation date for Get Metrics v1

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/372

Change Impact

Non-breaking

Decision

Get Metrics v2 endpoint obligations commence from July 1st 2021. Based on community feedback it was decided that the retirement data for the Get Metrics v1 endpoint be set to October 31st 2021.

MTLS and Client authentication requirements for PAR endpoint

Link to issue:

https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/374

Change Impact

No change

Decision

The decision is no change to the standards is required. MTLS is correctly defined where the communication between the ADR and the Data Holder is via the back channel, whilst TLS is used for front channel communications where the consumer is interacting in the flow.

Implementation considerations

No changes have resulted in breaking changes. Regarding retirement dates to older API endpoint versions, these are the dates *after* which Data Holders may retire support for those versions. However, Data Holders may continue to support those deprecated endpoints beyond those dates. This allows Data Holders to plan their release schedules accordingly taking into consideration other priorities.

Register

The CDR Register will be updated to hold additional metadata related to the Data Holder's preferred client authentication method. The CDR Register will be updated to support both methods of authentication with sufficient lead time to support the go-live of non-major Data Holder consumer data sharing obligations on July 1st 2021.

The ACCC has confirmed the CDR Register will support both V1 and V2 of Get Metrics prior to July up to and including 31st October 2021.

ACCC Certification Test Suite (CTS)

The CTS will be updated to support changes to client authentication arising in Issue 360. It has been confirmed with the ACCC these changes will be made to the CTS with sufficient lead time to support the go-live of non-major Data Holder consumer data sharing obligations on July 1st 2021.