Data Standards Body
Technical Working Group

Decision Proposal 065 – Transaction Security

Contact: James Bligh

Publish Date: 30th April 2019

Feedback Conclusion Date: 10th May 2019

Context

The Information Security profile has been undergoing consultation since mid to late 2018. During this time a number of decisions have been made regarding the approach the CDR regime will take to ensure information security practices are consistently applied to protect participants as data is shared.

This decision proposal, along with a number of others, packages a related group of these incremental decisions in a single common artefact that can be formally approved by the Data Standards Chair so that a binding standard can be established in accordance with the ACCC Consumer Data Rules.

This proposal specifically relates to the application of security controls, protocols and conventions to API transactions that occur under the CDR regime for any purpose.

Note that this proposal builds upon the previous decision proposal 033, Use of TLS-MTLS.

Decision To Be Made

Decide how participants will apply transaction security under the CDR regime.

Current Recommendation

Note that references to external standards are defined in Decision Proposal 063 – Normative References.

Use of TLS

All HTTP calls MUST be made using HTTPS incorporating TLS >= 1.2. This MUST include calls to public, unauthenticated end points.

Only the following cipher suites SHALL be permitted in accordance with section 8.5 of [FAPI-RW]:

- 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

Use of Mutual TLS

All back-channel communication between Data Recipient systems and Data Holder systems MUST incorporate, unless stated otherwise, MTLS as part of the TLS handshake:

- The presented Client transport certificate MUST be issued by the CDR Certificate Authority (CA). The Server MUST NOT trust Client transport certificates issued by other authorities.
- The presented Server transport certificate MUST be issued by the CDR Certificate Authority (CA). The Client MUST NOT trust Server transport certificates issued by other authorities.

End points for transferring CDR Data that is considered public and unauthenticated do not require the use of MTLS.

Holder of Key Mechanism

MTLS MUST be supported as a Holder of Key Mechanism.

OAUTB SHALL NOT be supported due to a lack of industry adoption.

MTLS Holder of Key allows issued tokens to be bound to a client certificate as specified in section 3 of [MTLS].