Australian Banking Association

DP 209 Consultation - FAPI 1.0

ABA members submit our views to the questions raised below:

1. General questions

(a) Should Refresh token expiry time be pegged to consent duration?

ABA members agree that security and business logic should not be coupled and previous introduction of this non-standard claim has caused increased complexity and customisation at the security layer.

ABA members believe that:

- This question is also related to refresh token cycling and for confidential clients operating under FAPI security profile it should be removed from Australian specifications. Please note: refresh token cycling is also being removed from FAPI 2 security profile.
- "refresh_token_expires_at" non-standard CDR claim should be made optional and, eventually decommissioned.
- Non-standard CDR refresh token introspection endpoint should also be decommissioned when "refresh_token_expires_at" and refresh token cycling are phased out.

(b) Should CDR authorisation input parameters be registered or otherwise moved out of the authorisation request object? If so, where should they be moved to for better Identity & Access Management (IAM) software supportability?

ABA members believe that “cdr_arrangement_id” non-standard CDR claim should not be registered and that they should be eventually replaced by “grant_id” parameter when Grant Management specification is adopted as a part of Decision Proposal 210 (transition to FAPI 2.0).

ABA members believe that “sharing_duration” non-standard CDR claim should not be registered and that it should be eventually moved out of the authorisation request object into authorization_details object when RAR specification is adopted as a part of Decision Proposal 210 (transition to FAPI 2.0).

(c) Should CDR token response parameters be registered or otherwise moved out of the parent token endpoint response JSON / ID token JWT? If so, where should they be moved to for better Identity & Access Management (IAM) software supportability?

ABA members believe that:

- “cdr_arrangement_id” non-standard CDR claim should be replaced by “grant_id” parameter when Grant Management specification is adopted as a part of Decision Proposal 210 (transition to FAPI 2.0).
- “sharing_expires_at” non-standard CDR claim should be decommissioned during the adoption of Rich Authorization Requests (RAR) and Grant Management specifications (after FAPI 1 final adoption, with or prior to FAPI 2 adoption).
- As per our answers above, "refresh_token_expires_at" non-standard CDR claim should be made optional and, eventually decommissioned together with refresh token cycling.

2. Phasing questions

(d) **Should the CDS explicitly define the request_uri must only be used once and cannot be replayed?**

ABA members agree that CDS should replace “SHOULD” with “MUST” to avoid request_uri replay after it has been used successfully (allowing reasonable time for state replication).

(e) Should the CDS explicitly define the upper lifetime of the PAR request_uri? If yes, what is the acceptable lifespan (e.g., 60 minutes)?

RFC 9126 (PAR) states that the request URI lifetime should be left “at the discretion of the authorization server but will typically be relatively short (e.g., between 5 and 600 seconds).”

Current CDS specification states that “the request URI MUST expire between 10 seconds and 90 seconds”.

ABA members believe, that both of these statements are sufficient and there is no need to change.

(f) **Should the Data Standards make requiring PAR mandatory for all Data Holders and Data Recipients?**

ABA members believe that PAR should be mandatory for all Data Holders and Data Recipients.

3. Phase 3

(g) Should JARM be supported when response_type is "code"?

Current FAPI 1 specification requires JARM for the code flow.

(h) Should the Data Standards *require* JARM when response_type is "code"?

Current FAPI 1 specification requires JARM for the code flow.

(i) Should the CDS mandate that the same "kid" is not allowed to be used by multiple keys within a JWKS?

ABA members believe that the same “kid” value MUST not be allowed to be used for multiple keys within a JWKS.

ABA members believe that the best outcome is delivered by adopting one of the options below:

Option 1. FAPI 1 final based on HYBRID flow and PKCE (RFC 9126).

- Phase 1 (optional FAPI 1 final) to allow Data Holders to complete their transition if they are ready.
  - Data Holders and Data Recipients SHOULD support FAPI1 final (current hybrid flow + PKCE)
  - Data Holders MUST support “PAR only”, and MUST ignore claims outside the request object
- Phase 2 (mandatory FAPI 1 final based on current hybrid flow) to complete ecosystem transition to FAPI 1 final.
  - Data Holders MUST support FAPI1 final (current hybrid flow + PKCE)
  - Data Recipients SHOULD support FAPI1 final (current hybrid flow + PKCE)
- Phase 3 (mandatory FAPI 1 final based on current hybrid flow) for data recipients.
  - Data Recipients MUST support FAPI1 final (current hybrid flow + PKCE)

Option 2. FAPI 1 final based on CODE flow, PKCE (RFC9126) and JARM.

- Phase 1 (optional FAPI 1 final) to allow Data Holders to complete their transition if they are ready.
  - Data Holders and Data Recipients SHOULD support new code flow with PKCE and JARM.

    - Data Holders MUST support PAR only, and MUST ignore claims outside the request object.
    - Data Holders MUST support current hybrid flow.
- Phase 2 (mandatory FAPI 1 final based on code flow) to complete ecosystem transition to FAPI 1 final.
    - Data Holders MUST support new code flow with PKCE and JARM.
    - Data Holders MUST support current hybrid flow.
    - Data Recipients SHOULD support new code flow with PKCE and JARM.
- Phase 3 (mandatory FAPI 1 final based on code flow) for data recipients.
    - Data Holders MUST NOT support current hybrid flow.
    - Data Recipients MUST support new code flow with PKCE and JARM.

Option 2 allows to simplify the flow **significantly** for all participants in one main release for each participant but it currently requires additional JARM support, which would require longer delivery timeframe.

Moving directly to FAPI 1 final allows Data Holders and their vendors to utilise the final version of the standards, fully certified products and OpenID Foundation Conformance test suite to assess security and interoperability. This also reduces delivery complexity and delivery team impacts (single main release for all participants with timing flexibility)

Re: Current Recommendation

ABA members agree that an independent security review should be conducted on each version of the Information Security profile before its deployment to production. The security review should cover all interactions between all participants of the CDR ecosystem (including register interactions, dynamic client registrations, non-standard cdr_arrangement revocation endpoint which has been implemented outside of the main security profile and etc.).

Conformance Testing

Given the majority of the changes discussed here are related to the security profile, ABA members strongly recommend to rely on official OpenID Foundation Conformance testing which covered FAPI 1 profile comprehensively. We also agree ACCC Conformance testing need to be updated for each phase to make sure it is not broken and it is available to participants prior to roll out.