galexia

Data 61

Consumer Data Standards – Security Profile (CDS-SP)

Galexia Review

19 December 2018 (v2)

Contact: Galexia
S2, Level 11, 175 Pitt St, Sydney NSW 2000
Ph: +61 2 9660 1111
www.galexia.com
Project Email: data61cds@galexia.com

Document Control

Client

This report has been written for Data61.

Document Purpose

This report provides an overview of the development of the Consumer Data Standards (CDS) Security Profile (SP) as at 19 December 2018 (4:30pm).

Document Identification

Document title	Data61 – Consumer Data Standards Security Profile (CDS-SP) – Galexia Review

Client Details

Client Contacts	**Data61** Consumer Data Standards <https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standard> <https://github.com/ConsumerDataStandardsAustralia/infosec> **Ellen Broad** (Head of Technical Delivery for Consumer Data Standards) Email: Ellen.Broad@data61.csiro.au

Consultant Details

Galexia Contact	**Peter van Dijk** (Managing Director) **Galexia** <www.galexia.com> S2, Level 11, 175 Pitt St, Sydney NSW 2000, Australia Phone: +612 9660 1111 Email: manage@galexia.com Mobile: +61 419 351 374 (Peter van Dijk)
Reference	GAL563
Project team email	data61cds@galexia.com

Document Revisions

#	Date	Author	Comments
v1	13-19 Dec 2019	Galexia & D61	Internal working version
v2	19 Dec 2019	Galexia	Comment version released to client

Contents

1. Executive Summary

This report provides an overview of the development of the Consumer Data Standards (CDS) Security Profile (SP) as at 19 December 2018 (4:30pm).

The Consumer Data Standards program, facilitated by Data61, falls within the Government's proposed Consumer Data Right regime. Galexia was engaged by Data61 to provide some independent analysis and oversight of the development of the Profile. The report examines the background, development process, issues raised and outcomes.

Galexia also provided direct contributions to Data61 in the drafting of the Security Profile and this report does not repeat all of those detailed inputs.

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.

Galexia and Data61 have discussed additional issues that may require future work or referral to other CDS work-streams. These include:

1. Stakeholders, Galexia and Data61 were all concerned about the interaction of consent requirements and security in the CDS environment, and this will need to be addressed in other work-streams. Data61 has advised that these requirements will be addressed across the entire program from January 2019 as part of the development of Version 1 of the Draft Standards;
2. Approaches to authentication of consumers may require further updating and innovation, as it is too soon to mandate new approaches (such as Vectors of Trust) in the current Security Profile. However, the concept has been introduced in the current draft of the Security Profile and may be further refined in future versions;
3. Greater integration with other initiatives in the general authentication space may be required. At this stage some key initiatives such as the Australian Government Trusted Digital Identity Framework (TDIF[1]) are still draft, so further collaboration, leadership and work on this issue will be required in the near future.

The report concludes with a brief discussion of project risks, including a recommendation for the development of a Risk Management Framework. This approach is necessary for projects where new technology and business processes are being rapidly introduced in an environment with significant security risks.

[1] <https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework>

2. Context

This section describes the context in which the Security Profile has been developed.

The Australian government is introducing a Consumer Data Right (CDR), designed to give consumers greater control over their data. Part of this right requires the creation of common technical standards – the Consumer Data Standards (CDS) – that 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.

Australia's major banks have been tasked with implementing an open banking standard by 1 July 2019. All other banks will need to comply with these standards by 1 July 2020.

One important component of these standards is the Consumer Data Standards Security Profile (CDS-SP).

2.1. Roles

There are four key institutions involved in the development of the Consumer Data Standards Security Profile (CDS-SP).

1. The **Treasury** will oversee the development of the Consumer Data Right (CDR) legislation, with its design informed by the recommendations of the Open Banking Review and adopted by the Government.
2. The **Australian Competition and Consumer Commission (ACCC)** will be the lead regulator for the CDR regime, responsible for developing the Rules, accrediting Data Recipients and managing the Register.
3. The **Office of the Australian Information Commissioner** (OAIC) will work with the ACCC and Treasury to establish privacy safeguards for the CDR regime.
4. **Data61** has been appointed as technical advisor to the interim Data Standards Body and, starting in the banking sector, is tasked with delivering open technical standards that empower consumers to share their data simply and safely with organisations of their choosing.

2.2. Structure

The legislative framework for the CDR is set out in the *Competition and Consumer Act 2010 (Cth*) (CCA) through the proposed legislative framework in the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*.

Under the legislative framework, the Australian Competition and Consumer Commission (ACCC) will develop rules to govern the application of the CDR, both in particular sectors and across the economy more generally.

The Consumer Data Standards program is being supported under three streams:

- **API Standards:** drafting and validating the Application Programming Interface (API) standards being developed.
- **Information Security**: defining the CDS Security Profile supporting the standards and authorisation and authentication flows.
- **Consumer Experience:** development of best practice language and design patterns for consumer consent and user experience.

2.3. Implementation phases

The CDR Security Profile (CDR-SP) is being developed in an agile manner over a series of sprints culminating in the publication of an initial version (v0.1) on 21 December 2018.

The sprint cadence was:

- Sprint 0: 19 November – 27 November (release v0.0.1)
- Sprint 1: 28 November – 7 December (release v0.0.2)
- Sprint 2: 10 December – 18 December (release v0.0.3)
- Sprint 3: 19 December – 21 December (release v0.1)

Data61 have forecast a 3 year work program to further refine the CDR-SP and extend its application from the banking sector to other sectors of the economy (e.g. energy and telecommunications).

3. Development of the Security Profile

This section describes the development of the Security Profile to date, including commentary on the degree of maturity and consensus that has been achieved.

3.1. Development process

The CDS-SP development process comprised:

1. A GitHub repository open to the banking community and other relevant organisations, allowing interactive updates and comments on draft versions of the Security profile, and the raising and closure of issues and proposals <https://github.com/ConsumerDataStandardsAustralia/infosec>;
2. Two community workshops held in Sydney (16 November) and Melbourne (6 December), attended by about 25 participants (each workshop). These workshops included expert presentations and open discussion. The Melbourne Workshop was complemented by a follow-up Webex debrief for people who could not attend;
3. A weekly newsletter distributed to over 260 stakeholders, with a solid spectrum of industry participants and greater than 50% read rates; and
4. Four weekly telephone conferences with the Australian Bankers Association (ABA) and its members led by Data61.

GitHub Repository

As stated above the Profile was developed in an iterative fashion: four versions were produced with the final (v0.1) to be published on 21 December 2018. Each version was published in the GitHub repository and reflected the changes made based on community feedback on the preceding version.

Within GitHub issues were categorised as follows:

- **feature**: is a piece of work that represents a change to be made to the profile and which will be moved into a sprint when it is being actioned.
- **question**: is a question that the team is posing back to the community and is open for discussion.
- **bug**: relates to a bug in the profile that needs to be fixed. For example, a spelling mistake.
- **proposal**: represents an intent to change the profile based on feedback or requirements and is open for discussion.

A new label (**Rules**) was introduced in Sprint 2 to reflect the fact that a number of issues relating directly to the ACCC Rules rather than the Profile.

The development team addressed:

- Closed Issues in Sprint 1
  - 2 Bugs
  - 3 feedback items
  - 8 features
- Open Issues in Sprint 2
  - 5 feedback items – 3 of which have been determined to be issues relating principally to the ACCC Rules rather than the Profile
  - 1 proposal
  - 1 question

Within the GitHub repository a relatively small number of community members were present and active.

As at 19 December there were 25 "Watchers"[2] and 7 "Stargazers"[3] on the Security Profile comprising representatives from Data61, Galexia, the ABA, the broader banking community, vendor representatives and independent technical experts.

From an activity perspective the majority of feedback and discussion originated with a very small number of individuals (3) and organisations (2).

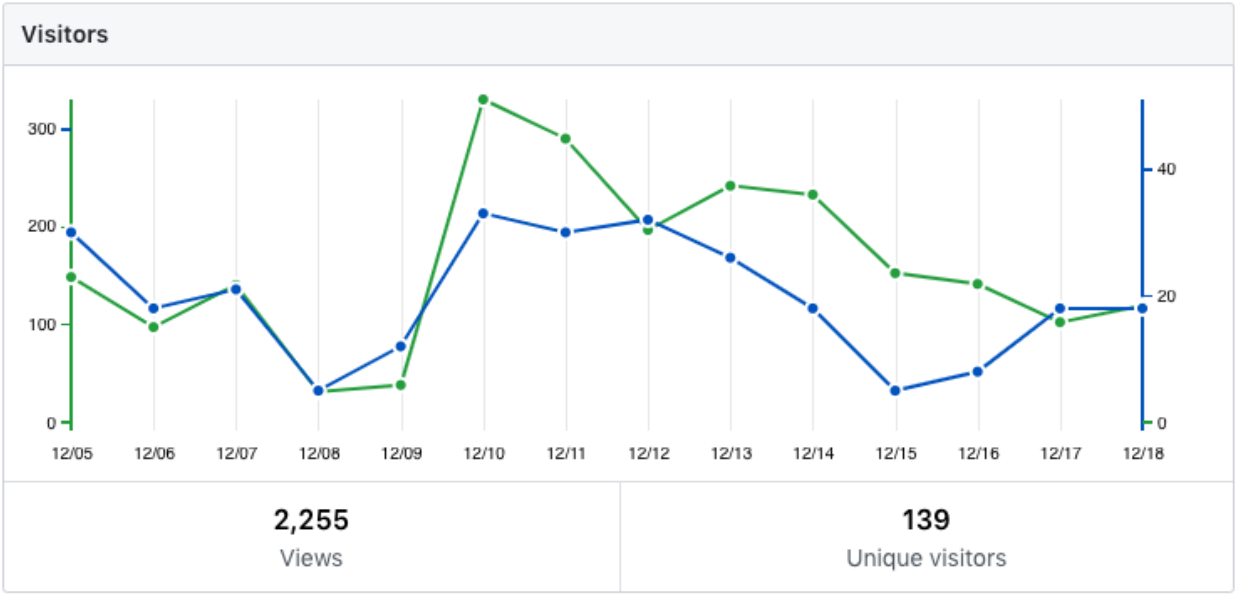

Figure: Visitors and views to the CDS-SP GitHub (showing peaks around releases of draft profiles)

Workshops

The two Workshops were well attended. There were around 30 attendees at the Sydney Workshop and 25 attendees at the Melbourne workshop due to size constraints at the venue. The Webex debrief on 10 December was well attended (**with 76 participants on the call**)

The ABA weekly teleconferences were also well attended with representatives of the majority of the ABA membership on the call. While well attended, comments and questions originated from only a small proportion of the members.

The majority of feedback and discussion within the GitHub repository originated from a small number of individuals (3) and organisations (2). In response to requests from the Advisory Committee for managing potentially sensitive material, the work stream also accepted correspondence via email.

[2] <https://github.com/ConsumerDataStandardsAustralia/infosec/watchers>
[3] <https://github.com/ConsumerDataStandardsAustralia/infosec/stargazers>

3.2. Consensus

Overall, Galexia believes that general consensus is possible on the Security Profile. Each version of the Security Profile has addressed issues and concerns raised by stakeholders in prior versions. Data61 continues to work on addressing a small number of outstanding issues. Feedback on the Security Profile is now turning to minor changes, or issues that are more relevant for other work streams (e.g. technical issues around consent that are likely to be required in the ACCC Rules or in the Consumer Experience work stream).

In addition, Galexia and Data61 have worked through a number of technical issues in the draft Security Profile and have agreed changes that will make the final version more focussed and succinct. The current version of the Security Profile also clarifies which sections are mandatory requirements and which sections are for information and guidance.

There does not appear to be significant areas of heated disagreement at this stage.

4. Issues

This section discusses the issues raised in the development of the Security Profile, including issues raised by stakeholders, Data61 and Galexia, and progress on addressing these issues.

4.1. Issues raised by Stakeholders

Stakeholders raised a number of issues via GitHub, email or during meetings. Stakeholder issues that were raised by email or in meetings were added to GitHub by Data61 where they were likely to have a direct impact on the development of the Security Profile, or where the issue needed to be captured so that it could be referred to other work-streams.

A full table of Issues appears below at 4.6. Summary GitHub Issues Table

4.2. Issues raised by Galexia

Galexia raised a range of issues relating to v0.0.3 of the Security Profile in writing and during a workshop with Data61. Many of the issues were minor changes to wording or minor technical changes, but some issues were more significant. The following table summarises the key issues raised by Galexia:

Galexia Issue Number	Issue	Data61 Response
G4	Recommended changes to some terminology for consistency with the Australian legal environment – e.g. use of Personal Information (to align with the term used in the Privacy Act) rather than Personally Identifiable Information (PII).	This change has been incorporated in the latest version of the Security Profile.
G14, G18, G19	Recommended caution over the inclusion of Vectors of Trust at this early stage – softening of language and clarity over support for VoT without mandating its implementation.	This change has been incorporated in the latest version of the Security Profile.
G8	Recommended improved clarity over the entities who need to be accredited, to align with ACCC Rules.	This change has been incorporated in the latest version of the Security Profile.
G16, G17	Recommended clarification of the interaction between the Level of Assurance (LoA) requirements and the Australian Government Trusted Digital Identity Framework (TDIF) – which is still draft.	The text that was causing this confusion has been removed from the latest version of the Security Profile.

4.3. Resolved

The majority of issues have been resolved.

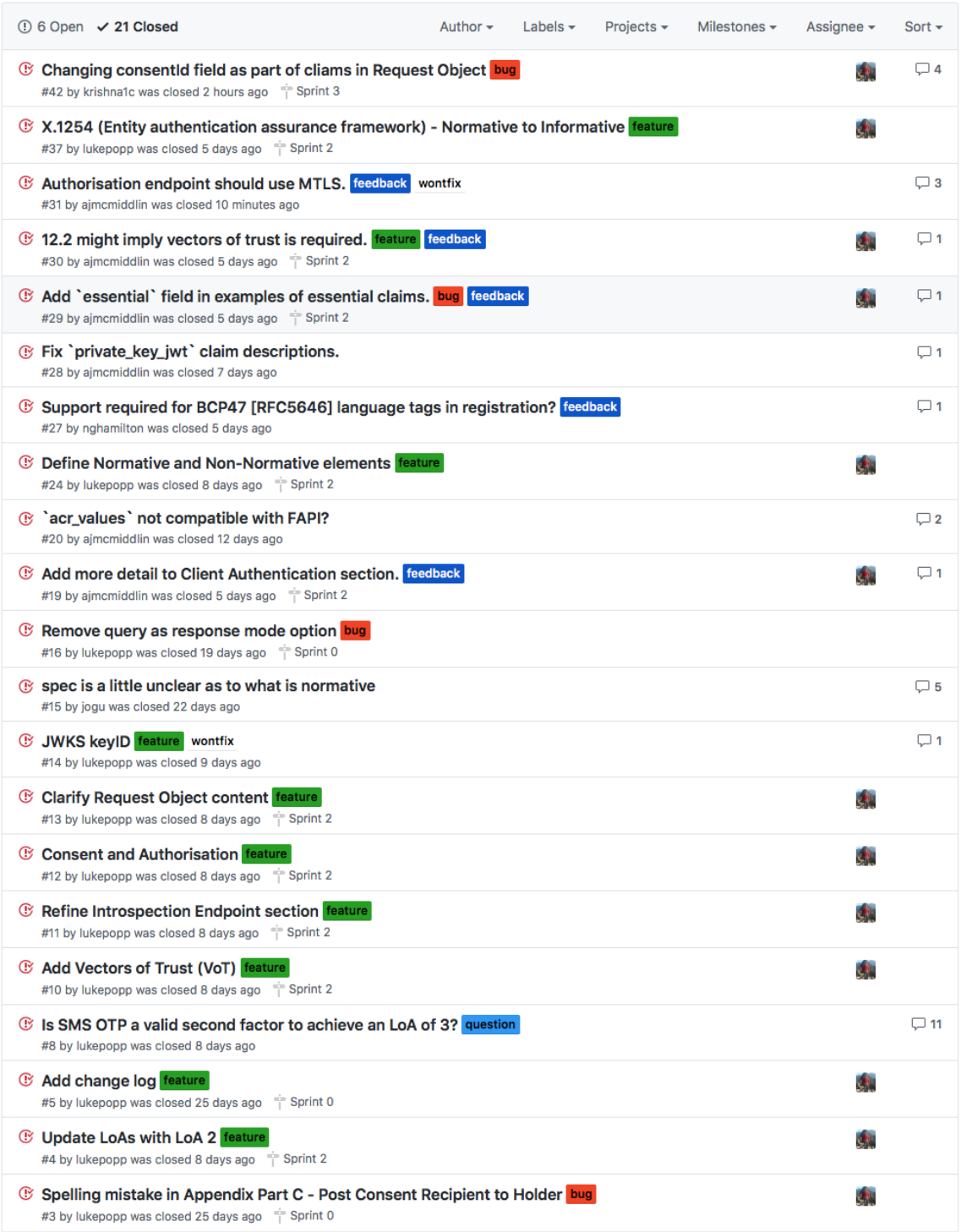

Figure: Closed GitHub Issues – as at 19 Dec 2018 (4:30pm)
<https://github.com/ConsumerDataStandardsAustralia/infosec/issues?q=is%3Aissue+is%3Aclosed>

The latest version of the Security Profile is available at:
<https://github.com/ConsumerDataStandardsAustralia/infosec/blob/master/slate/source/index.html.md>

All notable changes to the profile are published in a Change Log at:
<https://github.com/ConsumerDataStandardsAustralia/infosec/blob/master/CHANGELOG.md>

4.4. Deferred until future versions

Some issues have been deferred to future versions of the Security Profile. This was an important step in order to ensure that the first phase of the CDR can be implemented in a timely fashion.

The key issues deferred to future versions are:

Issue	Reason for deferral
Customisation or amendment of the Security Profile to accommodate future sectors outside the banking sector	Data61 and Galexia have discussed how the Principles will remain the same for all sectors, but the Security Profile may need to be adapted or split into sub-profiles for new sectors in the future
Levels of Assurance (LoAs) and Vectors of Trust (VoT)	Data61 and Galexia have discussed how the Security Profile may need to be updated to incorporate newer ideas and innovative approaches to authentication, including Vectors of Trust (VoT). The issue was raised with Stakeholders and presented at the Melbourne Workshop. Some requirements related to Vectors of Trust were included in V 0.0.3 of the Security Profile. Some stakeholders and Galexia raised concerns about including Vectors of Trust in the Security Profile at this early stage. Following this input, the concept has been introduced in the current draft of the Security Profile to enable and facilitate the use of VoT in the future. However, it has not been mandated. The requirements for VoT may be further refined in future versions.

4.5. Referred to other Data61 Working Groups

Some issues have been flagged as relevant for referral to other Data 61 Working Groups.

The key issues deferred to another Data61 Working Group are:

Issue	Reason for deferral
Consent requirements	Stakeholders raised several issues regarding consent management and revocation. Data61 and Galexia have discussed how requirements to facilitate consent as envisaged in the ACCC Rules are vital, but it can be difficult to manage within the work on the Security Profile. There are both technical and policy issues associated with consent in the CDS work the focus is on technical and functional requirements associated with consent (e.g. testing and facilitating granular levels of consent; time-based dimensions of consent; consent revocation; and front end permissions language). Data61 has advised that these requirements will be addressed across the entire program from January 2019 as part of the development of Version 1 of the draft standards.

Redirect flow and phishing attacks	Banking stakeholders have raised concerns about the redirect authentication flow exposing their systems and customers to a greater risk of phishing attacks. Banks have been educating their customers to NOT follow redirects to their websites, however under the CDR this may become a mandated practice. Phishing attacks are a threat faced by the banks, given existing support for single factor authentication (username and passwords/pins). There is a concern from banking stakeholders that a redirect flow under the CDR regime, without additional safeguards, would increase existing phishing risks. Ensuring the Security Profile aligns with ACCC requirements regarding multi-factor authentication (noting that Read and Write will have a minimum of 2FA) will be a priority in January 2019.

4.6. Summary GitHub Issues Table

The following issues have been raised via GitHub <https://github.com/ConsumerDataStandardsAustralia/infosec/issues> as at 19 December 2018 (4:30pm).

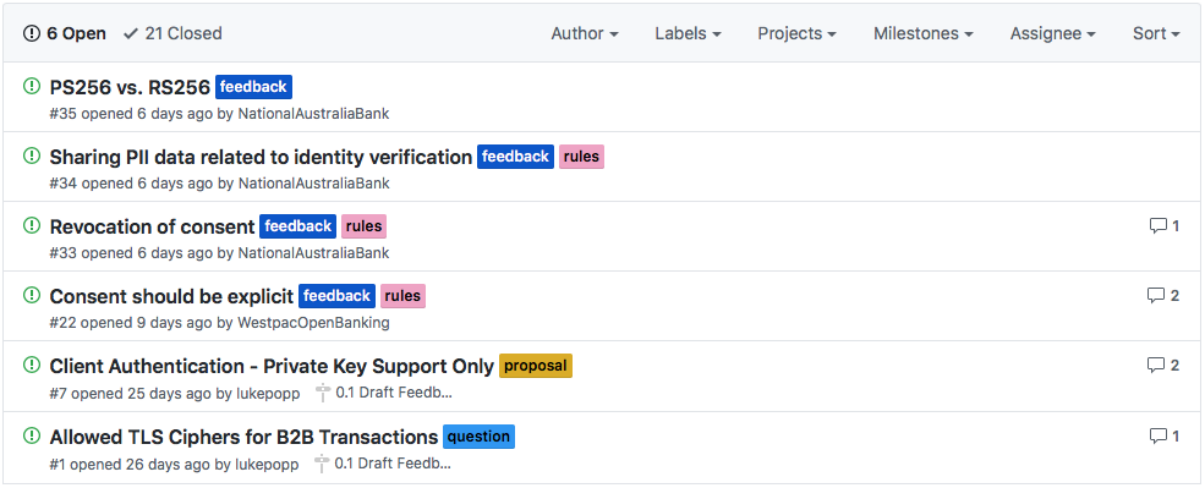

Figure: Open GitHub Issues (as at 19 Dec 2018 (4:30pm)) are mostly feedback and CDR Rules related.

#	Issue	Raised by	Category	Tags: Proposal (1) / Feature (11) / Question (2) / Feedback (9) / Wont Fix (2) / Rules (3) / Bug (6)	Status (as at 19 Dec 4:30pm) - Open (6) - Merged (13) - Closed (25)	Galexia Notes
#1	Question re crypto strength / cypher	Stakeholder	Question		Open	Still outstanding
#2	Initial Publication	Data61			Merged	Fixed
#3	Typo	Data61	Bug		Closed	Fixed
#4	Add LOA 2	Stakeholder	Feature		Closed	Added in v.0.0.3
#5	Add Change Log	Data61	Feature		Closed	
#6	Add Change Log	Data61			Merged	Merged with #5
#7	Client Authentication - Private Key Support Only	Data61	Proposal		Open	Two major banks have supported this on GitHub
#8	Is SMS OTP a valid second factor to achieve an LoA of 3?	Stakeholder	Question		Closed	Subject of significant debate and concern
#9	Typo	Data61			Merged	Merged with #3
#10	Add Vectors of Trust	Data61	Feature		Closed	Added to v0.0.3
#11	Refine Introspection Endpoint section	Data61	Feature		Closed	Added to v0.0.3
#12	Outline the mechanism for aligning consent with authorisation	Data61	Feature		Closed	Added to v0.0.3
#13	Clarify Request Object content	Data61	Feature		Closed	Added to v0.0.3
#14	Make the JWKS KeyIDs consistent with OBIE	Data61	Feature		Closed	Added to v0.0.3
#15	Spec is a little unclear as to what is normative	Stakeholder	Question		Closed	Raised a comms issue. Resolved in 24.
#16	Typo	Data61	Bug		Closed	Fixed
#17	Typo	Data61	Bug		Closed	Merged with #16
#18	Typo	Stakeholder	Bug		Closed	Raises numerous small typos, changes and suggestions
#19	Add more detail to Client Authentication section	Stakeholder	Feedback		Closed	
#20	acr_values` not compatible with FAPI?	Stakeholder	Question		Closed	Resolved in #24.
#21	Typo	Data61	Feature		Merged	Fixes numerous typos etc.
#22	Consent should be explicit	Stakeholder	Feedback		Open	Issue for ACCC Rules
#23	fix metadata typo on response modes supported	Data61	Bug		Merged	Fixed
#24	Define Normative and Non-Normative elements	Data61	Feature		Closed	This resolved issues raised in #15, #16 etc.
#25	Adding content for v0.0.3	Data61			Merged	Release of v0.0.3 and resolving earlier issues
#26	fix typo on userinfo endpoint	Data61	Bug		Closed	Fixed

#	Issue	Raised by	Category	Tags: Proposal (1) / Feature (11) / Question (2) / Feedback (9) / Wont Fix (2) / Rules (3) / Bug (6)	Status (as at 19 Dec 4:30pm) - Open (6) - Merged (13) - Closed (25)	Galexia Notes
#27	Support required for BCP47 [RFC5646] language tags in registration?	Stakeholder	Feedback		Closed	More likely an issue for other work, rather than the Profile
#28	Fix `private_key_jwt` claim descriptions.	Stakeholder			Closed	Withdrawn by the stakeholder
#29	Add `essential` field in examples of essential claims.	Stakeholder	Feedback		Closed	Flagging an inconsistency with OIDC
#30	12.2 might imply vectors of trust is required	Stakeholder	Feature		Closed	This issue also raised by Galexia - see G18, G14, G19 in Galexia review of v0.0.3 with D61 on 12 Dec
#31	Authorisation endpoint should use MTLS	Stakeholder	Feedback		Closed	Flagging an inconsistency with FAPI
#32	Typo	Data61	Bug		Closed	Fixed
#33	Revocation of consent	Stakeholder	Feedback		Open	Tricky query that veers into Consent API territory
#34	Sharing PII data related to identity verification	Stakeholder	Feedback		Open	Important query re clash between ACCC Policy and current business practice
#35	PS256 vs. RS256	Stakeholder	Feedback		Open	Concern re interoperability issues if one approach is selected
#36	Typo	Data61	Bug		Merged	Fixed
#37	X.1254 (Entity authentication assurance framework) - Normative to Informative	Data61	Feature		Closed	
#38	Updates for 0.0.3+3	Data61	Bug		Merged	Resolves #29, #30, #37
#39	Document improvements	Data61	Bug		Merged	Document improvements, typos, etc
#40	Consistent use of Data Holder and Data Recipient terms	Data61	Bug		Merged	
#41	READ ME update	Data61			Merged	
#42	Changing consentId field as part of cliams in Request Object	Stakeholder	Bug		Closed	Fixed
#43	Fixing bug #42 and updating examples	Data61	Bug		Merged	
#44	Updating Sequence Diagrams in Appendix - Consent Term to Authorisation Term	Data61			Merged	

6. Risk management

This section highlights the critical importance of developing and maintaining a comprehensive and up-to-date risk management framework.

Effective risk management is fundamental to good security practices. This is evident in the draft ACCC CDR Rules Framework[4] (section 6.2.1) where accreditation of Data Receivers will involve an assessment of their internal risk management processes, including:

- Effective procedures to identify, manage and monitor any risks to which it might be exposed with respect to CDR data;
- Procedures and processes to comply with the privacy safeguards;
- Procedures for monitoring, handling, and following up security incidents and security-related customer complaints;
- Measures and tools for the prevention of fraud and illegal use of CDR data; and
- Descriptions of security control and mitigation measures and procedures for the mandatory reporting of incidents.

In this context, development and implementation of the Information Security Profile should also involve the development of a comprehensive Risk Management Framework.

An effective risk management framework delivers the following benefits to an organisation.

- Improved ability to identify, evaluate and manage threats and opportunities;
- Improved accountability and better governance;
- Better management of complex and shared risks; and
- Improved decision making processes.

While development of such a risk management framework is out of scope for this report it is evident to Galexia that future development of the CDR policies, rules and standards will involve different degrees of risk that will need to be effectively managed – not just by Data61 but also Treasury, the ACCC and the OAIC.

As such a structured and coordinated approach to risk management will be essential across these key organisations in order to deliver the required CDR outcomes.

[4] *Draft ACCC CDR Rules Framework*, 11 September 2018 <https://www.accc.gov.au/system/files/ACCC%20CDR%20Rules%20Framework%20%28final%29.pdf>