InfoSec Profile 0.0.3 Standards Review

Summary of Recommendations

Commonwealth Bank supports the way that Data61, the data standards body, has worked collaboratively with the financial services sector.

Protecting and securing consumer data and privacy is of paramount importance for the success of the Open Banking regime. Criminals can leverage vulnerabilities to steal sensitive information and defraud consumers in the absence of minimum cyber protections and the right processes and controls being in place. Phishing is a persistent threat that costs Australians and businesses millions of dollars each year. The Australian Cyber Security Centre (ACSC) 2017 Report[1] states that despite criminals' "increasing sophistication and technical ability, cybercriminals are also continuing to use simple targeting methods and tools to compromise victims. This is likely due to their ongoing success, low start-up costs and the high dividends produced".

Once personal details or credentials have been stolen through phishing, criminals can attempt to conduct a wide range of malicious activities including identity theft, impersonation, diversion of funds and even the reselling of that personal data.

The Bank has three significant concerns with the Draft Standards that are related to these cyber security risks:

1. Authentication Flows

Commonwealth Bank is of the firm view that consumers must not be encouraged to share data in a way that puts their finances or identity at risk. We maintain the position that a decoupled authentication flow is the most secure option for consumers and is our preferred authentication flow option. In a decoupled flow consumers provide authentication and a scope of the data sharing request directly to their bank.

The Standards do not currently mandate a truly decoupled approach. Rather, the Standards mandate the use of an Open ID Connect Hybrid (OIDC Hybrid) approach. The OIDC Hybrid requires the support of redirect flows from consumer devices. The Standards allow, but do not mandate, the use of the decoupled variant known as Client Initiated Back Channel Authentication (CIBA).

Commonwealth Bank believes the OIDC Hybrid approach, which features redirection from the Data Receiver's website or application to the Data Holder, unacceptably increases the phishing risk to consumers in the following ways:

- An attacker could gain access to a Data Receiver's application and change the redirect URL to a malicious website;

[1] Australian Cyber Security Centre (ACSC), 2017, 'Threat Report 2017'

- An attacker could create a fake website posing as the Data Holder where they harvest bank credentials; and/or
- It may encourage consumers to adopt insecure behaviour and trust redirect links purporting to be authentic URLs, to the point where they enter banking credentials.

Though not as secure as a truly decoupled approach, CIBA represents the most flexible approach and is our preferred alternative. We recommend the Standards provide further detail on the implementation of CIBA, including greater clarity regarding the unique customer identifiers that consumers will be required to provide to Data Receivers. It is not apparent in the current version of the Standards what data can be used as a unique customer identifier and how the unique customer identifier is confirmed by the Data Holder. We are extremely concerned that sensitive information (such as mobile or banking credentials) may be used for this purpose, exposing consumers to unnecessary risk and making them more attractive and lucrative targets to cyber criminals.

2. Directory and Certificate Revocation

The Standards currently provide very little detail of the specifications of the Directory and Certificate Authority (CA).

The Directory underpins the functioning of the Open Banking Regime since, if functioning properly, it will provide a source of truth for identifying legitimate participants in the Open Banking regime. According to the Standards, "Data Holders and Recipients must be registered as accredited entities in the Directory in order for them to participate as members of the CDR Federation".

The Certificate Authority (CA) manages and issues the security certificates and public keys used for secure communications between Data Holders and Receivers. It is central to establishing trust between the participants and therefore crucial to Open Banking. We expect a digital CA to be established as part of the Directory. The CA should provide public key infrastructure and a highly-available certificate revocation list (CRL).

Data Holders should be able to digitally confirm that a certificate being used to authenticate a Data Receiver request is valid and can be trusted by querying the CRL. Digital certificates may be invalidated if, for example, they have been stolen or otherwise compromised. The CRL will need to be polled by a Data Receiver and Data Holder as often as every five seconds in order to check for changes in the status of a certificate before sharing any consumer data.

If the CA's CRL should ever be unavailable, it will likely impact the overall operations of Open Banking, potentially causing a halt to data flows between parties. For example, CRL unavailability would prevent data flow between a Data Holder and a Data Receiver if one or both parties enforces a CRL check prior to establishing a connection. (We believe that enforcement of a CRL check before establishing a connection is aligned with best practice).

In order to provide the appropriate foundation Directory service, the Standards should detail the requirements and capabilities of a fully functioning Directory and Certificate Authority.

3. Client Authentication

To protect sensitive customer data, and in particular, to ensure that malicious third-parties cannot impersonate authorised entities, Commonwealth Bank's view is that mutual Transport Layer Security (mTLS) should be required for all back channel calls made between Data Holders and Data Receivers to authenticate both parties and establish secure channels for communication. We propose that both mutual TLS and Private Key JWTs should be the preferred client authentication method.

Once a Data Receiver is authenticated by a data Holder, an access token issued to the Data Receiver should be bound to a certificate. This ensures that an access token can only be sent through the connection or channel that has been mutually authenticated between Data Receiver and Data Holder. Binding a certificate to a token improves the effectiveness and levels of assurance in identity proofing controls.

Commonwealth Bank also wishes to make public two broader security concerns, which are not covered in the scope of the draft Standards but which are crucial when considering the security and integrity of the regime.

Ongoing Security Obligations of Data Receivers

Participants should be subject to cyber security requirements as part of the initial on-boarding and accreditation. This will help ensure the security of the ecosystem is maintained and that consumers can feel confident in sharing their data with trusted third parties.

Additionally, Data Receivers should be subject to specific ongoing minimum security standards. As part of these standards, Data Holders should be able to conduct security testing against Data Recipients and perform ongoing fraud and security monitoring as additional safeguards. The Data Holders have the scale and resources to be able to carry out these tests. In light of the global cyber skills shortage Data Recipients may not be able to, or may not wish to, develop these capabilities themselves. These steps are taken today as part of normal supplier partnership arrangements and are important in ensuring the appropriate security controls and protections are in place.

Commonwealth Bank proposes further discussion on how best to help consumers make educated decisions about with whom they share their data. One possibility is that Data Receivers are awarded publicly accessible ratings that correspond to a Data Receiver's security posture similar to the way that Canstar rates other consumer services.

Exemptions to Consent

Data Holders should be able to deny or terminate the access of a Data Receiver to customer information, if there is reasonable cause to do so. For instance, if a Data Holder reasonably believes a third party is victim to a data breach, or if the Data Receiver is identified in an anti-money laundering (AML) and counter terrorism funding register. The Bank expects the Rules to provide further clarity on the circumstances under which a Data Holder is exempt from supporting customer consent.

3. CDR Federation

3.1 Data Holder

No comments from Commonwealth Bank.

3.2 Data Recipient

No comments from Commonwealth Bank.

3.3 Directory

The CDR Federation section of the Standards include the Directory, which is a central point of discovery for both Data Holders and Data Recipients. The Standards note that the functionality of the Directory is still subject to change. There are limited details regarding the scope of the services and expectations of the Certificate Authority (CA) or the Directory.

Commonwealth Bank expects a CA to provide the ability for Data Holders to access a real time, highly-available certificate revocation list (CRL) to enable the immediate revocation of access when necessary. Data Holders should be able to confirm through that a certificate being used to authenticate a Data Receiver request is valid and can be trusted.

We seek clarity in the Standards regarding the details associated with the availability, or service levels, of a CRL and whether certificate checks will be required to be completed before allowing for authentication between Data Receivers and Data Holders. Our expectation is that the CRL will be polled by a Data Receiver as often as every five seconds in order to check for changes in the status of a certificate before sharing any consumer data. We suggest that availability of the CRL should exceed the service availability requirements expected of participants i.e. in excess of 99.5%. If the CA's CRL should ever be unavailable, it will likely impact the overall operations of Open Banking, potentially causing a halt to data flows between parties. For example, CRL unavailability would prevent data flow between a Data Holder and a Data Receiver if one or both parties enforces a CRL check prior to establishing a connection. (We believe that enforcement of a CRL check before establishing a connection is aligned with best practice).

If an OIDC Hybrid authentication flow is mandated (as discussed in section 4 below), a register of Data Receiver URLs should be kept. This will help mitigate the risk posed by 'URL redirect' attacks (criminal redirection of a consumer to a malicious webpage to steal credentials). This would be populated at the point of registration by a Data Receiver and be maintained by the Directory. It would allow the Data Receiver to check the validity of a website before redirecting a consumer.

4. Authentication Flows

We regard consumer data security as paramount. Commonwealth Bank maintains its position that a decoupled authentication flow is the most secure option for consumers and our preferred authentication flow option.

The Standards do not currently mandate a truly decoupled approach, but mandate that an Open ID Connect Hybrid (OIDC Hybrid) approach should be used. The OIDC Hybrid requires the support of redirect flows from consumer devices. The Standards also allow the voluntary use of a decoupled variant named Client Initiated Back Channel Authentication (CIBA).

Commonwealth Bank strongly opposes the use of the OIDC Hybrid approach, which features redirection from the Data Receiver's website or application to the Data Holder. We are concerned that this will increase the phishing risk to consumers in the following ways:

- An attacker could gain access to a Data Receiver's application and change the redirect URL to a malicious website;
- An attacker could create a fake website posing as the Data Holder where they harvest bank credentials; and/or
- It may encourage consumers to adopt insecure behaviour and trust redirect links purporting to be authentic URLs, to the point where they enter banking credentials.

Though not as secure as a truly decoupled approach, CIBA is our preferred alternative. We would like the Standards to provide further detail on the implementation of CIBA. In particular, the Standards should provide greater clarity regarding the unique customer identifiers, which consumers will be required to provide to Data Receivers. It is not clear in the current version of the Standards what can be used as a unique customer identifier and how the unique customer identifier is confirmed by the Data Holder. We strongly oppose the use of sensitive information (such as mobile or banking credentials) for this purpose. We are concerned that this would condition consumers to providing sensitive banking credentials or other information into a third-party website. The Commonwealth Bank cannot support practices that do not align with cyber hygiene best practice.

5. Client Authentication

5.1 private_key_JWT

Commonwealth Bank maintains its view that mutual TLS should be required for all backchannel calls made between Data Holders and Data Receivers. Signed private key JWTs are an alternative option for client authentication. However, as these JWTs should be sent via a mutually authenticated TLS channel, the use of private key JWT and TLS client authentication is preferred.

5.2 tls_client_auth

Commonwealth Bank supports the use of mutual TLS and private_key_JWT for client authentication and to enable the sending of certificate bound access tokens.

This ensures that an access token can only be sent through the connection or channel that has been mutually authenticated between Data Receiver and Data Holder. Binding a certificate to a token improves the effectiveness and levels of assurance in identity proofing controls. Certificate bound access tokens protect access to consumer data contained within the token from unauthorised third parties.

6. OIDC Client Types

No comments from Commonwealth Bank.

7. Tokens

7.1 ID Token

The Bank seeks greater clarification on the use of symmetric key encryption to support protection of ID Tokens. The Standards are not clear on whether symmetric direct key use is permitted to support the protection of ID Tokens or whether Data Holders will be expected to perform key wrapping (key encapsulation to securely transport a key) to protect the encryption key.

ID Tokens are the only tokens visible to Data Receivers (the other tokens i.e. the Refresh and Access Tokens are opaque and not visible to Data Receivers). Therefore Data Receivers should expose their JSON Web Key Set (JWKS) endpoint to share their public key with the Data Holder. This enables a Data Holder to encrypt the token with a certificate so that only the Data Receiver is able to decrypt it.

If the endpoint is not exposed, key wrapping techniques would have to be used to encrypt and protect the ID Token. Key wrapping is a less secure form of token protection as multiple vulnerabilities have been identified in this method e.g. padding oracle attacks[2], which criminals can use to decrypt cipher text.

Commonwealth Bank supports the use of PS256 and ES256 signing to support ID Tokens. We would like clarification to understand why RS256 is not referenced in the Standards. PS256 is a more recently developed algorithm and there is limited adoption when compared with RS256.

7.2 Access Token

Commonwealth Bank requires greater clarity in the Standards of the length of time an Access Token is valid. The Bank recommends that Access Tokens are as short lived as possible. Best practice depends on how long it takes a consumer to enter the credentials required but can be as short as two minutes.

7.3 Refresh Token

Commonwealth Bank supports the alignment of lifetime of Consent with the lifetime of Refresh Tokens. Either the Standards or the Rules should ensure this is technically enforced. We recommend consent re-authentication at least every three months.

[2] https://resources.infosecinstitute.com/padding-oracle-attack-2/#gref

8. Scopes and Claims

8.1 Scopes

Our comments on this section are captured in 8.2.

8.2 Claims

Greater clarity is required regarding the rationale behind the claims returned by the UserInfo endpoint and the necessity, or intended use of the data. The UserInfo endpoint can be used to return consumer data such as first name, family name, and given name.

The Standards only provide optional recommendations based on Open ID standards for the claims returned by the UserInfo endpoint. In the interests of consumer privacy, Data Holders should be able to elect not to return values for some claims requested from the user info endpoint.

The risk is particularly acute if the connection to this endpoint is not made through mutual TLS secured channels (as described in Section 5).

9. Identifiers and Subject Types

No comments from Commonwealth Bank.

10. Levels of Assurance (LoAs)

Commonwealth Bank supports the use of at least LoA 2 for Read Operations and LoA 3 for Write Operations.

We recommend further discussion to fully define LoA 3 and whether for example, logging into a mobile application and then using a One Time Code is considered two factor authentication, if presented on the same device. This is, in theory, a weaker form of two factor authentication. Best practice is currently for a second factor of authentication to be generated on a device independent to the one used to access the Data Receiver service.

10.1 Single Ordinal

Commonwealth Bank agrees with the specification that authentications with an Authentication Context Class Reference (ACR) of 'level 0' should not be used to authorise access to any resource of any monetary value.

10.2 Vector

10.2.1 Overview

Commonwealth Bank supports Vector of Trust (VoT) as an alternative way to way authenticate to ACR claims, to allow flexibility assuring authentications.

10.2.2 VoT Values

The Bank is supportive of these specifications.

11. Transaction Security

11.1 Ciphers

Commonwealth Bank supports the use of these ciphers as the minimum permissible key lengths. These align with industry best practice.

11.2 Mutual TLS

Specifically regarding Transaction Security, Commonwealth Bank strongly supports the use of mutual TLS for all Business-to-Business (B2B) service calls, or backchannel communication, between Data Recipient and Data Holder systems.

11.3 Holder of Key Mechanism

The Bank strongly supports mutual TLS being used as a Holder of Key Mechanism.

12. Request Object

No comments from Commonwealth Bank.

12.1 Holder Authorisation Server Vector of Trust (VoT)

For Read/Write operations Commonwealth Bank expects the Rules to provide further clarity on how the Data Holder should validate the guarantee that the correct degree of Vector of Trust (VoT) has been requested by Data Receivers.

12.2 Recipient Client using VoT

We are supportive of the Data Receiver being able to request a particular VoT while requesting consent to access consumer data.

13. Endpoints

13.1 OpenID Provider Configuration Endpoint

The Bank is supportive of this specification.

13.2 Authorisation Endpoint

The Bank is supportive of this specification.

13.3 Backchannel Authorisation Endpoint

The Bank supports the use of mutual TLS for Backchannel Authorisation Endpoint.

As stated in 5.1, we also strongly support the use of mutual TLS for all backchannel communication between Data Recipients and Data Holders.

13.4 Token Endpoint

No comments from Commonwealth Bank

13.5 UserInfo Endpoint

In order to protect consumer privacy, Data Holders should be able to limit the claims returned by UserInfo endpoint. The UserInfo endpoint can be used to return personal consumer information such as first name, family name, and given name

13.6 JWKS Endpoint

The Standards note that the JWKS Endpoint is directly impacted by the emerging requirements of the Directory and thus subject to change. As a consequence the Standards do not capture explicit details about how public keys are exposed.

Commonwealth Bank expects greater detail around the JWKS Endpoint in order to meet the July implementation date.

13.7 Introspection Endpoint

Commonwealth Bank supports the Standards which state that the Introspection endpoint can only be used to receive the expiry details of refresh tokens.

Commonwealth Bank welcomes the clarity provided in the Standards in connection with the use of private key signing for calls made to the Authorisation endpoint and Registration endpoint.

13.8 Revocation Endpoint

Commonwealth Bank expects the Standards to fully define the service availability expectations for revocation endpoints, since they are required to support real-time Certificate Revocation List (CRL) checks as described in Section 3.

13.9 Client Registration Endpoint

13.9.1 Request

No comments from Commonwealth Bank.

13.9.2 Response

No comments from Commonwealth Bank.

14. Consent

Commonwealth Bank notes that this approach deviates from the Open ID Financial-grade API (FAPI) standards. We understand that this approach may include the ConsentID within Claims made by a consumer, so as to be aligned with existing UK standards.

The approach described in the Standards appears to separate intent and consent. In the UK standards, consent is captured in the Claims provided – either returned in the UserInfo response or the ID Token.

Commonwealth Bank expects that if a consumer wanted to update consent, then the Data Holder would have to be informed. Refresh Token expiry should also be explicitly linked to the length of time that consent has been provided by a consumer.