Developing a Consumer Data Standard in Banking

Working Draft 0.1 2 November 2018

Foreword from the independent Chair: Mr Andrew Stevens

As independent Chair of the Data Standards body, I have been focused on ensuring the data standards designed support Australian consumers exercising their Consumer Data Right. The Data Standards Body is a core element of the Consumer Data Right regime. It will design the data sharing standards that take a right in principle for consumers and make it a right in action, enabling consumers to meaningfully, safely and securely access and share data with accredited, trusted entities – when they want to, with their consent.

It has been a fast paced, energising and constructive experience initiating discussions around a data sharing standard for the banking sector (Open Banking) over the past five months. I've been grateful to the Advisory Committee for their frank and fearless advice, and to Data61 as technical advisor helping to drive this work forward.

At the beginning of this process this program of work committed to working in the open, seeking out feedback from across the financial industry, from other sectors and community groups. Being open about draft decisions and proposals has helped the program to iterate and improve on the standard quickly. Stakeholders can respond to each other's views. And now, with the 2nd November working draft, the program is knitting together decisions and discussions had so far and reviewing its progress.

We're certain we haven't got everything right the first time. That's why we're seeking your input. Designing a standard like this – giving consumers control over data held about them in the banking sector, in ways that could extend across other sectors of the Australian economy – is a world first.

This working draft is just that: a draft. It's an opportunity to test assumptions and use the feedback that's received to get the next version right. Over the coming weeks, the program will publish all the feedback it receives and work on prioritising key issues to address for Version One, the blueprint for implementing a consumer's right to access and share data at their choosing, in the banking sector.

This is just the beginning. Technologies and societies change over time, and the standards will need to adjust too. What ends up in Version One – the version that ultimately is used as a starting point for those organisations obliged to ensure consumers can share their data – will not be the only version produced by the Data Standards Body. My goal is an entity supporting sustainable, living standards that ultimately give consumers greater choice and control over how they share data and with who.

The Data Standards Body, as a formal entity, will be created with the passage of legislation introducing the Consumer Data Right. What has inspired me so far has been the enthusiasm and interest shown across a wide community in helping us move towards a strong standard. We have learnt a great deal, which will inform how that formal Data Standards Body operates. Thank you for taking the time to respond to this draft.

The journey so far

Data61 was appointed technical advisor to the interim Data Standards Body as part of the 2018/2019 Federal Budget. Since then, a team has been established inside Data61 to deliver the Consumer Data Standards program, comprising a mix of employees and contractors with banking domain expertise.

Given legislation creating the Consumer Data Right hasn't yet been passed, Data61 has been describing its role, and the Data Standards Body, as being "interim" participants. Once a legislative regime has been established, it's anticipated that a separate entity will be established to develop and monitor technical standards, with support from Data61.

Data61's role within the broader Consumer Data Right regime is to deliver technical standards that make it simple and secure for consumers to share data held about them within key sectors with trusted third parties of their choice. The proposed Consumer Data Right is a government priority requiring close collaboration across several key agencies.

Working with Treasury, the ACCC and OAIC

The Treasury is responsible for overseeing the development of the Consumer Data Right legislation (CDR), with its design informed by the recommendations of the *Review into Open Banking in Australia – Final Report,* an independent review chaired by Mr Scott Farrell. The Australian Government committed to implementing Open Banking as part of the Consumer Data Right in its response to the review released in May 2018.

Treasury has been consulting on draft legislation implementing the Consumer Data Right regime from 15 August to 7 September and from 12 September to 12 October. It has also been developing and consulting on the designation instrument for the banking sector. Treasury has a role in providing updates and advice to the Treasurer on progress regarding implementation. It will also provide advice on future designated sectors and rules submitted by the ACCC for consent.

The Australian Competition and Consumer Commission (ACCC) is the lead regulator for the CDR regime. The ACCC's approach in designing rules supporting the CDR legislation, and shaping technical standards developed by the Data Standards Body, is focussed on the objectives of the Consumer Data Right regime to empower consumers to request data about themselves safely and conveniently and to foster competition in designated sectors. As well as developing rules defining how the CDR will be implemented, the ACCC will manage the accreditation of third parties permitted to receive data at a consumer's consent within the regime. Only accredited parties, with a consumer's consent, and consumers themselves, will be able to request data from a data holder like a bank, energy retailer or telco. The ACCC also has responsibility for a Register of Accredited Data Recipients, providing information about organisations within the CDR and their accreditation status for consumers and data holders. The ACCC will also take enforcement action to ensure compliance with the CDR, and recommend future industries/sectors to government to be designated sectors within the CDR.

The Office of the Australian Information Commissioner (OAIC) advises the Treasury and ACCC on privacy safeguards included within the CDR regime, will handle consumer complaints once the regime is in operation and take enforcement action in relation to the Privacy Safeguards.

Each of these organisations has observer status on the interim Data Standards Body's Advisory Committee, a committee of banking, fintech, consumer, telecoms, energy and software vendor representatives helping to shape the emerging standards. The Consumer Data Standards team has been working closely with the ACCC and Treasury as the legislation, standards and rules are designed in

parallel. With each decision proposal, the Consumer Data Standards team has discussed with the other government agencies issues regarding alignment, and adjusted its approach as more information about the rules and legislation in development come to light.

Collaborating with the Advisory Committee and technical community

The interim Advisory Committee has been appointed for 12 months, to guide the development of the first iteration of technical standards. Because banking is the first sector to be designated under the proposed CDR, the Advisory Committee's composition has skewed towards banking domain expertise.

The Advisory Committee works collaboratively and transparently, with minutes from each meeting being published online following a period for review and feedback among Committee members. The Advisory Committee has met monthly, with four meetings held between July – October.

The work of the Consumer Data Standards program has been split into three streams:

- API standards
- Information Security
- User Experience

All work streams have been sharing progress openly using GitHub and via in person workshops and email lists. The majority of work so far has focused on setting up the API standards workstream and beginning high level discussions around information security. To date, 33 mini decision proposals and 3 noting papers have been shared publicly in the Consumer Data Standards program GitHub repository: https://github.com/ConsumerDataStandardsAustralia/standards/issues . Open, transparent discussion regarding the standards has been encouraged among all participants. There have been:

- 44 unique contributors[1]
- 382 total comments[2]
- Average of approximately 10 comments per decision proposal/noting paper

What you read in the working draft reflects contributions and insights from that community of contributors. We want to thank those contributors for their thoughtful, detailed commentary and persistence in responding to decision proposals to typically tight timeframes.

Across work streams, the Consumer Data Standards program has also:

- Hosted an October API Working Group meet up, inviting commenters on the GitHub repository and subscribers to its API Working Group mailing list
- Delivered three workshops exploring user experience concerns and priorities and use cases to support Open Banking
- Spoken about its work at 9 conferences.

The GitHub process has been a success in capturing discussions transparently and allowing contributors to respond to each other as well as the Consumer Data Standards team. But not everyone is on GitHub; nor has the process been necessarily visible for everyone. The contributions captured have not necessarily reflected the whole community invested in the standards. From November onwards, the

[1] 'Contributors' are accounts making comments on the GitHub repository, and reflect a mix of organisational and individual accounts. This figure only includes those unique accounts making contributions: a number of accounts made contributions on behalf of a wider group of organisations.

[2] Including responses to comments by CDS team

Consumer Data Standards program will move to supplement what have been primarily online, GitHub focused discussions with more opportunities for in person workshops and teleconferences.

Our starting point: the UK standards

The Consumer Data Standards program was directed to begin with the UK Open Banking Standard both by the independent Farrell review of Open Banking in Australia and the Government's response to that Review. Because Australia is implementing a banking standard within a broader Consumer Data Right regime, intended to operate across sectors, the Consumer Data Standards program has necessarily had to diverge from the UK standard in a number of places.

Given the need to design API standards at a high level to support cross-sector implementation, early decision proposals – regarding HTTP Headers, URI structure and naming conventions – had to diverge. On feedback from the technical community, a different approach to Versioning for the standards (endpoint versioning, as compared with block versioning) was also proposed. Draft proposed payloads also vary, in some cases reasonably significantly, from the UK open banking standard payloads, given the need to make changes in response to emerging ACCC rules and to align with Australian banking services and products.

While the design of the APIs does diverge from the UK standards in some practical respects, both sets of banking standards reflect certain common principles: they're open standards to be adopted and reused; and are designed to be flexible and responsive to change. The Consumer Data Standards program is following the UK's lead on information security, adopting common information security protocols including OAuth 2.0 and OpenID Connect, closely. Information Security is too important for the program to design a bespoke implementation in a short period of time. Instead, the program has adopted globally used information security protocols that are already in some cases being used by Australian vendors and banks.

Providing feedback on the working draft

The working draft is available in as static documentation hosted on GitHub at https://consumerdatastandardsaustralia.github.io/standards/#introduction.

It is very much a working draft. We've assembled a working draft reflecting the decision proposals that have been debated within the community on GitHub so far, over three months. There will be some inconsistencies. There may be a need to revisit and revise decision proposals that have already been finalised, in order to improve the next draft of the standards.

Feedback on the working draft will be open for **three weeks,** closing 5pm on Friday 23 November. We are accepting feedback:

- via GitHub, where participants are able to upload their own commentary either on discrete issues or regarding the complete draft here: https://github.com/ConsumerDataStandardsAustralia/standards/issues/39
- via email in **Word doc** format, to cdr-data61@csiro.au.

Please note: **confidential submissions will not be accepted.** We have committed to working transparently with stakeholders across the industry. All submissions received via email will also be published online upon receipt.

Once we have digested feedback from the community, we will work towards publishing a second draft of the technical standard for the banking sector for further review by Christmas 2018.

The working draft: what's in it?

Of most importance for many respondents will be reviewing the emerging API endpoints and payloads: these dictate data that is to be provided by a data holder to an accredited third party, where they are authorised to do so by a consumer (who has given their consent to the accredited third party to access their data). A brief overview of key areas for review and directions to help stakeholders navigate to and interpret those proposals is below.

What's not included:

The working draft doesn't reflect decisions made with respect to an information security profile. It includes some high-level proposals to shape further work on authentication and authorisation, but does not comprehensively articulate information security related requirements for participants in the CDR regime. Digging into information security requirements will be a core focus for the program over the coming 3-5 weeks.

The working draft also doesn't reflect insights from the Consumer Experience work stream, which has begun reviewing the emerging API specifications with the intent to test these with Australian consumers. Data61 and Treasury are jointly commissioning user experience research examining consumer expectations of consent and control over data sharing, and insights into how they might navigate consent, authorisation and authentication within the regime. Outputs from this testing will influence how the API standards are changed.

The working draft does not reflect:

- finalised rules or legislation for the CDR. Further changes will require adjustments to the technical standards
- non-functional requirements associated with the API standards
- ongoing monitoring and testing of compliance with the standards

Key areas for review:

While some stakeholders will want to review the draft specification in detail, others will be primarily interested in choices made in the design of the APIs so far that substantively shape how a consumer can direct their data to be shared, the control they have over that data, and the ease (or difficulty) data holders and recipients experience responding to the consumer's wishes. They're technical implementations that give effect to the policy behind the Consumer Data Right.

There are some key areas that organisations interested in the overall experience and design of the API standards so far may be interested in:

- **Information to be shared ("payloads"):** This information is at the core of the Consumer Data Right and the standards. The right is designed for consumers to share granular information about themselves – like their transaction information, their direct debits list - with accredited, trusted organisations of their choice. Consumers might want independent budgeting advice, or to sense check whether they really have the best deal with their bank, or to easily switch banks without having to manually re-build payee lists and direct debits.
  A "payload" in technical terms is the information that is being shared when an API endpoint is called. So understanding what's in the draft payloads is really important for consumers consenting to sharing their information, as well as making sure that what's in those payloads meaningfully helps consumers access better products and services. They will contain sensitive information. And only a consumer can consent to sharing that information. Only accredited

parties will be able to receive that information.
The draft payloads as currently described can be found as part of the documentation here: https://consumerdatastandardsaustralia.github.io/standards/#banking-apis. They will be tested further through the user research work stream, to sense check that the information they contain can be comprehended by consumers giving consent. We're interested in understanding whether the information currently in those payloads has been defined sufficiently to support implementation; whether it has gaps; and how they could be structured to support use cases for open banking; whether there is information that isn't necessary to support use cases like product comparisons and account switching; and how they can be designed to support consumers giving consent.

- **Level of authorisation granularity:** in designing APIs, it's necessarily to consider the kind of 'authorisation granularity' that APIs will support, and when granularity is important. Authorisation granularity describes the level of specificity of information consumers will see to consent to: how detailed, or how high level, the set of options are that they are presented with. A consumer's consent drives authorisation.
  At present, the payloads are designed to support coarse-grained authorisation: consumers will be able to authorise access to sets of information, but not within those sets of information to a deeply granular level. Authorisation granularity is tricky. Too much granularity can result in too many options and bits of information for a consumer to consider. It can make certain use cases hard to implement in practice. But too little granularity and consumers can cease feel as though they're exercising meaningful control over what they're consenting to. We're interested in where granularity might be important in the payloads and for what use cases, while managing this relationship between useability and information overload. Authorisation granularity will also be tested with the user experience work stream. The draft decision made on Authorisation Granularity can be found at https://consumerdatastandardsaustralia.github.io/standards/#authorisation-scopes.
- **Authentication and Authorisation:** how consumers experience authentication and authorisation flows navigating open banking is a key user experience and information security concern. "Authentication" is the process by which as consumer proves that they are the "owner" or holder of the information that is being requested by a third party, with their bank. At the end of the authentication process, the identity of the consumer is confirmed. "Authorisation" is the process by which a bank confirms with a consumer that the request they have received for data is what the consumer had consented to. The current standards propose at a high level, a starting point for those flows. We are seeking further feedback on whether that is the right starting point, and how considerations around authentication and authorisation can support a frictionless consumer experience accessing use cases for open banking.

None of these areas reflect a standard set in stone. We want to direct organisations to these areas so that they can offer us feedback on the decisions made so far, and tell us what we may have failed to consider.

Next steps

Having digested feedback, we will work towards publishing a second draft of the technical standards, including an information security profile and emerging insights from the consumer experience workstream, by Christmas 2018.

We are also beginning to explore conformance tools and reference implementations, to support the industry implementing APIs in accordance with the technical standards. We'll share more updates about this work on the Consumer Data Standards website and on GitHub.

Stay in touch:

Join our mailing lists at https://consumerdatastandards.org.au or email cdr-data61@csiro.au.

CONTACT US

t 1300 363 400
+61 3 9545 2176
e csiroenquiries@csiro.au
w www.data61.csiro.au

FOR FURTHER INFORMATION

Terri McLachlan
t +61 2 9490 5722
e terri.mclachlan@@data61.csiro.au
w www.data61.csiro.au