Data Standards Body
Technical Working Group

Decision 78 – Independent Information Security Review

Contact: James Bligh

Publish Date: 15th July 2019

Decision Approved By Chairman: 16th July 2019

Context

Upon the release of the May 2019 draft version of the CDR standards (version 0.9.3) the Data Standards Body commissioned Fortian (https://fortian.com.au) to undertake an independent review of the Information Security profile included in the May 2019 draft.

This document is a response to the report that Fortian has delivered addressing the recommendations made in that report.

Decision To Be Made

Decide the changes to the CDR standards arising from the independent information security review.

Feedback Provided

This decision is in direct response to the independent information security review report. This has been published on GitHub at:
https://github.com/ConsumerDataStandardsAustralia/standards/issues/78

Decision For Approval

The following is a response to the report arising from the independent information security review.

Note that the report documents a number of observations that are positive or neutral in nature. Not all of these observations are responded to. Only the observations that are significant or have given rise to specific recommendations are addressed.

Finding Of Suitability

The Data Standards Body acknowledges the finding that the information security profile is assessed as being suitable for the initial phase of the CDR regime (acknowledging that some changes are recommended). In light of this, significant changes the to the information security profile will not be undertaken prior to the commencement of the initial implementation phase.

Considerations For Future Phases

The report identified three specific areas of future consideration. These have been noted and will be actively investigated in subsequent phases of the CDR regime. These areas of future consideration are:

- Investigate support for bank risk engines including mechanisms to provide the data and controls that these engines need to function effectively
- Investigate the inclusion of emerging standards and features that will increase the overall security of the regime (such as detached signatures and the JARM specification)
- Investigate the utility and impacts of introducing mechanisms for the customer to provide more fine-grained authorisation

Authorisation Flow

The recommendation to adopt a pure redirect model in the initial phase due (in part) to the standardised nature of this mechanism has been noted. This option was seriously considered along side the other four articulated options via a number of targeted consultations with stakeholders including the security teams of the impacted banks.

The final decision was to adopt the Redirect with OTP flow. While this was not completely aligned to the recommendation of the report, the arguments and findings of the report were of considerable value in the choice and were incorporated. The final decision for Redirect with OTP was made so as to address concerns with systemic phishing risks that are perceived to be associated with the pure redirect flow. It was also made to accommodate future sectors where existing digital channels are not ubiquitous, such as the energy sector.

The full description of the final decision on authorisation flow for the first phase of implementation, along with the rationale, has been published at:
https://github.com/ConsumerDataStandardsAustralia/standards/issues/76

Consent

The final decision on consent for the first phase of implementation aligns with the recommendation of the review. Detail on the decision and rationale has been published at: https://github.com/ConsumerDataStandardsAustralia/standards/issues/77

OBS-01 IP address forwarding

Recommendation: *It is recommended that the CDS use the 403 forbidden response code with an error payload detailing the reason for authorisation failure.*

Decision: This recommendation will be adopted into the standards.

OBS-02 Browser metadata

Recommendation: *It is recommended that the CDS be extended to forward browser headers to the data holder. A solution could be to Base 64 encode all inbound headers and forward them to the data holder with a custom X-Originating-Agent header. This will permit banks to continue use of tools that detect malicious end-user behaviour.*

Decision: This recommendation will be adopted into the standards. It aligns with the feedback in matter A14 to the May 2019 draft. The decision in response to matter A14 is believed to also address this recommendation.

OBS-05b JARM response types

Recommendation: *Consider implementation of JARM. It is noted that JARM was introduced in October 2018, so may not have been specified in the original development of the CDS.*

Decision: Due to the need to understand the impacts of this recommendation it will not be incorporated into the standards at this stage but will be considered for incorporation into the next phase of the regime.

OBS-06 Hybrid flow and phishing attacks

Recommendation: *It is recommended that:*

- *Product certification must ensure that Request Objects are digitally signed, but also that there is no way to disable such a feature. This is important to note as many solution providers are building on top of existing, less secure OIDC implementations.*
- *The CDR Register must restrict redirects to known endpoints that have been previously registered, and this must likewise be assured in product certification.*
- *Stronger authentication mechanisms (e.g. FIDO) should be considered as another method to counter phishing risks.*

Decision: This first two points of this recommendation fall into the purview of the accreditation regime and the register. This feedback will be passed on to the appropriate stakeholders

accordingly. The recommendation regarding stronger authentication mechanisms (such as FIDO) will be considered for ongoing consultation.

OBS-09 Consent – broad access to data

Recommendation: *It is recommended that the CDS be updated to note that the competitive space will find solutions for authorisation of individual accounts.*

Decision: This recommendation will be adopted into the standards.

OBS-11 Consent – rich access to data

Recommendation: *It is recommended that banks review the use of transaction data for end-user authentication at the phone channel. Banks that make use of 'rich data' for phone-based authentication may choose to move to alternate approach in advance of Open Banking deployment.*

Decision: This recommendation will be communicated to the Banks via the Australian Banking Association.

OBS-16b Integrity controls of APIs

Recommendation: *Consider inclusion of Detached JWT Headers (x-jws-signature). This has been introduced by UK Open Banking as a standardised control for API response integrity.*

Decision: Due to the need to understand the impacts of this recommendation it will not be incorporated into the standards at this stage but will be considered for incorporation into the next phase of the regime. This decision has been made noting that the first phase incorporates read only data only and has compensating controls in the form of MA-TLS with HoK for all calls to resource end points.

OBS-17 Scope and linkage to intent

Recommendation: *The CDS should define scope labels that better convey intent.*

Decision: This recommendation will be adopted into the standards. Specifically scopes will be modified to meet the following form:

```
<namespace>:<type>.<sub-type (optional)>:<access>
```

For example:

- bank:accounts.detail:read
- common:customer.basic:read
- bank:payees:read

OBS-18 Consent – non-repudiation

Recommendation: *Guidance should be provided to Data Recipients to record the following each time consent events occur, including: Username (consumer's ID at the Data Recipient), Timestamp, IP, Consent Scopes.*

Decision: This recommendation will be adopted into the standards.