Data Standards Body
Technical Working Group

Decision Proposal 005 – API Authorisation

Contact: James Bligh

Publish Date: 16th August 2018

Feedback Conclusion Date: 31st August 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.

Identified Options

There are potentially many different options for this domain. It is therefore not seen as constructive to articulate an arbitrary subset of these options. Instead a specific recommendation is provided without reference to the different options considered.

Current Recommendation

The recommendations have been formulated balancing the feedback previously submitted under various reviews with the need to deliver a capability according to the announced timeframes.

From a feedback perspective, the recommendation has tried to incorporate the feedback specifically focused on the need for customer control and understanding of the authorisations they provide. For instance, the need for customers to control the granularity of the data that is transferred and for how long the transfers can continue.

Cross Channel Integration

It is recommended that existing credentials already being used by customers for accessing their data via digital channels should be used for the authorisation of access to API standards.

There are a number of advantages driving this recommendation:

1. Greater understanding and familiarity on behalf of the customer when providing authorisation. This translates into a reduction in friction for the customer in taking up of Open Banking (as the first industry to be covered). As the customer's existing credentials will be used for authorisation there will be fewer steps for customers to perform an authorisation for the first time. This will lead to increased adoption of data sharing under the regime.
2. This approach resolves many of the issues with low granularity authorisation. As authorisation is given via a specific credential it implies that only the data and services accessible from that credential can be authorised. This resolves issues around joint accounts and the complex authorisations for business customers by leveraging the existing mechanisms created for existing Digital channels.
3. Servicing events such as password resets, account locking and account creation should already be in place for the existing set of credentials. This will reduce implementation costs.

The implication of this approach is that the APIs under the standard simply become another channel for a customer along side their existing channels with the same levels of access and servicing mechanisms. If they can access an account via Internet Banking then they should be able to access it via the Open APIs. If they lose access to an account in Internet Banking then they should also lose access to that account via the Open APIs – even if they have previously authorised access to that account.

Essentially, authorisation is for a third party to access data that the authorising entity has access to for as long as that authorising entity themselves can also access that data.

Authorisation Granularity

It is recommended that a set of high-level authorisation scopes be defined and that each API end point should be mapped to one of these authorisation scopes as part of the standard setting process.

A small number of high-level scopes maps well to the OAuth authorisation protocol, so implementation complexity will be reduced. A small number of scope that are easily understood by the customer will also increase customer understanding of the process and thereby increase confidence in the sharing of data.

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

- **Bank Account Data**
  This scope would allow for the third party to access details of the customer's accounts including product information (rates, etc) and current balance. It would not allow access to more detailed information such as transaction data.
- **Bank Transaction Data**
  This scope would allow the third party to access transaction data for accounts. This scope is effectively additional authorisation to the 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.

It would be recommended to the User Experience Working Group that uniform language be adopted to describe these scopes so that customers would receive consistent messaging on these scopes regardless of the data consumer or data providers that they are interacting with.

Other Recommendations

In consideration of issues that may arise during implementation the following is also recommended:

- **Additional authorisation in the competitive space**
  It will be left to the competitive space if a provider wishes to provide their customers with additional authorisation flexibility. For instance, a data provider may wish to allow a customer to specify which accounts should be accessible under a registration. This level of granularity would not be mandated for all providers by the standards, however. If providers wish to provide additional authorisation capability it would be expected that this would not impact the user experience mandated for authorisation by the User Experience Working Group.
- **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. 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.
- **Scopes will be set via consumer registration**
  Scopes required by a client will be presented to the customer during the authorisation process. The customer will, however, not be given the option of partial authorisation (i.e. approving one requested scope but denying another). Allowing this will increase complexity of implementation for both the consumers and providers and, given the small number of defined scopes, there would be little benefit to the customer. As the regime expands this recommendation may be revisited.
- **Time based authorisation**
  At the time of authorisation, along with the scope of authorisation, the customer will also be informed of the length of time that authorisation is being sought by the third party. This allows the customer to decide if the length of authorisation matches their understanding of the service being offered.
- **All authorisations are time based**
  There should be no concept of indefinite authorisation. All authorisations should be time limited with an expectation that the customer needs to reaffirm consent for the data transfer to continue.
- **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.