Data Standards Body
Information Security Technical Working Group
Decision Proposal 033 – Use of TLS/MTLS

Contact: Seyit Camtepe, James Bligh

Publish Date: 15th October 2018

Feedback Conclusion Date: 19th October 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.

Current Recommendation

The options that were considered (implicitly or explicitly) are listed in the next section. In a previous version of this proposal a recommendation was put forward that is now referred to as option 3. After receipt and review of feedback on this proposal the recommendation has been modified to align to what has been defined as option 2 (with option 1 being provided for context and completeness).

The recommendation of this proposal 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*

Additional Notes

- As the role and functionality of the ACCC Directory in the overall regime is not yet clear some variability around data consumer authentication is found in the proposal. This variability will be removed once the role of the Directory is clarified.
- No explicit consideration has been given to variations between what the FAPI profile describes as *Public* or *Confidential* clients. This is due to the fact that it is not yet determined if the use of the Implicit flow or Hybrid flows of OAuth 2.0 will be allowed under the standards.

Identified Options

Option 1 – Align with FAPI Read Only Profile

The FAPI Read Only Profile requires the following:

- Use of TLS for all interactions
- Requirement to use TLS 1.2 or greater
- Use of any BPC 195 recognised cipher suites
- Use of *client_secret_jwt* or *private_key_jwt* or MTLS for data consumer authentication
- A TLS server certificate check shall be performed, as per RFC 6125

Following feedback in response to Decision Proposal 023 (Initial Directions towards establishing security profiles in Australian banking), aligning with the FAPI Read/Write Profile is preferred. As such, Option 1 Is not the recommended option.

Option 2 – Align with FAPI Read/Write Profile

The FAPI Read/Write profile builds on the Read Only profile with the following additional constraints:

- 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*
- *client_secret_jwt* may not be used for data consumer authentication

Option 3 – Align with FAPI Read/Write Profile but constrain to TLS 1.3+

Extend the FAPI Read/Write profile but require the use of TLS 1.3. In addition the following features of TLS 1.3 would be required:

- ***Cryptographic Primitives and Key Sizes***
  Use of cryptographic primitives supported by TLS 1.3, and the adoption of an at least 80-bit security rating, preferably over 128-bit security rating, following the NIST key size guidelines.
- ***Support for Certificate Bound Access Tokens***
  Adoption of certificate bound access tokens with MTLS, to prevent the replay of, or use of, stolen access tokens by any malicious parties.

Certificate Extensions

Adoption of standard X.509 v3 extensions, and to define custom extensions for passing accreditation information and redirect-uri information from the accredited receiver to data holder. This will be used as an additional protection on top of the methods proposed by OAuth 2.0 standards and provide a means for data holders to cross check uris before redirecting the customer along with authorization code, access token or ID token.

The previous version of this proposal suggested constraining to TLS 1.3 as a starting point. Feedback has already been provided in the repository that imposing TLS 1.3 as a constraint would be

premature. We are leaving in this option to seek further feedback before moving forward with an approach.