Data Standards Body
Information Security Technical Working Group
Decision 023 – Initial Directions for Information Security

Contact: Seyit Camtepe, James Bligh

Publish Date: 15th October 2018

Decision Approved By Chairman: 20th October 2018

Context

To facilitate the creation of the Consumer Data Rights Standards, an Information Security Technical Working Group (the IS Working Group) has been established.

The purpose of this document is to kick-start activities of the information security technical working group (ISTWG). ISTWG's first step is to investigate UK standards and identify the initial directions to follow towards establishing security profiles for Australian banking.

Decision To Be Made

The UK Open Banking regime has published a security profile based on the OpenID Foundation's (OIDF) Financial API Read/Write specification document. This decision aims to determine the way to use the UK results towards establishing security profiles for Australian data transfer under the Consumer Data Standards.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/open-banking/issues/7

Feedback was broadly supportive of the recommendation although some participants did call for option 1 as a more secure path. There was also some feedback indicating that there was concern that changes for the Australian context could result in a FAPI+ situation that would make the Australian regime non-standard. This feedback has been incorporated into the final recommendation.

Decision For Approval

The decision for the Australian Consumer Data Right API standards is to adopt the Financial API Read/Write security profile with an expectation that there will be changes to accommodate local considerations.

Local changes of the FAPI R/W security profile will only be made where:

- They are required to accommodate industries other than financial services (recognising the economy wide scope of the Consumer Data Right in Australia)
- They are explicitly requested by a plurality of stakeholders and the result of the changes is to make the regime more secure
- They are made to allow for implementation timeframes and scope to be met
- They are made to accommodate specific implementation considerations such as the ACCC Directory design

The implication of this decision is that the fundamentals of the UK profiles will continue to be supported. Namely:

- OpenID as an identity and authentication protocol,
- OAuth 2.0 as a delegated authorization protocol, and
- Transport Layer Security (TLS) as a secure web communication protocol.