Data Standards Body

Technical Working Group

Decision 298 – Change Request 576 (Urgent)

Contact: Hemang Rathod, Mark Verstege

Publish Date: 11th April 2023

Decision Approved By Chair: 14th April 2023

Context

This decision relates to change request 576, which was consulted on in maintenance iteration 14 (MI14) of the Data Standards. The change requested has been separated from MI14 to be treated as urgent and give affected participants sufficient time to implement this change as soon as possible.

This change request was raised to highlight the following issue in the existing information security standards:

- As part of transitioning to FAPI 1.0, support for "Hybrid Flow" authentication flow will be phased out on the 10th of July 2023. "Authorization Code Flow" will then be required.
- Encryption of security tokens is not required for Authorization Code Flow as the they are exchanged via secure back channel. However, they are still required for Hybrid Flow.
- The standards currently state that ID token encryption must not be performed for Authorization Code Flow (in other words, it was originally intended for OIDC Hybrid Flow only)
- Participants raised the need to allow encryption of ID tokens when using Authorization Code Flow until the transition to FAPI 1.0 is complete. The main reason presented was that some Identity and Access Management vendors do not offer a way to conditionally ignore encryption for Authorization Code Flow at this stage. It is anticipated that all Data Holders using impacted vendors will encounter a similar issue.
- There was a desire from Data Holders to minimise disruption to ADRs and ensure their software products continue to work during the transition period.

Decision To Be Made

Define changes to information security standards to allow encryption of security tokens when Authorization Code Flow is used until transition to FAPI 1.0 is complete.

Feedback Provided

The original change request and the associated feedback can be found at:
https://github.com/ConsumerDataStandardsAustralia/standards-maintenance/issues/576

Overall, participants supported the change as it simplifies the transition to FAPI 1.0.

Various options were discussed, most of them requiring a change in the transition period that would take effect from the day the Chair approves the change along with a future date obligation change that aligns with completion of the FAPI 1.0 transition.

The change recommended for approval in this decision addresses the issue without impacting existing DH and ADR implementations. It does not require a transition phase as it and will continue to work post FAPI 1.0 adoption. Further details are provided in the Implementation Considerations section.

Decision For Approval

The following changes are being presented for approval:

Security Profile

To facilitate the transition period where OIDC Hybrid Flow is still supported, the following changes will be made in the Security Profile section:

1. Security Profile -> Tokens -> ID Token -> Authorization Code Flow requirements:

The description in this section will be updated to the following:

> For `response_type` "code", in accordance with **[FAPI-1.0-Advanced]**, ID Tokens **MUST** be signed when returned to a Data Recipient Software Product from the Token End Point.

The change above removes the statement that ID tokens must not be encrypted. Instead, it leaves this negotiation to the client and authorisation server according to the OpenID Connect Dynamic Client Registration specification. If the ADR client is only registering for the Authorization Code Flow, they can omit the ID Token encryption claims. This will ensure that the Data Holder authorisation server does not encrypt the ID token. Further, this remains in accordance with the FAPI 1.0 profile.

The requirement to apply ID token encryption for OIDC Hybrid Flow remains as it is a FAPI 1.0 Advanced profile requirement.

2. Security Profile -> Client Registration-> ID Token -> Registration Request using JWT:

Update the description of the following two fields:

Name	Required	Description
id_token_encrypted_response_alg	Conditional	JWE alg algorithm with which an id_token is to be encrypted. Required if OIDC Hybrid Flow (response_type "code id_token") is registered.
id_token_encrypted_response_enc	Conditional	JWE enc algorithm with which an id_token is to be encrypted. Required if OIDC Hybrid Flow (response_type "code id_token") is registered.

Note: The relevant DCR swagger specifications will be updated to reflect the above changes.

The change above relaxes the requirement for both fields to be Required. Instead, they are conditional based on the flows being presented to the Data Holder. If the Data Recipient wishes to only register for Authorisation Code Flow the two fields are not required. This would indicate to the Data Holder that ID token encryption is not to be performed according to the OpenID Connect Dynamic Client Registration specification:

> **id_token_encrypted_response_alg**
>
> OPTIONAL. JWE alg algorithm [JWA] REQUIRED for encrypting the ID Token issued to this Client. If this is requested, the response will be signed then encrypted, with the result being a Nested JWT, as defined in [JWT]. The default, if omitted, is that no encryption is performed.
>
> **id_token_encrypted_response_enc**
>
> OPTIONAL. JWE enc algorithm [JWA] REQUIRED for encrypting the ID Token issued to this Client. If id_token_encrypted_response_alg is specified, the default for this value is A128CBC-HS256. When id_token_encrypted_response_enc is included, id_token_encrypted_response_alg MUST also be provided.

Implementation Considerations

The changes will be applicable from the day the decision is approved by the Chair.

Further,

- Consideration was given to minimise impact to Data Holders that are phasing out the use of OIDC Hybrid Flow without creating a hard obligation date from the 10th of July 2023. This was important to ensure the ADR software products continued to operate.
- It also allows for ADRs to progressively update their software clients with each Data Holder as and when they are confident that the Data Holder properly supports the Authorization Code Flow. ID Token encryption will continue to apply until they update their client registration with the Data Holder to (a) request only the Authorization Code Flow and (b)

discontinue sending the ID token encryption claims (id_token_encrypted_response_alg, id_token_encrypted_response_enc).

- Careful consideration was given to ensure upstream standards were relied upon to make the transition non-customised and where vendors fully support open standards then they will work and align to the Consumer Data Standards.
- There is no forced retirement of OIDC Hybrid Flow after the 10th of July 2023. Data Holders may retire this authorisation flow after this date. If a Data Holder continues to support dual authorisation flows after this date, then the requirement to not perform ID token encryption for Authorization Code Flow applies and the Data Holder must ensure ID token encryption is no longer performed for Authorization Code Flow.
- Data Recipients indicate to Data Holders through client registration when they no longer with to receive encrypted ID tokens by omitting the ID token encryption claims in their registration request.