ANZ Bank's Feedback on InfoSec profile 0.1.1

- Section 3.3 Registry

ANZ notes the feedback provided previously about the lack of detailed information on how the central registry / Certificate Authority will operate, and supports the other views expressed on the need to provide such detail, including the availability of CRL/JWKS endpoint to be hosted by the central registry.

ANZ recommend that the validity of CDR participants should be checked as frequently as practicable (every few seconds,) in order to ensure that data share happens only between permitted CDR participants. The unavailability of CRL/JWKS endpoints from this perspective directly impacts the ability for participants to share data between parties.

- Section 3. CDR Federation

ANZ support the feedback provided by CBA and recommends that there should be provision in the standards for Data Holders to deny or suspend access to a Data Recipient when there is a reasonable cause; such as in the instance of a security compromise or data breach at the Data recipient.

- Section 4.

With the revision to CDR scope to include Joint Account, there is now a need to provide further details on if and how OIDC Hybrid flow will be supported.

Where multiple people need to provide authorisation, should CIBA be the only supported method? If OIDC Hybrid flow is supported, would tokens be issued and consent held in an 'awaiting authorisation' state of some from, until multiple associated parties provide consent?

The standard should also provide clarity on expected handling in 'error' situations, for example what happens to Data receipt access when only one party approves consent?

- Section 5.

ANZ supports the proposed method for client authentication at Token endpoint using 'private_key_jwt' in line with our earlier feedback, and MTLS for HOK to bind accessToken to data recipient over a secure authenticated channel.

- Section 7.2

There is reference back to CDR rules on expiry of access token, which unlike Refresh Token doesn't offer any detail that can be referenced to assess the validity of access Token.

Is there an intent to specify access Token validity in the security profile, or should this be left to Data Holders discretion? ANZ recommends validity of access Tokens to be short lived (2-5mins) in line with good security practices.

- Section 7.3

The validity of a refresh token in alignment with maximum duration of consent can be up to 12 months. ANZ recommends that consideration be given to reauthorizing consent every 3 months along with notification to customer.

- Section 8.1

Section 7. 1 states “ID Token returned from Authorisation Endpoint MUST NOT contain any PI claims.” ANZ notes however that in section 8.1 it states “Data Holders MUST support the profile scope as described in section 5.4 of [OIDC].” This suggests the default profile claims be returned where the response type includes Id Token.

The [OIDC] 5.4 Default profile Claims, include PI claims (e.g. name, family_name, given_name, middle_name, etc…)

Section 8.1 should therefore also clarify if the expectation is not to return PI data on Id Token and supported claims as per decision proposal.

- Section 11 Transport Security

ANZ has concerns that cipher suites including DHE for key exchange are susceptible to attack. In line with our previous feedback, where use of DH cipher suites of FAPI R/W is considered, we strongly recommend that key size of over 2048 bit is mandated, to close any vulnerabilities associated with the downgrade of key size.

- Section 13 Endpoints –

The rules outline mentions there should be two way notification between data recipient and data holder on revocation of consent by consumer. There are no endpoint defined in standard to communicate consent revocation back to Data recipient where its revoked from Data Holder’s end?

Likewise there clarity needed on end point to notify Data recipient when the authorisation is fully approved in joint account scenario?

User info endpoint should provide more clarity on supported claims as first name, family name and given name in line with decision proposal.