Data Standards Body
Information Security Technical Working Group

Decision 033 – Use of TLS/MTLS

Contact: James Bligh

Publish Date: 2nd November 2018

Decision Approved By Chairman: 2nd November 2018

Context

The Information Security Working Group's starting point is the UK open banking security profile, based on Open ID's Financial-grade API (FAPI) Read/Write API Security Profile. The FAPI profile builds upon a set of OAuth 2.0, OpenID Connect and Transport Layer Security standards, drafts and specifications.

This decision proposal identifies Transport Layer Security models (TLS) and associated services used to secure interactions between regime participants.

Decision To Be Made

This proposal outlines the requirements for securing of communications between a data provider and a data consumer. These requirements are based on the OIDC Financial API Read/Write profile with specific constraints relevant to the meet the July 1st implementation date.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/open-banking/issues/33

Feedback was varied on this proposal and has been largely incorporated, especially regarding the implications of mandating TLS v1.3 as opposed to TLS 1.2. The decision represents a step forward in determining aspects of the security profile for the standard it is acknowledged that this position will iterate via in person working group meetings where other aspects of the profile will be considered.

Decision For Approval

The decision is to adopt the Financial API Read/Write security profile requirements for the use of TLS and Mutual Authentication TLS (MTLS) with some specific caveats to accommodate the specific context of the Consumer Data Right regime. In particular, the role of the ACCC Directory in the operation of the overall regime is an important consideration.

Specifically this implies that the following will be incorporated into the standards:

- Use of TLS mandated for all interactions
- Requirement to use TLS 1.2 or greater
- The version and configuration of TLS for the Consumer Data Right API standards will not be a lower version or less secure than other that of other digital channels deployed by the data provider
- A TLS server certificate check shall be performed, as per RFC 6125
- MTLS will be used to encrypt back-channel communication between the data consumer and data provider
- The choice of MTLS or *private_key_jwt* for data consumer authentication will be driven by the design of the ACCC Directory and will not be optional in the July 1st 2019 timeframe.
- For all interactions except for authorisation only the following cipher suites may be used:
    - *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
    - *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*