July 2019 Updated Draft Standards

17 July, 2019

Since the previous release on 31 May of the draft Consumer Data Standards (CDS), developed by CSIRO's Data61 for the Data Standards Body, the CDS team has continued to liaise with the broader ecosystem participants to develop and refine the technical standards in support of the Australian Government's Consumer Data Right regime. These draft standards are intended to make it easier and safer for consumers to access data collected about them by businesses, and – with their explicit approval – to share this data via application programming interfaces (APIs) with trusted, accredited third parties.

We are pleased to note that since the May 2019 release, the Product Reference Data API standards have been utilised by three banks in a voluntary release of their Product Data on 1 July, 2019.

In this July 2019 draft update of the CDS, we have pulled together all the work on the standards and Consumer Experience (CX) research. We believe this current release will represent a final draft of the standards, subject to any legislative changes, and provides a stable version of the standards suitable for pilot testing the initial Consumer Data Right (CDR) implementation.

We know that many in the community have been monitoring the discussions relating to the draft CDS and have actively contributed feedback in workshops, on GitHub, via email and in bilateral discussions. We thank the CDR community for your active participation which has helped develop these draft standards and encourage everyone to continue to help evolve these as living standards to serve the future CDR regime.

We will continue our practice of encouraging ongoing comment on the standards and suggestions for improvements and future development through GitHub and the CX workstream. Comments made from the date of this release will be taken into our backlog and considered for incorporation in subsequent releases of the standards.

We will further review the standards when the legislation passes Parliament (expected in the near future) and when ACCC finalises the Rules after passage of the legislation. Any changes to the standards required to assure alignment with the legislation and the rules will be made at that time.

The CDR regime is entering an exciting phase with testing of the rules and standards scheduled to be undertaken in the near future and a live implementation rolled out shortly thereafter. Over this period, we will work with participants in the CDR ecosystem to develop an appropriate operating model for this new phase, through continued consultation on the Decision Proposal that has been published on GitHub.

The Data Standards Body looks forward to ensuring the standards continue to evolve and incorporate new innovations. As they progress to become a reality for Australian consumers, we are committed to working with all CDR participants to build a strong and useful set of standards.

The background in summary:

- The Data Standards Body has been working transparently in public to create and refine draft technical standards since late July 2018, working in parallel with Treasury and the Australian Competition and Consumer Commission (ACCC). The ACCC is responsible for the design of the rules relating to the Consumer Data Right regime. Treasury has carriage of the legislation and Designation Instrument.
    - For a summary of how the process was initiated and how technical decisions have been made, see the following document attached to our 2nd of November draft:

      https://consumerdatastandards.org.au/wp-content/uploads/2018/11/Working-Draft_CDR_2-November-2018-1.pdf
- The ACCC has released draft versions of the applicable rules in December 2018 and a further updated version in April 2019. The Data Standards Body has worked closely with ACCC and Treasury to ensure the CDR standards issued align to the rules, the legislation and the Designation Instrument in a way that makes implementation of the regime as easy as possible from a technical perspective. It is expected that ACCC will issue a further draft of the Rules once the legislation passes through Parliament.
- The Interim Chair of the Data Standards Body invited 15 representatives from across the CDR ecosystem to form an Advisory Committee in July 2018 which has met every month since then to provide strategic input for the Interim Chair and the CDS team to consider as it develops the standards. This has provided very productive discussions of key issues that need to be addressed in the standards. For 2019-20 the Advisory Committee membership is focussed on Banking. Separate Advisory Committees will be established as additional sectors are designated by the Government.
- The CDS program comprises four working group streams:
    - **API Standards:** drafting and validating API specifications;
    - **Information Security:** defining the information security profile supporting the API specifications, and authorisation and authentication flows;
    - **Consumer Experience (CX):** providing best practice language and user experience (UX) design patterns to request consumer consent and guide authentication and authorisation flows; and
    - **Engineering:** focuses on demonstrating the API Standards through the delivery of usable software artefacts that assist ecosystem participants demonstrate conformance with the standards and rules for CDR.
- All the work streams are open for public and industry participation. Interested participants can join the groups and mailing lists at: https://consumerdatastandards.org.au/workinggroups/
- The work streams have used a combination of GitHub updates, teleconferences, workshops, bilateral conversations and email circulation of draft outputs to engage with stakeholders in the banking, FinTech, software vendor, consumer and regulatory communities throughout the process.

The Working Drafts

The Interim Data Standards Body released its first overarching draft of the API specifications on 2 November, 2018, which was updated with further releases issued on 20 December, 2018 and 31 May, 2019.

This current draft released on **17 July, 2019** addresses all the outstanding issues in this full draft of the CDS expected to be implemented for the proposed pilot testing phase. This consolidates the feedback received on the May 2019 draft from 13 respondents across 28 different issues. 55% of these issues were seen as technical corrections to the standards and have been automatically incorporated into the standards. The remainder, including the 4 major matters identified in the May update, have been reviewed in detail by the CDS team, and subsequently with the Advisory Committee, to provide the Chair with a detailed understanding of the issues prior to making his final decisions, which are documented in this current update.

All issues raised with, and the submissions received regarding the May 2019 release of the CDS, have been openly published on GitHub (in line with previous releases). The on-going consultation with CDR ecosystem participants has provided the basis for the changes described in this July 2019 release, and our consultative approach will continue as we move to full implementation.

Over the past 12 months we have received in excess of 300 interactions from the community across approximately 100 individual contributors via GitHub and through written submissions. In addition, we have connected with more than 500 interested parties through a series of workshops held in Sydney and Melbourne. Over 900 people follow our development work through our regular mailing lists and blogs. The community has provided valuable input to the ongoing development of the standards.

As with the previous drafts, the July 2019 draft is aligned to the rules as released and will be assessed further when the registry design specifications are finalised and published by ACCC. As the rules are updated subsequent to the passage of legislation through Parliament, the DSB will similarly review and update the standards as required.

What's included in the July 2019 draft

Since the 20 December release, work across every work stream has accelerated. We are excited to be bringing together:

- **Draft API Standards (July 2019 version)** - incorporating feedback from the 31 May draft, the latest API Standards can be accessed via this link:
    - https://consumerdatastandardsaustralia.github.io/standards/#standards
- **Draft Information Security Profile** - similarly incorporating feedback from the 31 May release and alignment to the updated Rules released by the ACCC. As part of this publication the Information Security profile has been reviewed by our internal security team and by independent security advisors (see below) to assess the ability of the profile to support a safe implementation of the standards for the CDR regime in its initial implementation.

The DSB's position on the specific issues where additional consultation was sought following the May 2019 release have now been clarified, and the latest security profile includes the decisions made that will be utilised for the pilot testing phase.

The latest draft of the information security profile can be accessed via this link:

  - https://consumerdatastandardsaustralia.github.io/standards/#security-profile

- **Independent Security Review** – the Information Security profile and the intersection with the API standards has been independently reviewed by information security specialists Fortian Pty Ltd. The conclusion reached is that the current Information Security profile is suitable for use in the initial implementation of CDR. The report notes further matters that could be considered for incorporation in subsequent versions of the standards. A full copy of this report can be accessed via this link:
  - https://consumerdatastandards.org.au/resources/reports/reports-information-security/
- **A draft of the CX Guidelines to be utilised in conjunction with the standards.**
  - https://consumerdatastandards.org.au/wp-content/uploads/2019/07/CX_Guidelines_v0.9.5.pdf
- **The final Phase Two CX reports undertaken by the CDS team and four consultancies.** Phase Two built on Phase One research and design activities and has helped inform the CX Consent Flow Guidelines.
  - https://consumerdatastandards.org.au/resources/reports/reports-cx/phase-2-cx-reports/
- **A status summary of the of the Engineering workstream.**
  - https://consumerdatastandards.org.au/workinggroups/engineering/
- **A copy of the Data Sets map.** The Data Sets map included in previous versions of the draft standards to make it easier for non-developer readers to appreciate how the data standards address different issues has been now included as a separate document on the website and can be accessed at:
  - https://consumerdatastandards.org.au/wp-content/uploads/2019/07/Data-Sets-Map.pdf

The above artefacts form the updated draft of the standards and will be the basis for the proposed Pilot Trial Phase of the CDR regime to be conducted by the banks in conjunction with ACCC prior to a live release of consumer data.

Consideration of new issues and improvements will continue to be discussed across the Data Standards Body community forums and utilised to build consensus for subsequent versions of the standards.

A key focus for the CDS team for the remainder of 2019 is to ensure the draft standards are implementable and, with experience from the testing phase, to ensure they deliver the consistency and quality of data transfers envisaged by the Government. Once this testing is completed and the legislation is enacted, the standards will be finalised as Version 1 to support the live introduction of the regime in early 2020.

API Standards and Information Security Profile

The API standards currently identify the required Banking endpoints and the expected payloads which are provided in response. This July 2019 update incorporates a range of feedback from stakeholders and the submissions for both the API Standards and Information Security Profile. This feedback has been summarised and is accessible via GitHub. The summary of all feedback received on the May 2019 version of the standards is summarised in the link below:

https://github.com/ConsumerDataStandardsAustralia/standards/files/3388294/Draft.Standards.Feedback.Summary.-.v0.9.3.May.2019.pdf

The feedback provided below references the identifying references used in the above-mentioned document (e.g. Feedback ID A05, relates to Issue A05).

Key Matters identified in the May 2019 Update for further feedback

In response to the feedback received, the July 2019 draft now includes decisions taken by the DSB Chair on the key matters identified in the May 2019 update and for which additional feedback was requested:

- A decision on the Authorisation Flow (Feedback ID I01)
- A decision on the Re-Authorisation Flow (Feedback ID I02)
- A decision on the Consent API (Feedback ID I03)
- An update on ACCC's design decision on Client Registration (Feedback ID I05)

Authorisation Flow

The May 2019 draft of the standards evaluated five options for the authorisation flow and the Chair of the DSB has determined that:

- A single, consistent, authorisation flow will be adopted by the CDR regime;
- **Redirect with one-time password** will be the flow to be incorporated into version 1 of the standards; and,
- Client Initiated Backchannel Authentication (CIBA) be actively considered for addition to the regime at a later date if it becomes more widely implementable.

Re-Authorisation Flow

There have been a number of submissions suggesting it would be appropriate to have a simple, light-weight means of enabling consumers to extend or broaden the scope of previously provided approval to Approved Data Recipients.

After considering the submissions, reviewing the CX reports and holding further discussion with OAIC it is clear that consumer confusion is still prevalent around the use of dashboards and the re-authorisation process. On this basis, the DSB has determined that for version 1 of the CDR implementation:

- A full re-authorisation flow will be required for any extensions of approval.

Further CX work is encouraged to identify ways in which re-authorisation flows can be simplified without detracting from the clarity of consent for consumers.

Consent API

The manner in which the CDR regime is to capture and transmit the consumer's clear, explicit and informed consent has been the subject of extensive consultation over a number of iterations.

While CX research and consultation have indicated that fine-grained consent offers a potential benefit for future versions of the CDR regime, it is currently not fully understood by consumers. Further, the ACCC rules do not currently require granular consent and therefore other, non-banking sectors of the regime should be further consulted as to the manner in which a fine-grained consent might be implemented by the standards.

After significant deliberation with the community, the Chair of the DSB has determined that for version 1 of the CDR implementation:

- The use of scopes and optional claim for sharing duration will be retained in the standards; and,
- A mandatory consent API will not be included in the first version of the standards.

Design options for the handling of fine-grained consent will continue to be reviewed with a decision, guided by more CX research and made in consultation with CDR participants, expected to guide the implementation of a subsequent version of the CDR standards released around July, 2020.

Static v Dynamic Client Registration

Since publishing the May Update the ACCC has confirmed that for version 1 of the CDR implementation of the Registry will be designed around static client registration.

The draft standards and Information Security profile had been previously updated to reflect this position and have now been further reviewed to ensure there is consistency with this decision by ACCC.

Resolution of Other Matters

The feedback on the May 2019 update re-stated a number of matters which had previously been raised in GitHub and decisions reached. The following lists those restated matters which were revisited by the CDS team with the Advisory Committee and the community to arrive at the current DSB determination for the version 1 CDR implementation:

1. Product Bundles (Feedback ID A05)
   The decision has been taken to retain the current, limited representation of bundles, with clarification provided in the standards as to the intended level of detail to be provided. More comprehensive details and endpoints for product bundles will be developed with the ecosystem participants for an early implementation in 2020.

2. Pending Transactions (Feedback ID A06)
   The decision was taken to retain pending transactions to ensure the CDR regime was a viable replacement for screen scraping. Explicit limitations of the inclusion of pending transactions will be further elaborated in the standards.

3. Transactions Search (Feedback ID A07)
   The decision was taken to retain the transactions search query parameter in the standards however it will be made optional for implementation.

4. Pagination (Feedback ID A08)
   The decision was taken to retain the current mechanism for obtaining transaction information as it offers the greatest flexibility.

5. Bulk Transaction Data (Feedback ID A09)
   The decision was taken to retain the bulk transaction end point in the standards however it will be made optional for implementation. It was agreed an adjustment will be made to the corresponding NFR's to the limitation on daily calls to enable Data Recipients to gain appropriate access to data approved by consumers.

6. Personally Identifiable Information (PII) Data (Feedback ID A12)
   The decision was taken to maintain the CDR payloads in the current version of the standard in order to comply with the current requirements of the Rules and the Designation Instrument for the Banking sector.

7. Scope/ Data Alignment (Feedback ID A15)
   The decision was taken to retain the current scope boundaries which have been aligned to the result of CX testing and so expected to result in less customer confusion.

8. Access Token TTL
   In response to the feedback provided the decision was taken that the non-functional requirements and Information Security profile will be adjusted as follows:

   - Access Token TTL will be at the discretion of the Data Holder but will be required to be in a range of 2min to 10min
   - Non-functional requirements for the number of sessions allowed for data recipients will be increased to assume a 2min TTL has been set

   It is also noted that the ability to track the impact and frequency of changes to Access Token TTL will need to be discussed and agreed so that this aspect of the regime can be monitored and understood.

Consumer Experience

Since the May update the CX Workstream has conducted a workshop on the Consent Flow, completed Phase 2 design and research activities, and developed CX Consent Flow Guidelines.

Phase Two CX

Phase 2 included 3 streams of work as follows:

Stream 1

Focus areas: Consent Flow, accessibility, preliminary investigation of joint accounts, preliminary investigation of cross sector sharing

Stream 2

Focus areas: Dashboards and revocation

Stream 3

Focus areas: Consent Flow, Authentication models, Reauthorisation, 90-day notification

We have also completed a survey for the data language standards. Phase Two engaged 121 participants and, combined with Phase 1, a total of 202 people across Australia and with diverse needs have been engaged in our CX research.

Consent Flow Workshop

The Consent Flow workshop held in June included participants from 26 organisations representing Data Holders, Data Recipients, Consumer Advocacy Groups, the OAIC, and the ACCC. The overall purpose of the workshop was to facilitate the generation of a cross-sector perspective, to identify key areas of improvement for the Consumer Data Standard program's proposed Consent Flow; and for diverse industry perspectives to collaboratively inform alternatives to those key areas. The outputs from the full-day workshop have been used to help frame and inform decisions made by the Chair of the Data Standards Body and being considered by ACCC to be included separately in the Rules.

Consolidated CX Feedback

The feedback period ending 21st June has also been comprehensively reviewed. A complete CX recommendations list has been produced based on this feedback, all other CX feedback received to date, Phase 1 and 2 CX reports, and other issues that the CX Workstream has identified. This recommendations list has been reviewed internally by Data61, OAIC, Treasury, and ACCC to develop a view of what should constitute version 1 guidance for pilot testing, post version 1 CDR issues, and next steps.

CX Guidelines

The CX Guidelines are included in this July Update. Contents of the CX Guidelines have been endorsed by the Chair of the DSB and are being further reviewed by the ACCC to determine items that may be elevated to the level of the Rules or authorised as Standards, or to sit at the level of Guidance.

Key decisions stated in the API and Information Security Profile update regarding authentication flows, reauthorisation, and fine-grained control are consistent and aligned with the CX Guidelines.

Engineering Work Stream

The Engineering work stream provides software tools/artefacts to assist ecosystem participants in demonstrating conformance with the API Standards, initially with a Product API focus. The description of these artefacts is necessarily technical in nature with the source publicly available on:

https://consumerdatastandardsaustralia.github.io/engineering/artefacts/runtime/index.html

Since the May 2019 draft was released, the Engineering stream held its second workshop on the 6th June to demonstrate the current state of the desktop sandbox and conformance tools available to the CDR community. These tools are available for download on GitHub and a comprehensive Quickstart document describing the usage of the engineering artefacts is available at:

https://consumerdatastandardsaustralia.github.io/engineering/artefacts/quickstart.html

The conformance tools currently support the syntactic checking of Product Reference Data (PRD) payloads against the banking API standard. A simple proof-of-concept PRD viewer/comparator tool has also been developed to provide a human-readable interface for the product data released by the banks on 1 July so that sit could be evaluated and reviewed for usability.

The Engineering steam will continue to update these tools in line with the evolving standards and is currently refactoring the code as we prepare to extend payload checking to encompass consumer banking data. We are also working with ACCC to determine the best use of the engineering artefacts as the development of the Register advances and the CDR regime's testing strategy is implemented.

Next steps: third quarter 2019

Each work stream is continuing to refine its work towards issuing a final version 1.0 of draft technical standards to support the first implementation of the Consumer Data Right, in the banking sector. While outstanding issues for post-Version 1.0 implementations of the technical standards are outlined under each work stream above, we believe the standards are at a point where they can be utilised and tested for usability by intending participants in the CDR regime.

The CDS team will continue work with the banks to review the outputs of the live Product Reference Data sets to ensure there is consistency of data released utilising these API-based standards.

The focus for the next phase will also be for the Data Standards Body to work with the ACCC and ecosystem participants to develop and implement a test process to ensure the standards are consistent and implementable for both Data Holders and Data Recipients.

Once the testing has been undertaken the Data Standards Body will review the results and publish a final update of the standards which are intended to become the formal version 1.0 to be implemented once the regime goes live for the banking sector.

During this phase the Engineering Working Group will aim to further develop and identify conformance tools and reference implementations for participants to ensure they are building conforming platforms.

The CX stream will hold further workshops and consultation periods on Dashboards, Revocation, and Reauthorisation to extend our guidance. The Consumer Experience Working Group will, together with ACCC and OAIC, also commence development of a further phase of CX work which provide continuing clarity to matters identified in Phase Two research, such as around dashboard management and re-authorisation of previous consumer permissions.

The Data Standards Body will also continue to work with the Energy sector in this next period to assess how best to facilitate the application of CDR for the benefit of consumers who wish to utilise their energy data for more tailored opportunities.

Providing feedback on the July 2019 draft

We're aware that the July 2019 draft covers deliverables across all four work streams, with a lot of information for organisations and individuals following our progress to digest. Some stakeholders will only be interested in certain components of the documents, depending on their area of expertise.

Feedback will continue to be received through GitHub and issues raised will form part of an on-going backlog for consideration in subsequent versions of the standards which will be updated on a regular basis to facilitate emerging technologies and innovations. For key issues identified we will also continue to hold detailed workshops to help elicit eco-system consensus and good design of future enhancements to the standards.

- **Comments and queries on the API standards:** A dedicated GitHub Issue for capturing feedback has been created here:

  https://github.com/ConsumerDataStandardsAustralia/standards/issues/79

- **Comments and queries on the information security profile:** A dedicated GitHub Issue for capturing feedback has been created here:

  https://github.com/ConsumerDataStandardsAustralia/standards/issues/79

- **Comments and queries on the CX guidelines, artefacts, findings, and recommendations can be emailed to:** CDR email address: cdr-data61@csiro.au

- **Comments and queries on the Engineering artefacts:** feedback can be provided through the existing Engineering GitHub Issues page noted here:

  https://github.com/ConsumerDataStandardsAustralia/engineering/issues/41

Where participants believe they have sensitive information to convey we will consider those discussions and give guidance on our preferred disclosure approach prior to meeting to discuss such issues. To discuss such issues please email us at the CDR email address: cdr-data61@csiro.au