The Christmas Draft: continuing towards Version 1 of an open standard for the banking sector

Working Draft 20 December 2018

In the lead up to the Christmas break, the Data61 Consumer Data Standards team has been working hard continuing to develop and refine common technical standards in support of the Australian Government's Consumer Data Right Regime. The draft standards being developed by Data61 are intended to make it easier and safer for consumers to access data held about them by businesses, and – if they choose to – share this data via application programming interfaces (APIs) with trusted, accredited third parties.

In this Christmas working draft, we're summarising the progress we've made so far, drawing attention to documents and deliverables organisations might have missed across the work streams, and summarising next steps for 2019. We know that many in the community have been monitoring the open discussions and have actively contributed to making these drafts what they are, with feedback in workshops, on GitHub, via email and in bilateral discussions. Thank you!

Mechanisms to provide feedback on the draft technical standards are outlined at the bottom of this overview. Knowing a growing number of stakeholders have already provided extensive feedback across work streams, sometimes on a weekly basis, and in response to our 2nd November working draft, we have suggested informal mechanisms to keep adding feedback in each work stream. We'll leave comments open on the draft API standards and information security profile as they are until **Friday 18 January** to give people time to return from their holidays and check back in with what we've been doing.

Now we're taking a break and we hope you do too. We'll be back in the office from 3 January 2019.

Merry Christmas!

A quick recap:

- The Consumer Data Standards program has been working in the open to create and iterate on draft technical standards since late July 2018, while Treasury and the ACCC design legislation and rules introducing the Consumer Data Right in parallel.
    - For a full summary of how the process was initiated and how technical decisions have been made, read the summary attached to our 2nd of November working draft: https://consumerdatastandards.org.au/2nd-november-working-draft/
- There are three work streams under the Consumer Data Standards program:
    - **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:** articulating best practice language and design patterns to support seeking consumer consent, and providing UX guidance on authentication and authorisation flows
- All the work streams are open work streams, with mailing lists interested participants can join: 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 2nd November Working Draft

The Consumer Data Standards program released its first overarching working draft of the API specifications on Friday 2nd November 2018. This draft knitted together the outcomes of 33 decision proposals that had been consulted on in the open via GitHub between end July 2018 - October 2018. It was an early first draft, with a range of inconsistencies and gaps to subsequently address. It didn't include a draft information security profile or planned deliverables within the Consumer Experience work stream.

35 submissions were received in response to the working draft from a combination of individual and organisational contributors. A summary of the feedback on the 2nd November Working Draft was published to GitHub here: https://github.com/ConsumerDataStandardsAustralia/standards/issues/39, and has also been re-published on the Consumer Data Standards website https://consumerdatastandards.org.au/2nd-november-working-draft/. FinTech Australia were granted an extension with a late submission, which has also been uploaded to Issue 39 on GitHub and whose feedback continues to be worked into the API specifications.

Unwrapping our Christmas working draft

Since the 2nd of November, work across every work stream has accelerated. We're excited to be bringing together:

- **Draft API Standards (v0.2.0)** incorporating feedback from the 2nd of November working draft
    - https://consumerdatastandardsaustralia.github.io/standards/#introduction
- **A draft information security profile (v0.1.0)**
    - https://consumerdatastandardsaustralia.github.io/infosec/#introduction
- **An independent review of progress so far bringing together an information security profile by expert consultancy Galexia**
    - https://consumerdatastandards.org.au/christmas-2018-working-draft/

- **A report exploring use cases and priorities for the Consumer Experience work stream, *Defining the UX of Consent,* and a draft Consumer Experience work stream roadmap,** following feedback from the CX workstream participants
    - https://consumerdatastandards.org.au/reports/

These are all works in progress. Within each work stream, there are still issues to unpack and insights to align across work streams. At the moment, the work streams can appear disjointed to external stakeholders who must review documents and drafts across separate GitHub repositories, mailing lists and documents. A key focus for the Consumer Data Standards team in 2019 is making the connections between our work streams more visible, bringing the draft standards together as one comprehensive set of documentation and continuing to refine communications in the lead up to a Version 1.0 for implementation.

What's included and what's not included in our Christmas draft

API standards

The API standards incorporate a range of feedback from stakeholders that roamed from technical commentary on the draft Swagger to questions and clarifications on the design of the documentation overall. You can read the summary of feedback that informed the latest draft of the standards here: https://consumerdatastandards.org.au/2nd-november-working-draft/.

The Christmas working draft API standard doesn't include:

- An **updated product reference payload** - feedback was sought from major banks through the Australian Banking Association as to how a product reference payload might be designed for Version 1 of the standard. That feedback, received in mid December, has yet to be incorporated into this working draft and will be a priority for inclusion in January 2019 alongside feedback from FinTech Australia.
- A draft payload for **scheduled payments -** this is the focus of discussions with the ACCC and will be included, once resolved in the ACCC Rules, in January 2019
- Detailed **non-functional requirements -** the ACCC and Data61 are working together to articulate NFRs in draft rules and standards. A preliminary draft proposal, designed to begin eliciting feedback, has been published on the Consumer Data Standards GitHub here: https://github.com/ConsumerDataStandardsAustralia/standards/issues/21
- **Insights from Consumer Experience permissions language testing -** the current scopes and arrangement of payloads may change in order to improve consumer understanding of what is contained in each payload, for them to grant consent to an accredited data recipient to access. The Consumer Experience work stream has commenced preliminary testing of the existing payload structures with a small cross-section of Australian consumers. The approach to testing and some early insights are outlined below, with a full report to follow in January 2019.

Understanding the payloads

The Consumer Data Standards program received feedback on the last draft of the API standards that critical elements of the standards, in particular the draft 'payloads' (the technical term describing the data that's accessible from each endpoint in the API standards) weren't accessible for non-technical audiences. With support from the ACCC, who have mapped requirements in the draft designation instrument outlining the proposed Consumer Data Right in banking against their own draft rules and Consumer Data Standard draft payloads, a table summarising information currently in each draft API payload is below.

Data sets map (source: ACCC)

Note:

- This table is for illustrative purposes only and should not be taken as a definitive statement of the data sets for the CDR.
- Some categories of payloads do not align precisely with the draft Designation Instrument and may be captured under multiple limbs. For example, some 'account data' is within what the Designation Instrument refers to as 'information about the user of the product'.

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
Information about user of product	'**Customer data'** is data that identifies the customer and any persons authorised to act on the consumer's account and will include, at a minimum: - the customer's name, which may include a business name and number(s) (such as ABN, ACN) - the customer's contact details, which may include phone numbers, email addresses, and physical addresses. Customer data may include other identifying information, including where that information assists to distinguish one customer from another. Customer data does not include the date of birth of an individual. In relation to business customers, customer data may include the type of business, establishment date, registration date, organisation type, country of registration and whether the business is a charitable/non-profit organisation. Customer data also includes information the customer provided at the time of opening the account that relates to the customer's eligibility for to acquire the product (that is, in connection with an application process). However this information will not be required to be shared via an API and	Basic Customer data	Get Customer*	Customer type (e.g. person or organisation) *Person*: last update time, first name, last name, middle names, prefix, suffix, occupation code, *Organisation*: last update time, agent first name, agent last name, agent role, business name, legal name, short name, ABN, ACN, industry code, organisation type (e.g. 'sole trader'), registered country, establishment date
		Detailed Customer Data	Get Customer Detail*	Customer type (e.g. person or organisation), *Person*: last update time, first name, last name, middle names, prefix, suffix, occupation code, *Organisation*: last update time, agent first name, agent last name, agent role, business name, legal name, short name, ABN, ACN, industry code, organisation type (e.g. 'sole trader'), registered country, establishment date Phone numbers (purpose and preferred number),

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	must be shared directly with the consumer in response to the consumer's valid request.			Email addresses (purpose and preferred email), Physical address (mailing name and purpose).

Information about use of the product	**'Account data'** includes, at a minimum:
	- information identifying the account, including the account number, and account name(s)
	  o credit card account numbers must be treated in accordance with any applicable laws, obligations and/or standards, which may include masking credit card numbers to meet security requirements
	- the opening and closing balances for the account, including as current balance and available funds
	  o a running balance may be shared by the data holder, but is not a mandatory inclusion
	- authorisations on the account, including:
	  o direct debit deductions, which will include, to the extent available:
	  ▪ identifying information for the merchant/party making the debit
	  ▪ the amount debited
	  ▪ the date of the transaction
	  o scheduled payments, which may include regular payments, payments to billers, international payments
	  o details of payees stored with the account, such as if entered by the customer in a payee address book.
		Basic Bank Account	Get Accounts	Account ID, display name, nickname, masked number (BSB/ACC, CC number, PAN)
				Product: category, type, name

			Get Bulk Balances	Account IDs, Balance: type (e.g. 'deposits'), amount (current and available), currency
			Get Balances For Specific Accounts	Account IDs, Balance: type (e.g. 'deposits'), amount (current and available), currency
			Get Payees	PayeeID, nickname, description, type (e.g. domestic, international biller)
		Detailed Bank Account	Get Account Detail	Account ID, display name, nickname, account number (BSB/ACC, CC number, PAN) Product: category, type Balance: type (e.g. 'deposits'), amount (current and available), currency Features (type and information) Fees: name, type, amount, Discounts: description, type, amount, conditions

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	The ACCC recognises the limitations in providing direct debit information, hence the information is to be provided to the extent available. The ACCC expects though that as more information becomes available, and better processes develop, over time in relation to direct debits, it will be able to be included.			Deposit rate, lending rate, address, bundle details (i.e. details of other linked accounts)
			Get Direct Debits For Account	Direct debit authorisations: account ID, authorised entity (name, financial institution, ABN, ACN), last debit date and time, last debit amount
			Get Bulk Direct Debits	List of direct debit authorisations Direct debit authorisations: account ID, authorised entity (name, financial institution, ABN, ACN), last debit date and time, last debit amount
			Get Direct Debits For Specific Accounts	Account ID Authorised entity information [Name, Financial institution, ABN, CAN, Last debit time, Last debit amount]
		Bank Payee	Get Payee Detail	PayeeID, nickname, description, type (domestic, international, biller) *Domestic*: account (name, BSB, account number), Card (card number), PayID (name, identifier, type-mobile, email, organisation name) *International*: (beneficiary name/country/message, bank country/account number/address/name, Beneficiary Bank BIC/fed wire number/sort code/ chip number/ routing number) *Biller*: code, name

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads

	'**Transaction data**' includes, at a minimum:
	- the date on which the transaction occurred
	- the relevant identifier for the counter-party to a transaction
	  o where the counter-party is a merchant, this will include information the merchant has provided as a mandatory inclusion, and any additional merchant identifiers the data holder may have added as an optional inclusion
	- the amount debited or credited pursuant to a transaction
	- any description of the transaction
	- the 'simple categorisation' of the transaction (e.g., whether the transaction is debit, credit, fee, interest etc.)
	  o any additional, descriptive categorisation of the transaction added by the data holder (e.g., 'transport', 'health', 'entertainment' etc.) is not a mandatory inclusion but may be included.
		Bank Transactions Data	Get Transactions For Account	Account ID, display name, nickname, list of transactions (transaction ID, status, description, post time, execution time, amount, currency], reference number from merchant)

			Get Transaction Detail	Account ID, display name, nickname, list of transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant), payer, payee, extended description
			Get Bulk Transactions	Account ID, list of transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant),
			Get Transactions For Specific Accounts	Account ID, transactions (transaction ID, status, description, post time, execution time, amount, currency, reference number from merchant),
Information about a product	'**Product data**' includes product reference (generic) data, which includes, at a minimum, data on: - product type - product name - product prices, including fees, charges, interest rates etc (however described)	Public data	Get Products	Products ID, effective from and to, last updated, product category, product name, description, brand, application URI, overview URI, terms URI, eligibility URI, fees and pricing URI, bundle URI

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	- features and benefits, including discounts, bundles etc (however described) - terms and conditions - customer eligibility requirements.		Get Product Detail	Products ID, effective from and to, last updated, product category, product name, description, brand, application URI, overview URI, Eligibility (eligibility URI, type and additional information) Fees and Pricing (fees and pricing URI, name, type, amount, balance rate, transaction rate, currency, additional info, discounts) Bundle (bundle URI, name, description, additional information URI, product IDs) Features (type and additional information) Constraints (type and additional information) Deposit rate (type, additional info) Lending rates (type additional info) Repayment type (interest only, principal and interest, negotiable)
	'**Product data**' includes consumer product data, that is product data that relates to an account(s) held by a consumer and includes, at a minimum, data on: - product type - product name - product prices, including fees, charges, interest rates etc (however described) o interest rates will include the current applicable interest rate, as well as any other interest rates applicable to the product, and any terms and conditions associated with those interest rates	Detailed Bank Account	Get Account Detail	Account ID, display name, nickname, masked number (BSB/ACC, CC number, PAN), product category, product type (term deposit, credit card, loan), bundle name, balance type, balance, features, fees (name, type, amount, balance rate, transaction rate, currency, additional information, discounts), discounts (description, type, amount, additional info), deposit rate, lending rate, address, bundle details (i.e. details of other linked accounts)

Designation instrument	Rules	Standards – Authorisation scopes	Standards – APIs	Payloads
	○ these will include details of any prices etc negotiated individually with the consumer - features and benefits, including discounts, bundles etc (however described), including details of any features and benefits negotiated with the customer - terms and conditions - customer eligibility requirements.			

Consumer Experience

Testing the structure and description of draft payloads with consumers

In parallel with development of the API standards, the Consumer Experience work stream has begun conducting research with consumers to explore mechanisms that give effect to ACCC rules regarding 'informed' and 'explicit' consent. It is investigating how consumers interpret and interact with data clusters within scope for the API standards, designing consumer-facing permissions language and a consent model.

The CX work stream is currently exploring how scopes and payloads translate into permissions language consumers will be exposed to, as part of providing consent to accredited data recipients to request that data from data holders. This testing is part of Phase One of research proposed in the Consumer Experience Roadmap (https://consumerdatastandards.org.au/reports/) exploring comprehension of consent patterns and permissions language; understanding consumer expectations around how data will be shared and used, including how data is clustered and the level of granularity; and what data participants are and are not comfortable sharing.

Phase One of the research, due to be completed by close of January 2019, involves a mix of qualitative and quantitative testing with 80 individuals, across three testing phases. The first phase, a qualitative card sorting exercise and in depth interview with 10 participants (of the 80 participants total), has just been completed. The participants chosen were weighted to include at least 50% vulnerable participants, with an even mix of male and female, and single banked and multi-banked participants interviewed. Other characteristics of participants in the interview and card sorting exercise included:

- **Age**
  - 18 - 34 (1)
  - 35 - 50 (2)
  - 51 - 65 (6)
  - 65+ (0)
- **Income**
  - Low (under $37,000 per year) (6)
  - Medium (between $37,000 and $87,000) (1)
  - High (over $87,000) (2)
- **Financial distress**
  - Yes (4)
  - No (6)
- **Disability**
  - Hearing impairment (1)
  - Visual impairment (1)
  - Speech / auditory impairment (1)

Further characteristics of the participants interviewed for the initial card sorting exercise will be included in a final report. This research is being conducted with a small number of people, in up to 2 hour sessions each, to facilitate the generation of in-depth qualitative insights in naturalistic settings. This approach allows new insights, themes, connections, and hypotheses to be generated due to the exploratory and in-depth nature of the research. These findings can then be tested at scale with a quantitative study, where we can also test what we already know, or assumptions and hypotheses we currently have, in a shorter period of time and with a larger number of people. While the research has yet to be completed, some emerging themes so far that may necessitate further iteration of technical draft scopes and payloads include:

- The logic of some groupings of information within scopes and payloads needs to be clearer: participants distinguished between ingoing and outgoing transactions; account and product information; business information; and when and how personal contact information was included
- How and when mailing address is included in a data cluster for consumers to consent to needs careful consideration and communication
- In some instances, information repeated across data clusters added to confusion for consumers
- Finding terms to describe the information being shared that does not presume a level of financial literacy requires further work.

Two phases of further testing of data clusters and language used to describe the information a consumer might consent to sharing are still to be undertaken in January. Insights from the full Phase One testing will be published in February 2019 and will include: recommendations regarding language accredited data recipients and data holders should use as part of their consent and authorisation screens, as well as proposed changes to the draft API standards.

Information security

A comprehensive draft information security profile has been developed over November - December 2018, in consultation with stakeholders via workshops, email and on GitHub. An independent review of this process and assessment of outstanding issues has been provided by expert consultancy Galexia, and published online alongside this summary.

Overall, Galexia concluded that the development of the CDS Security Profile has reached a stage where:

1. There is a general consensus amongst stakeholders on the core content of the Security Profile;
2. The text of the Security Profile is sufficiently clear and focussed;
3. The Security Profile is broadly aligned with international developments, and where it does diverge this is made clear to participants; and
4. The Security Profile is appropriate for implementation in the banking sector, and the underlying principles will be useful for refining the Security Profile for use in other sectors in the future.

In their review, Galexia noted a number of issues that have been deferred to future versions of the Information Security profile, including:

- **Levels of Assurance (LoAs) and Vectors of Trust (VoT):** while innovative and emerging approaches to authentication, including Vectors of Trust, stakeholders raised concerns about Vectors of Trust being included at this early stage. The concept has been introduced in this working draft, to enable the use of VoT in future, but has not been mandated.
- **Customisation or amendment of the security profile to accommodate future sectors outside the banking sector**

The draft information security profile does not include:

- A mandate with respect to two factor authentication (2FA) of account holders by banks. This will be consulted on further in January 2019
- Alignment with the Register of Accredited Data Recipients being developed by the ACCC. As the Register is developed, it will be aligned with the information security profile.
- A consent model, integrating insights from the CX workstream with authentication and authorisation flows and mechanisms to ensure the technical fulfilment of consent.

Next steps: first quarter 2019

Each work stream is rapidly progressing towards version 1.0 of draft technical standards to support the implementation of the Consumer Data Right in the banking sector. While outstanding issues for Version 1.0 of the technical standards are outlined under each work stream above, there are certain cross-cutting priorities that will become a key focus in 2019:

- **Designing a consent model** providing technical support for the dimensions of consent, authentication and authorisation envisaged in draft ACCC rules. While there are both policy and technical challenges associated with consent, the focus of the Consumer Data Standards program will be on technical and functional requirements of consent its standards should support (e.g. testing and facilitating granular levels of consent; time-based dimensions of consent; consent revocation; front end permissions language).
- **Publishing an implementation support plan** for assisting accredited data recipients and data holders building and testing their own implementations. The Consumer Data Standards Program is developing proposals regarding conformance tools and reference implementations for stakeholders, and will seek feedback from the technical community on its proposed approach in January 2019.
- **Pulling our documentation, guidance and history of contributions to the technical standards** into one forum for easier access by stakeholders

Providing feedback on the Christmas working draft

We're aware that this Christmas working draft covers deliverables across all three 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.

To try to reduce feedback overload for contributors, we've proposed focusing feedback within each work stream. We'll keep these drafts open until **Friday 18 January** to give people time to return from their holidays and check back in with what we've been doing.

- **Comments and queries on the API standards:** A dedicated GitHub Issue for capturing feedback has been created here: https://github.com/ConsumerDataStandardsAustralia/standards/issues/44
- **Comments and queries on the information security profile:** A dedicated GitHub Issue for capturing feedback has been created here: https://github.com/ConsumerDataStandardsAustralia/infosec/issues/45
- **Comments and queries on the CX Roadmap or *Defining the UX of Consent* report:** please email Michael Palmyre (michael.palmyre@data61.csiro.au) with feedback and questions on the draft Roadmap or *Defining the UX of Consent* report.

You can also submit feedback via email to cdr-data61@csiro.au. Please specify in your email **which work stream or streams your feedback relates to.** In line with our normal policy all submissions received via email will be published openly online. The Consumer Data Standards program will not accept confidential submissions.

For further information or any questions, please email cdr-data61@csiro.au.

Watch this space in 2019 for more standards updates, and have a safe and happy holiday.

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