Data Standards Body
Technical Working Group

Decision Proposal 062 – Authorisation Flow

Contact: James Bligh

Publish Date: 2nd 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 authorisation flow where CDR Consumer grants consent for data sharing from a Data Holder to a Data Recipient. This proposal covers the mechanisms for performing this authorisation within the CDR Regime.

Decision To Be Made

Define the overall authorisation flow for sharing of CDR Data.

Identified Options

This proposal has been formulated according to the decision previously made by the Data Standards Chair in Decision 035 – Customer Authentication Flows.

The CDR Participant community has suggested other flows for authorisation and the Data Standards Chair is reviewing these. If a change in direction is decided any decisions arising from this proposal will be amended accordingly.

Current Recommendation

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

Authentication Flows

This profile supports a subset of the authentication flows specified by FAPI [FAPI].

Specifically the Hybrid Flow outlined at section 3.3 of [OIDC] is supported. This flow MUST be supported by Data Holders.

No other flows are currently supported.

OIDC Hybrid Flow

The [OIDC] Hybrid Flow is a type of redirection flow where the CDR Consumer's user agent is redirected from a Data Recipient's (Relying Party) web site to a Data Holder's Authorisation endpoint in the context of an [OIDC] authentication request. The Hybrid flow incorporates aspects of both the implicit flow and authorisation code flow detailed under [OIDC].

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

The request_uri parameter SHALL NOT be supported.

Authentication Via Known Channel

Upon redirection under the [OIDC] Hybrid Flow the Data Holder MUST NOT authenticate the Customer via the redirected page. This is to mitigate the risk of phishing attacks via Customer education.

Data Holders MUST support the capture of the Customer's username via the redirected page. This username would be the same identifier the Customer would normally use for other digital channels provided by the Data Holder. The Data Holder would then direct the Customer to complete authorisation via an existing digital channel that the Customer is familiar with using.

Data Holders MUST support the completion of authorisation via the various digital channels they offer that Customers would reasonably expect to use on a regular basis.

Data Holders MUST identify that an authorisation is in progress in their existing digital channels upon authentication and initiate the appropriate user experience.

Data Holders MUST NOT automatically launch their existing digital channel from the redirect page. The initiation of authentication by the Customer in the existing digital channel MUST be a volitionary action by the Customer.

Data Holders MUST apply a timeout of five minutes for the completion of the volitionary action by the customer of authenticating in an existing channel. Failing to authenticate within this timeout SHOULD be considered as abandonment of the authorisation process and require the process to be reinitiated by the customer.

Upon completion of consent the Data Holder must utilise the redirect URI supplied by the Data Recipient from the existing digital channel according to the [OIDC] Hybrid Flow.

As the Customer may have used a different device to access the existing digital channel to complete authorisation the use of the redirect URI supplied by the Data Recipient may occur from a different device. The Data Holder and Data Recipient must facilitate this scenario.

The mechanism by which the information captured on the redirect page presented by the Data Holder under the [OIDC] Hybrid Flow and the implementation of the existing known channel is not prescribed. This mechanism is left to the competitive space.

The specific user experience requirements for this flow will be defined by the Customer Experience standards for the CDR regime and are beyond the scope of this proposal.

OIDC Client Types

Confidential Clients MUST be supported under this profile.

Public clients MUST NOT be supported.

Consent

Previously the CDR Information Security profile indicated that a separate API for establishing consent prior to authorisation being initiated would be the case. This position has changed and the Consent API and associated Consent ID are no longer required by the profile.

Instead, consent requirements will be communicated between the Data Recipient and Data Holder using scopes and claims under [OIDC].