Data Standards Body

Information Security Technical Working Group

Decision 036 – OIDC userinfo Support

Contact: James Bligh

Publish Date: 2nd November 2018

Decision Approved By Chairman: 2nd November 2018

Context

The decision to adopt the Financial API Read/Write security profile implies the adoption of the Open ID Connect (OIDC). OIDC contains within the specification an end point for a data consumer to request various elements of information about the user. It also allows for extension of this data.

The CDR regime also includes this data in scope but with a need for significant visibility and control for the customer about what information has been requested. As a consequence it has been decided to introduce a series of resource specific end points for the Customer record which will deliver information equivalent to that provided by the userinfo end point under OIDC.

This introduces the possibility of duplication within the regime with the same data obtainable via the Customer end points as via the userinfo end point. This proposal puts forward options for resolving (or accepting) this duplication.

Decision To Be Made

To what extent will data providers under the Consumer Data Right standards be expected to support the OIDC userinfo end point.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/open-banking/issues/36

There was a wide range of feedback for this decision proposal that was hard to synthesize due to its divergence. A number of international stakeholders indicated that the customer payload should be deprecated and the userinfo end point should be used as an alternative. Stakeholders in the financial services industry in Australia supported minimal implementation of userinfo and retention of the customer payload.

The documented decision has been set to give a position for the draft standards that balances this feedback and considers the policy goals of the regime.

Decision For Approval

The standard will support the use of the userinfo end point but limits this support only to data required to support the working of the interactions between the data consumer and data provider. Other customer specific data will be obtained via the customer end points and payloads.

Specifically, this means that the standards will support the following OIDC scopes:

- openid scope
- profile scope

The following claims, associated with the profile scope, will be supported:

- name
- family_name
- given_name

Additional claims required for the proper functioning of the OIDC protocol but that do not relate to personal information will also be supported.