Data Standards Body
Technical Working Group

Decision Proposal 066 – Authorisation End Points

Contact: James Bligh

Publish Date: 6th May 2019

Feedback Conclusion Date: 17th 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 end points that must be supported by data holders and data recipients to facilitate consent, authorisation and authentication management within the CDR Regime.

This proposal takes into account the Data Standards Body's current understanding of the design of the CDR Register. Design decisions that change these assumptions may prompt amendments to these end points.

Decision To Be Made

Define the information security end points that must be supported under the CDR Regime.

Current Recommendation

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

Initial Notes

Some additional notes specific for this proposal in response to previous feedback and positions that have evolved:

- Dynamic registration MUST not be supported. Clients will register with the ACCC Register, which will then make the information required to facilitate consent and authorisation available to other CDR Participants. Note that this includes information pertaining to both Data Holders and Data Recipients.
- A Consent API is no longer included in the Information Security profile so no end point will be defined.
- An endpoint for re-authorisation is required to be included in the CDR Regime but this is beyond the scope of this decision proposal and will be articulated through a separate decision proposal.
- This decision proposal does not include any specification for endpoints to be implemented by the ACCC Register.

OpenID Provider Configuration Endpoint

Hosted By	Data Holder
Transport Security	TLS
Client Authentication Required	No
Bearer Token Required	No

Data Holders MUST make their OpenID Provider Metadata available via a configuration endpoint as outlined in Section 3 and 4 of the OpenID Connect Discovery standards [OIDD].

Where a Data Holder is supporting Vectors of Trust [VOT] the published OpenID Provider metadata SHALL reflect that support.

At a minimum, the Data Provider metadata MUST include:

- issuer: URL that the Data Holder asserts as its Issuer Identifier.
- authorization_endpoint: URL of the Authorization Endpoint.
- token_endpoint: URL of the Token Endpoint.
- introspection_endpoint: URL of the Introspection Endpoint.
- revocation_endpoint: URL of the Revocation Endpoint.
- userinfo_endpoint: URL of the UserInfo Endpoint.
- jwks_uri: URL of the JWKS Endpoint.
- scopes_supported: This list of supported scopes.
- claims_supported: The list of supported claims.
- acr_values_supported: The supported ACR values.

Data Holders that support Vectors of Trust [VOT] MUST include:

- vot_values_supported: The list of supported component values.

Authorisation Endpoint

Hosted By	Data Holder
Transport Security	TLS
Client Authentication Required	No
Bearer Token Required	No

The requirements for the Authorisation Endpoint are specified in section 3.3.2 of [OIDC] and further specified under section 5.2.2 of [FAPI-RW]. This endpoint is invoked as part of the Hybrid Authentication flow.

Only a response_type (see section 3 of [OIDC]) of code id_token SHALL be allowed.

The request_uri parameter SHALL NOT be supported.

A description of requirements relating to the request parameter can be found in *Decision Proposal 064 – Scopes, Claims & Tokens*.

Token Endpoint

Hosted By	Data Holder
Transport Security	MTLS
Client Authentication Required	Yes
Bearer Token Required	No

The requirements for the Token Endpoint are specified in section 3.3.3 of [OIDC].

To obtain an Access Token, an ID Token, and a Refresh Token, the Data Recipient sends a Token Request to the Token Endpoint.

The Token Endpoint MUST incorporate the extensions required in *Decision Proposal 064 – Scopes, Claims & Tokens*.

Data Holders MUST support a Token Endpoint.

UserInfo Endpoint

Hosted By	Data Holder
Transport Security	MTLS
Client Authentication Required	No
Bearer Token Required	Yes

The requirements for the UserInfo Endpoint are specified in section 5.3 of [OIDC].

Data Holders MUST support a UserInfo Endpoint.

Introspection Endpoint

Hosted By	Data Holder
Transport Security	MTLS
Client Authentication Required	Yes
Bearer Token Required	No

Data Holders MUST implement an Introspection Endpoint to allow Data Recipients to determine the status and expiry date of Refresh Tokens and Sharing IDs. The requirements for an Introspection Endpoint are described in section 2 of [RFC7662].

Introspection of Refresh Tokens MUST be supported.

Introspection of Sharing IDs MUST be supported. In this case the token_type_hint parameter MUST be set by the client to sharing_id to indicate that the token parameter contains a Sharing ID.

Introspection of Access Tokens and ID Tokens MUST NOT be supported.

An Introspection Endpoint Response SHALL only include the following fields:

- active: Boolean indicator of whether or not the presented token is currently active.
- exp: A JSON number representing the number of seconds from 1970-01-01T00:00:00Z to the UTC expiry time.

Token Revocation Endpoint

Hosted By	Data Holder & Data Recipient
Transport Security	MTLS
Client Authentication Required	Yes
Bearer Token Required	No

Data Holders and Data Recipients MUST implement a Token Revocation Endpoint as described in section 2 of [RFC7009].

Requirements for Data Holder implementations

The Revocation Endpoint serves as a revocation mechanism that allows a Data Recipient to invalidate its tokens as required to allow for token clean up. It also provides a mechanism for a Data Recipient to notify the Data Holder of the revocation of a sharing arrangement by the Customer in totality as required by the ACCC CDR Rules. This revocation will have been actioned by the Customer via the Data Recipient's consent dashboard as described in the ACCC CDR Rules.

Revocation of Refresh Tokens and Access Tokens MUST be supported.

Revocation of Sharing IDs MUST be supported. In this case the token_type_hint parameter MUST be set by the client to sharing_id to indicate that the token parameter contains a Sharing ID.

If consent is withdrawn by a Customer in writing or by using the Data Holder's dashboard the Data Holder MUST use the revocation endpoint to notify the Data Recipient.

If a Sharing ID is revoked by a Data Recipient then the Data Holder MUST invalidate all active Access Tokens and Refresh Tokens associated with that Sharing ID.

Requirements for Data Recipient implementations

The Revocation Endpoint, when implemented by the Data Recipient allows a Data Holder to notify the Data Recipient of the revocation of a sharing arrangement by the Customer in totality as required by the ACCC CDR Rules. This revocation will have been actioned by the Customer via the Data Holder's consent dashboard as described in the ACCC CDR Rules.

Revocation of Refresh Tokens and Access Tokens MUST be supported. Note that Data Holder's MAY notify the Data Recipient of the invalidation of an Access Token or Refresh Token but this is not required.

Revocation of Sharing IDs MUST be supported. In this case the token_type_hint parameter MUST be set by the client to sharing_id to indicate that the token parameter contains a Sharing ID.

If consent is withdrawn by a Customer in writing or by using the Data Recipient's dashboard the Data Recipient MUST use the revocation endpoint to notify the Data Holder.

If a Sharing ID is revoked by a Data Recipient then the Data Holder MUST invalidate all active Access Tokens and Refresh Tokens associated with that Sharing ID.