Data Standards Body

Technical Working Group

Decision 005 – API Authorisation

Contact: James Bligh

Publish Date: 11th September 2018

Decision Approved By Chairman: 19th September 2018

Context

As part of the definition of API endpoints there is a need for defining the scope of authorisation that the end point fits into as well as the expectations around how lower level authorisation should occur.

Specifically this decision will cover two areas of importance: how the APIs should integrate with existing Digital channels offered by the providers and what specific authorisation scopes should exist for the APIs.

This decision is assuming that the authorisation model will be leveraging OAuth 2 as the UK standard has but it is not seeking to pre-empt decisions made by the security working group. It does, however, seek to clarify how APIs should respond once authorisation has been given and whether that authorisation will be covered by the standard or left to the competitive space.

Decision To Be Made

Determine how authorisation will interact with existing Digital channels and what authorisation scopes will be implemented.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/open-banking/issues/5

This proposal elicited extensive feedback. The average response was also unusually detailed relative to previous decision proposals.

In addition, since the decision proposal was initially published the ACCC rules framework has been exposed for comment and there is overlap between this proposal and the proposed rules. The final decision for approval contains a subset of the original proposal and excludes items that need to be confirmed in the ACCC rules and items that were contentious in the feedback.

Decision For Approval

The API standards will include the following with regard to authorisation scopes and behaviour. Note that the API standards are subject to the ACCC rules so areas that will be stipulated explicitly in the rules have been excluded from this decision.

Cross Channel Integration

Existing credentials already being used by customers for accessing their data via digital channels should be used when authenticating customers for the purpose of authorisation of access to API standards.

The implication of this approach is that the APIs under the standard become another channel for a customer along side their existing channels with the same levels of access and servicing mechanisms.

For in scope products that do not have an existing digital channel available for servicing there is an expectation that a new credential will be created and any subsequent digital access in the future would then use that credential. Alternatively, the product can be added to an existing digital access capability to achieve the same outcome.

Authorisation Granularity

A set high-level authorisation scopes will be defined. Each API end point should be mapped to one of these authorisation scopes as part of the standard setting process.

Based on the scope for the initial implementation for July 1st 2019 the following scopes are recommended:

- **Basic Bank Account Data**
  This scope would allow for the third party to access basic information of the customer's accounts. This would include balance but not account identifiers, product information or transaction data.
- **Detailed Bank Account Data**
  This scope would allow for the third party to access detailed information of the customer's accounts including account identifiers and product information. It would not include transaction data. This scope is effectively additional authorisation to the *Basic Bank Account Data* scope. Granting this authorisation only makes sense if the Bank Account Data scope is also authorised.
- **Bank Transaction Data**
  This scope would allow the third party to access transaction data for accounts. This scope is effectively additional authorisation to the *Basic Bank Account Data scope*. Granting this authorisation only makes sense if the Bank Account Data scope is also authorised.
- **Customer Data**
  The scope would allow the third party to access personally identifiable information about the customer (e.g. name, address, etc). For retail customers this would be information about the customer themselves. For business customers it would imply information about the specific user but also information about the business.

- **Public**
  A customer would never need to grant this scope. This scope is included so that end points that can be called without requiring authorisation can be identified. This would include end points allowing access to generic product information, branch locations, etc.

Other Considerations

In consideration of issues that may arise during implementation the following is also included in this decision:

- **Additional scopes for extended data**
  Under the extensibility model for the standards, if additional data types are made available then additional scopes may be required. For instance, if a provider wishes to make a payment API available that would require an additional scope specific to that provider. This would be considered acceptable under the standards, however, it is requested that new scopes are made in consultation with the Data Standards Body to ensure they do not clash with existing scopes or future planned scopes. If multiple providers are creating similar scopes the language and meaning can then be standardised even if end points are not being created for these scopes under the standard.
- **Scopes will be added as the regime expands**
  Over time, as the regime expands, new scopes will be added to the regime.
- **Customer can arbitrarily end authorisation**
  The provider should provide a mechanism for a customer to see the authorisations that are currently active as well as the ability to cancel any of these authorisations if they so desire.