Data Standards Body
Information Security Technical Working Group
Decision 036 – Customer Authentication Flow

Contact: James Bligh

Publish Date: 2nd November 2018

Decision Approved By Chairman: 2nd November 2018

Context

The flow between the three parties involved in the establishment of authorisation is critical to the success for the CDR regime. This flow will have significant impact on the regime as it will be the first interaction point for a customer that is interested in sharing their data.

There are a number of options for how this flow can work. This proposal articulates some constraints on these options so that the authentication flow(s) that are likely to be viable for the CDR regime can be the focus of ongoing discussions of the Information Security and Customer Experience working groups.

Decision To Be Made

What are the constraints and restrictions on the OAuth authentication flow options for the CDR regime.

Feedback Provided

The original proposal and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/open-banking/issues/035

This is a significant area of contention for the standards as there is significant tension between customer experience and security. As such, the feedback was highly disparate. This decision therefore is not definitive and articulates areas of solution that will not be pursued instead.

Decision For Approval

The Appendix for this decision outlines the options as they were articulated in the initial decision proposal. Based on feedback and subsequent review the following decisions indicate the options that will not be pursued:

- **The authentication flow will not be left to the discretion of the data provider**
  This decision was taken to facilitate a uniform and consistent customer experience across the regime, to ensure a consistent level of security and to minimise the number of variations that need to be accommodate by data consumers.
- **The Redirect model will not be used in isolation**
  Due to concerns around increased risk of phishing the Redirect model (option 1 as presented in the initial proposal) will not be supported. It should be noted, however, that in an app to app context option 2 and option 1 are essential the same process.
- **The flow will facilitate the data provider receiving direct communication from the initiating device**
  To allow for device identification and behavioural monitoring techniques the flow will facilitate direct communication from the initiating customer device without interception by the data consumer.

These decisions to not necessary predicate one of the remaining options 2 to 3 being implemented. The Information Security Working Group, in due course, will make a more specific decision.

Appendix

The following options were presented in the initial decision proposal.

Option 1 – Redirect

The Redirect flow is the standard sequence defined in the OAuth 2 standard (see Appendix for a link to the OAuth 2 standard). In this flow a data consumer opens a browser window with a link to page provided by the targeted data provider. This page requests a user identifier and a password from the customer that is used to authenticate the customer. The customer is then asked to complete authorisation by approving terms, data scopes, etc. On completion the page redirects to a known URL for the data consumer with appropriate tokens as part of the redirect message.

Commentary
As this model is the classic model for OAuth it is standards compliant and has good vendor support. Unfortunately it encourages behaviour that can lead to customers becoming more likely to succumb to phishing or spear phishing as this model requires a user to enter their banking credentials in an arbitrary web page provided to them by a third party with no real way to validate the authenticity of the page. If this flow were adopted for the standard it would be a tacit endorsement of this behaviour for customers. This would open customers to the risk of repeating this behaviour with a fake web page that captures their credentials.

Option 2 – Redirect With Known Channel Authentication

This flow is a variation to the standard Redirect flow to reduce the risk of increased phishing fraud by removing the step where authentication credentials are entered into an arbitrary web page popped by a third party application.

As far as the data consumer implementation is concerned this flow is identical to the Redirect flow. The key difference is that, instead of requesting the user identifier and password, the redirect page hosted by the data provider only requests the user identifier. The customer is then directed to a known channel to complete the authorisation. Once they have authenticated on an existing, known, interface the data provider then completes the redirection back to the data consumer.

This flow is effectively a hybrid between the Redirect flow and the Client Initiated Backchannel Authentication flow described in Option 3.

Commentary
As a variation to the Redirect flow this option allows data consumer implementations to be entirely standards compliant. For the data provider it is likely that this implementation will require customisation of their existing channels (similar to Option 3 and Option 4). The key advantages of this flow are:

- The user identifier, which is considered sensitive by many banks, is not shared with the data consumer
- The device the customer is using to initiate authorisation, which may be different to the device normally used for banking, is observable by the data provider. This assists in the

implementation of fraud detection techniques that rely on the tracking and finger printing of devices used by customers
- The implementation from a data consumer perspective is standard

Option 3 – CIBA

The Client Initiated Backchannel Authentication (CIBA) flow is a draft standard for authentication in an OAuth context that addresses some of the concerns of the Redirect flow (see Appendix A for a link to the CIBA standard).

Under this flow, the customer provides their user identifier to the data consumer who then requests authorisation to a data provider via a known back channel. The customer then authenticates using one of the data provider's existing channels. Once authorisation is complete the data provider calls communicates the result to the data consumer via the back channel (using polling or a registered callback).

Commentary
Like option 2, CIBA removes the social engineering risks of the Redirect flow. In most other respects it is equivalent to option 2 except that:
- The data consumer is required to know the customer's identifier which is considered sensitive information by many financial institutions
- The data provider has no interaction with the device hosting the data consumer's client. This means that they are unable to independently observe the device, which is a key pre-requisite for many fraud detection techniques based on device finger printing
- The data provider is unable to provide additional guidance during the initial the steps of authorisation that may be relevant to helping the customer complete authorisation using their existing channels

Option 4 – Entirely Decoupled

This flow would be similar to CIBA except that instead of a user identifier being captured by the data consumer in their user interface the customer would go to a known channel of the data provider where they would obtain a one-time password or code that they would then provide to the data consumer. This would mean that both the user identifier and the password are never exposed outside of the data provider's existing channels.

Commentary
This option is probably the most protective of the user's credential information. It may, however, be perceived by the customer to be more complicated. This would create friction in the user experience, with customers potentially abandoning services. As with CIBA, under this flow, the data provider has no interaction with the device hosting the data consumer's client. This means that they are unable to independently observe the device, which is a key pre-requisite for many fraud detection techniques.

Option 5 – Data Provider Discretion

The final option is to leave the selection of the authentication flow to the discretion of the data provider.

Commentary

While this option is the most flexible it creates a number specific problems that has been observed in other jurisdictions where an industry standard API has been established:

- It makes it difficult for a client ecosystem to get traction, as data consumers must build tailored support for each data provider.
- Customers have an inconsistent experience of the authorisation across multiple providers potentially reducing trust in the regime and subsequently adoption.
- Security is inconsistent across the ecosystem leading to a greater chance of a possible incident.