CDR INFOSEC DRAFT STANDARD V0.1.1 REVIEW

NAB summary review and recommendations

1. Introduction

NAB welcomes the opportunity to collaborate and provide feedback to advance the CDR InfoSec draft standards v 0.1.1.

NAB has been an active participant during the compilation process of the InfoSec standards, collaborating with Data61 and Industry stakeholders on GitHub and providing public feedback to help shape Australia's Open Banking / CDR implementation. The security of consumer data is paramount and NAB has and will continue to voice security concerns and requirements to ensure the success and stability of the scheme.

We compliment the collaborative approach Data61 has adopted during the consultation processes and documentation of the InfoSec standard. Despite the delayed start, it has evolved quickly through engaged collaboration with stakeholders in the financial industry. However, there is disparity across the multiple technical industry streams and rules framework. NAB believes closer collaboration between the multiple parties will be beneficial to produce a consistent, easy-to-use and secure set of standards.

It is important to note that while the InfoSec standards so far have covered technical details for authentication, authorisation and secure communication, NAB has identified gaps in the security specifications, including:

- **Data Security: controls for sharing and securing Personally Identifiable Information (PII)**

  NAB has previously raised concerns on the rules' requirements to share PII information, including data used by banks to perform customer authentication. To protect customers and the Open Banking regime, the mandatory requirements for the sharing of PII information including consumer name and contact details must be removed. In the event where consumer information is compromised, the richness of this data could be maliciously used for criminal purposes such as identity takeover, resulting in financial fraud and losses.

  From a technical standpoint, and in support of the consumer data ownership, the security controls must ensure that in the circumstances where PII data is required to be shared, the consumer is in full control to select what attributes can be shared (or not). Also, appropriate access controls must be consistently enforced throughout the Data, InfoSec and UI/UX standards. (e.g. the data payload is encrypted in-transit and at-rest).

  Note: The ACCC rules outline issued in December 2018 adds a new concept of user pseudonym. NAB welcomes this addition and seeks clarification from the technical standards.

- **Consent Authorisation flows (OAUTH flow)**

  A security consideration in the OAUTH2 authorisation flows is the threat of Phishing Attacks. This threat is documented on RFC6819 (OAuth 2.0 Threat Model and Security Considerations) together with a set of recommended mitigating controls.

  Furthermore, NAB expects significant changes on the consent authorisation flows to cover requirements set on the ACCC rules outline (Dec 2018) for authorisation of joint-accounts, where individual authorisation may be required for each account holder / authoriser before consent is provided.

  Consent management APIs will need to be standardised by Data61 to avoid unnecessary friction within the scheme. This includes granting consent, consent revocation APIs, notification of consent revocation APIs, supporting processes and reporting.

  NAB expects Data61 to facilitate further industry group discussions on this topic to cement the authorisation framework and define a robust set of acceptable controls.

- **Security Non-Functional Requirements (SNFRs)**

  For Open Banking to succeed, security must not be treated as an after-thought. NAB believes that starting off activities early to define Security NFRs will help the industry and stakeholders to better understand security challenges and outline mitigating security controls. For example, these are some of the areas where NAB is seeking further clarification:

  - Data Integrity controls at the Data Holder and Data Recipient
  - Management and lifetime of credentials including keys, tokens and certificates
  - Logging and monitoring requirements

- **The Directory and Registration**

  The accreditation process and the related technical services to manage an accredited party is a core capability for the CDR / Open Banking scheme. NAB seeks further information on the proposed solution for the Directory and PKI services as well as the use-cases and integration between Data Recipients and Data Holders. Also, we expect these services (or a subset) to be available for consumption for the July 2019 – pilot release.

2. GitHub Feedback to the CDR InfoSec draft version 0.1.0

NAB has been actively collaborating and providing direct and public feedback to the iterative development of the CDR InfoSec standard via GitHub. The following is a summary of key feedback previously provided:

- **Issue #7 – Client Authentication - Private Key Support only**
  NAB is supportive of the use of Private_Key_JWT for client authentication at an application level. MTLS is required for network level authentication and certificates used for data encryption in-transit.

- **Issue #33 – Revocation of Consent**
  The CDR rules outline that consumers must be able to initiate the consent revocation process either via the Data Recipient or the Data Holder solution. NAB requires clarification on how notifications for revocation of consent will be performed and how it will be technically enforced. More specifically, no matter who the consumer notifies of their consent revocation, both Data Holder and Data Recipient systems must be in-sync in either scenario. There is an obligation on both Data Holder and Data Recipient to ensure no dormant consents are active:

  - When a consumer revokes consent through a Data Recipient's channel the Data Recipient is compelled by the rules to revoke consent using the appropriate Data Holder API (to be defined by Data 61). The concern is that tokens will be valid until formal notification of revocation is provided; even if consumers are not able to access their data, we must not leave loopholes within the scheme.

  - In the same regard, when a consumer revokes consent through a Data Holder channel – there is an obligation on the Data Holder to notify the Data Recipient that consent has been revoked through their implemented API (also, to be defined by Data 61). It is then expected the Data Recipient will perform the required data removal or de-identification processes to remain compliant.

- **Issue #35 – PS256 vs. RS256**
  NAB has proposed the adoption of the RS256 as per OIDC's default algorithm. Due to limited support, we believe that the restricted use of PSS will lead into interoperability issues, potentially requiring extensive testing and troubleshooting amongst stakeholders. A formal position is required.

- **Issue #47 – Consent API and definition**
  NAB is concerned with the lack of definition for consent management and we are seeking further information on guidelines such as for management of consents, data structures and notification services.

3. Feedback to the current CDR InfoSec draft version 0.1.1

NAB has performed a review of the latest published draft version and we have outlined our comments, questions and requirements.

- **Chapter 3.3 – Registry**
  As previously mentioned, NAB seeks further information on the proposed solution for the Directory and PKI services as well as the use-cases and integration between Data Recipients and Data Holders. NAB expects these services (or a subset) to be available for consumption for the July 2019 – pilot release.

- **Chapter 4.1 – OIDC Hybrid Flow**
  Further details are sought regarding the *request_uri* parameter (e.g. shall this parameter be ignored if present or if/when the Data Holder returns an error). NAB also seeks clarification on the reasoning behind the removal of this parameter.

- **Chapter 7.1 – ID Token**
  NAB is supportive of the signing and the encryption of ID Tokens containing PII information.

  Note: The ACCC rules outline from Dec 2018 introduces a concept of consumer's pseudonym. Clarification is required if Personally Identifiable Information (PII) will be shared with Data Recipients when a consumer pseudonym is in use. NAB opposes the sharing of PII data with Data Recipients.

- **Chapter 8.1 – Scopes**
  Section 5.4 of OIDC specifies many PII data elements as part of the profile scope. Given the content of section 8.2 (claims) it is our understanding that only the following data elements will be included in the profile scope: *name*, *given_name*, *family_name* and *updated_at*. A formal position is required.

  Further to section 7.1 (ID Token), it is our understanding that the ID Token returned from the Authorisation Endpoint can only contain *updated_at* element given that the rest of the profiles scope is considered PII. A formal position is required.

- **Chapter 8.2 – Claims**
  NAB is seeking clarification on the use of the *userinfo* endpoint to share PII data. Payload data submitted on this endpoint is not encrypted. Therefore, NAB expects the use of the ID Token submitted via the token endpoint if any PII data is required to be submitted. There are conflicting views between the security and data standards.

- **Chapter 12 – Requested Object**
  NAB is seeking a view of the full definition of the request object that is to be supplied at the authorisation endpoint.

  Furthermore, the example provided conflicts with the mandatory requirement on section 4.1, negating the support for *redirect_uri* parameter.

  Note: The URL link to section 14 does not seem to point to the correct location.

- **Chapter 14 – Consent**
  NAB seeks clarity on the validity period for refresh tokens versus the validity of consent (e.g. if the refresh token expires, can the DR re-use the consent ID in the new authorisation request?)

  In this scenario, we expect the consumer to undergo a new authorisation process and the issuing of a new consent id to gracefully close previously provided consents.