Data Standards Body
Technical Working Group
Decision Proposal 036 – OIDC userinfo Support

Contact: James Bligh

Publish Date: 21st October

Feedback Conclusion Date: 2nd November

NOTE

Leading up to the definition of the first draft of the standards, the security working group decision proposals will be high level only. Due to the sensitivities around sharing security concerns and discussing current implementations in the financial sector the Advisory Committee has requested detailed security design decisions to be formulated via a series of in person meetings. These in person meetings will be co-ordinated using the security working group mailing list. You can sign up to this list at http://eepurl.com/dCNaTn.

The end result of this process will be a working draft proposal that will then be published and opened for transparent public comment, as has been the practice to date for the Data Standards Body.

For this reason this proposal, and others in this series, will focus on high level decisions that shape the overall approach to security under the regime rather than low level technical specifics.

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.

Identified Options

Option 1 – Use "userinfo" Exclusively

Deprecate the Customer end points and fold this information into the userinfo end point.

Pros

- Aligns with the OIDC standard
- Has broad vendor support

Cons

- Data payloads exposed via this end point will not necessarily align with other payloads. Conventions we have adopted such as versioning, version negotiation, payload structure are not easily carried into the userinfo end point as it is already structurally defined by the OIDC standard.
- There is a possibility that the need to extend the userinfo payload to meet the CDR requirements for the customer will make it complex and difficult to use over time. This is a data entity that is likely to be expanded in the future as KYC and other identity considerations are addressed.
- The ACCC has indicated that the customer should be able to access their own information themselves via a known channel. This could take the form of a download site for files in compliant payload form. In this scenario a separate payload definition will need to be defined anyway

Option 2 – Make "userinfo" Support Discretionary

Continue to require the implementation of the Customer end points and then leave it up to individual data providers as to the level of support they provide for the userinfo end point. Each provider would define the data accessible through userinfo and the scopes that are used to control this access.

Pros

- The CDR standard does not need to make any proposals regarding userinfo
- Data providers have discretion and control over their implementation from a cost and schedule perspective for implementing the userinfo end point

Cons

- Data consumers would need to build individual implementations for each data provider to take advantage of the userinfo end points as there would not be consistency
- The use of "claims" and "scopes" to access the same data would be required. This could introduce some conflicting situations where a customer denies a scope required to access their data but approves a claim to access the same data. Interpretation of whether the approval or the rejection takes precedence could result in some confusing audit scenarios.

- There is a possibility that there will be inconsistent levels of customer control of the sharing of customer data across data providers due to differing implementations. Customers exposed to similar claim language with different specific meanings across providers could result in misunderstanding of the data actually being shared.
- The standard payload of the OIDC profile claim includes data that is being specifically excluded, or separately authorised under the CDR standards due to the sensitivities perceived in the Australian context.

Option 3 – Minimally Support "userinfo"

The standard supports 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 (such as unique identifiers for the customer, consents, etc). While simple fields to help identify the customer reliably (such as name) may be shared via this end point, other personally identifiable information would not be. The allowable claims would be defined under the CDR standards. A request for an id_token would follow the same constraints.

Pros

- End point is still supported
- Restricts the possibility of customer misunderstanding due to differing implementation (as articulated as a Con for option 2)
- The ability to retrieve a known user identifier is useful
- Could be extended to provide additional information that supports the workings of the regime but is not personally identifiable such as information about authorisation expiration

Cons

- As the amount of information being returned is minimal the cost of supporting the end point for many data providers may be unnecessary. This would become especially true as the regime expands

Option 4 – No Support For "userinfo"

The standard does not support the userinfo end point. To facilitate the OIDC standard id_token will still be supported but only with minimal scope as defined in option 3.

Pros

- No duplication of effort and lower implementation costs as a result
- Restricts the possibility of inadvertent data leakage

Cons

- Not fully supportive of the OIDC standard

Current Recommendation

Commentary from the community is sought in regard to the approach to be used for this decision. As such a firm recommendation is not being provided.

The initial view of the Data Standards Body with regard to the four options are as follows:

Option 1 – Not Recommended
It is believed that this approach will limit the future evolution and expansion of the regime, especially as the regime expands to other industries.

Option 2 – Not Recommended
While this option would seem to be the most flexible the risk of customer misunderstanding due to the possibility of differing implementations and the overlaps between claims and scope for the same data is a concern.

Option 3 & 4 – Recommended
These options would be implementable and do not introduce additional risk although the non-standard nature of option 4 would potentially make this option less preferable.

Appendices

Appendix A: References

Open ID Connect Core - https://openid.net/specs/openid-connect-core-1_0.html

Financial API Read/Write Profile - https://openid.net/specs/openid-financial-api-part-2.html

Financial API Read Only Profile - https://openid.net/specs/openid-financial-api-part-1.html