CONSUMER DATA RIGHT SECURITY REVIEW

July 2019

FORTIAN
Security | Privacy | Risk

Fortian Pty Ltd
ABN: 33 164 874 695

1. CONTENTS

2. EXECUTIVE SUMMARY

THE CONSUMER DATA RIGHT (AND ITS FIRST IMPLEMENTATION IN OPEN BANKING) WILL GIVE AUSTRALIANS GREATER CONTROL OVER DATA HELD ABOUT THEM, EMPOWERING THEM TO CHOOSE TO SHARE THEIR DATA WITH TRUSTED RECIPIENTS. IN DOING SO, THE CONSUMER DATA RIGHT IS EXPECTED TO DELIVER A RANGE OF BENEFITS.

As with many opportunities in the digital space, the Consumer Data Right must be underpinned by a foundation of strong security. There is much at stake. Australians expect that their data is well protected and held to the most rigorous security standards. An information security incident could cause a loss of trust and confidence in the Open Banking ecosystem, thus eroding the economic benefits that the Consumer Data Right is expected to deliver.

Fortian has undertaken an independent security review of the Consumer Data Standard with a focus on the Information Security Profile, which are the technical standards underpinning the Consumer Data Right.

Overall, while several security issues have been identified throughout the review, the Information Security Profile is assessed as suitable for use in the initial implementation of the Consumer Data Right, due to the relatively low risk nature of read-only APIs and limited account types.

Many of the findings of this review have implications for the future development of the Consumer Data Standard as it is extended both in functionality to more complex use cases and to other industry sectors beyond banking. It is recommended that these issues be given early scrutiny given both the foundational importance of security as part of the Consumer Data Standard and the increasing cost and complexity of retrospectively implementing security controls.

2. EXECUTIVE SUMMARY CONT.

THREE KEY FINDINGS THAT SHOULD BE CONSIDERED IN FURTHER ITERATIONS OF THE CONSUMER DATA STANDARDS INCLUDE:

Interaction with security risk engines

Many organisations, particularly banks, have deployed security risk engines that can either block or alert on malicious behaviour. Under the Consumer Data Standard, there is currently no means for security risk engines to receive the data intelligence required, nor a means to respond that a security risk has been identified. This will become more critical if payments are introduced to the Consumer Data Standard.

Further security hardening

The Financial-grade API Working Group has introduced features that can further enhance security, such as Detached Signatures for API calls or the use of the JARM specification. These could become compelling security features, particularly when payment support is introduced.

Lack of fine-grained authorisation support

There is an overlap between the approach for fine-grained authorisation and coarse-grained authorisation. This overlap could lead to technical re-work, if future requirements for fine-grained authorisation arise. There may be utility in considering changing to a fine-grained model, to avoid the risk of re-work at a future time[1].

[1] Similar to the 'permissions' construct used in the UK Open Banking model.

3. INTRODUCTION

THE AUSTRALIAN GOVERNMENT HAS COMMITTED TO IMPLEMENTING THE CONSUMER DATA RIGHT (CDR) IN LINE WITH THE RECOMMENDATIONS OF THE REVIEW INTO OPEN BANKING IN AUSTRALIA.

The CDR will give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients for the purposes that they have authorised.

The CDR seeks to deliver a range of potential benefits. These include greatly improved access to customers' data in a usable form and the ability to direct its secure transfer to trusted third parties and, building on this, the development of better and more convenient products and services that are customised to customer needs.

The CDR is intended to apply sector by sector across the economy, beginning in the banking sector before expanding into the energy sector, followed by telecommunications.

Open Banking is the application of the CDR in the banking sector and will commence in July 2019 as part of a staged rollout, with basic product information to be made available voluntarily from 1 July 2019 and consumer data for mortgage accounts, credit and debit cards and deposit and transaction accounts by 1 February 2020.

The CDR is underpinned by the creation of common technical standards (known as the Consumer Data Standards (CDS)) upon which CDR participants would establish consent and share data securely. The CDS in turn uses open industry standards wherever possible, such as the Financial-Grade API (FAPI) and UK Open Banking–with the aim of minimising implementation costs for participants and ensuring greater security.

While the CDR has the potential to deliver significant benefits, it also has the potential, if not properly managed and implemented, to expose consumers to additional security and privacy risks. Maintaining a secure CDR ecosystem, beginning with a secure technical standard, is therefore vital to its success.

The Information Security Profile is the key technical artefact that that defines the security requirements in the CDS.

The purpose of this report is to undertake an independent review of the most recent release of the Information Security Profile with a view to highlighting potential security risks.

4. SECURITY REVIEW SCOPE

FORTIAN HAS BEEN COMMISSIONED TO UNDERTAKE AN INDEPENDENT SECURITY REVIEW OF THE PROPOSED CDS, SPECIFICALLY THE MOST RECENT RELEASE OF THE INFORMATION SECURITY PROFILE (VERSION 0.9.3).

The purpose of this review is to:

1. Provide confidence in the profile for use in the first phase of testing of the regime;
2. Identify areas of the profile that could give rise to specific security risks or vulnerabilities with recommendations on how these areas of deficiency can be remediated; and
3. Identify areas of unjustified divergence from open standards that should be remediated.

The specific scope of the review was to undertake activities that satisfy the objectives outlined above and deliver a report that provides:

- An expert assessment of the suitability of the Information Security Profile for use in the first phase of implementation of the CDR Regime;
- An expert assessment of the points of divergence with open standards that could introduce risk, along with the specific risks that have been identified;
- Specific risks or vulnerabilities associated with the Information Security Profile;
- Recommendations for how these risks and vulnerabilities can be mitigated; and
- Recommendations for further investigative work to be conducted to more fully address specific aspects of the Information Security Profile.

In addition to the defined scope outlined above, Data61 has requested a security review of open topics in the Consumer Data Standard which remain unresolved by the Data Standards Body and recommendations on these topics.

5. THREAT MODELLING

A KEY COMPONENT IN EXAMINING THE SUITABILITY OF THE INFORMATION SECURITY PROFILE FOR USE IN THE FIRST PHASE OF CDR IMPLEMENTATION IS THREAT MODELLING. THIS ENSURES THAT ALL ATTACK VECTORS ARE CONSIDERED TO ENSURE COMPLETENESS OF COVERAGE.

Threat modelling involves developing a comprehensive threat model that the Information Security Profile can be assessed against.

In assessing the Information Security Profile against this threat model, this review concludes that the Information Security Profile mitigates or manages these threats effectively.

It is important to note that:

- **The mitigation of some threats is outside the scope of the CDS (and therefore this review),** because these threats are focussed on external components or bodies. For example, some threats relate to the CDR register, the Customer Experience Stream or CDR Users; and
- **Some threats also have mitigations at the implementation level,** such as through secure development standards used by a Data Recipient or Data Holder.

THE KEY THREATS IDENTIFIED IN THIS REVIEW ARE SUMMARISED BELOW, WITH DETAILED THREAT MODELLING SET OUT IN **APPENDIX A**. REFERENCES SUCH AS **OBS-02** ARE REFERENCES TO RECOMMENDATIONS IN THIS REPORT THAT MITIGATE THESE THREATS.

Device Malware and Rogue Applications

There is no ability to control CDR User devices (such as laptops or phones). A compromised device enables the theft of user credentials and data related to the CDS. However:

- The use of the authorisation code hybrid flow (OBS-05) and signed request objects (OBS-07) prevent the theft of access or refresh tokens and alteration of authentication requests respectively;
- CDR Users are responsible for the security of their own devices (such as choosing (or not) to install anti-virus software), the scope of which is outside the CDS; and
- As discussed in OBS-02, allowing the passthrough of additional endpoint information (such as user agent and referrer headers) may allow a Data Holder to identify if a request is indicative of a compromised machine. However other controls that analyse and rank user behaviour are out of scope of the CDS but should be considered by Data Recipients and Data Holders alike.

5. THREAT MODELLING CONT.

Phishing

A CDR User can be tricked into entering credentials for a Data Holder in a location controlled by an attacker. This can be achieved through altering request objects (to redirect the user elsewhere on the internet) or through social engineering (tricking the user to navigate to a phishing site).

- Signed request objects (OBS-07) prevent the modification of response URLs, preventing an attacker from hijacking the authorisation flow and sending the user elsewhere on the internet, making it harder for an attacker to try and direct a user to a phishing site during sign-in.
- Banks have provided advice to their customers to never enter credentials on a website that they didn't navigate to themselves. The OpenID authentication flow used in this scheme changes this behaviour as users will be redirected to a site to log in. This is a banking ecosystem problem and potentially solved as the authentication options available to banking customers improve over time.
- As discussed above, allowing passthrough of additional endpoint information (such as User Agent and Referrer) may also aid in detecting if a phishing attack has occurred against a user, however other controls that analyse and rank user behaviour (which may also indicate phishing) are outside the scope of the CDS, but should be considered by Data Recipients and Data Holders alike.

Compromised Data Recipients or Data Holders

An attacker could use access to a compromised Data Recipient or Data Holder to attempt to access User data or access Data Holders.

- Both Data Recipients and Data Holders should ensure key material for MTLS certificates and keys for signing client JWTs are stored separately.
- Internal operational security for Data Recipients and Data Holders is out of scope of the security profile, however the accreditation scheme should include checks to ensure all parties have a baseline level of security capability.
- MTLS with HoK (OBS-07) and the private_key_jwt client authentication mechanisms (OBS-07) make it difficult for an attacker to attempt to forge authorisation requests, access tokens and refresh tokens.
- The CDS does not include data protection requirements, as it is not relevant to the specification, however Data Recipients and Data Holders will still be bound by legislative requirements for protecting and using User data (such as the Privacy Act 1988).

6. COMPARISON TO OPEN STANDARDS

THE CDS IS BASED ON AND USES THE FINANCIAL-GRADE API (FAPI) STANDARD AND HAS SOME ALIGNMENT TO UK OPEN BANKING. THE USE OF EXISTING STANDARDS AIMS TO MINIMISE IMPLEMENTATION COSTS FOR PARTICIPANTS AND LEVERAGES THE SCRUTINY ALREADY GIVEN TO THE SECURITY OF EXISTING MODELS.

This section identifies the similarities and points of divergence between the CDS, FAPI and UK Open Banking, with a focus on the security implications of those points of divergence. It should be noted that UK Open Banking uses the FAPI specification and is not a parallel or incompatible specification.

This review has identified points of divergence between the CDS, FAPI and UK Open Banking.

For the most part, these differences have either a positive security impact or no security impact. This is generally the case where the CDS adopts a more limited feature set than other standards, resulting in a smaller attack surface.

However, this review has identified several differences that have a negative security impact. These relate to fine grained permissioning and security hardening.

6. COMPARISON TO OPEN STANDARDS CONT.

Fine Grained Permissioning

UK Open Banking has devised a fine-grained permissioning scheme that has not yet been adopted in Australia. This gives UK consumers a high level of control over the consent they are granting over their data.

For example, in the UK, consumers may authorise access to their transaction history, but only for debit transactions within the last three months. In Australia, consumers can only authorise access to their entire transaction history or not at all.

The current approach by the CDR may present an increased security risk to Australian consumers. Should a data recipient be compromised, the amount of data exposed for each Australian consumer would potentially be greater than in the UK, consequently leading to an increased likelihood that such data will be useful for attacks such as identity theft.

Security Hardening

UK Open Banking supports higher risk scenarios, including payments and public clients. As a result, it includes security features such as CORS, JARM and Detached Signatures, which can all reduce data tampering risks.

This increased level of security hardening is unnecessary in the Australian environment, due to the lower risk of the current CDS profile. However, these features will become increasingly relevant as the CDS adopts higher risk APIs or chooses to allow use of public clients.

The detailed analysis of the differences between the CDS and industry standards, and their impact on security are set out in **Appendix B**.

7. REVIEW OF OPEN TOPICS

AS OF THE TIME OF WRITING, THERE WERE THREE OPEN TOPICS IN THE CDS WHICH REMAIN UNRESOLVED BY THE DATA STANDARDS BODY. THESE INCLUDE OPEN ITEMS ON AUTHENTICATION, RE-AUTHORISATION AND CONSENT. THIS REPORT REVIEWS AND PROVIDES DETAILED SECURITY FOCUSSED RECOMMENDATIONS ON EACH OPEN TOPIC IN **APPENDIX C**.

Note that "Authentication" as used in this document covers flows referred to as "Authorisation" in elements of the broader CDS design documentation.

These are summarised below:

AUTHENTICATION OPEN ITEMS

Standard redirect	**Adopt this flow.** This flow is established and resilient but there is an inherent phishing risk that should be managed through end-user education and product certification.
Redirect with One Time Password (OTP)	There are security risks associated with this flow due to the use of SMS as an OTP (noting that SMS does also have benefit due to its widespread use).
Redirect with known channel	This flow is not based on established protocols and would require more definition to provide security assurance.
Client initiated backchannel authentication (CIBA)	**Adopt this flow** once is it more established and once clearer use cases (and implementation details) are both defined, and security reviewed.
CDR specific decoupled	This is a non-standard approach that is not associated with common protocols. Further security assurance would be required.

7. REVIEW OF OPEN TOPICS CONT.

RE-AUTHORISATION OPEN ITEMS

Client initiated backchannel authentication (CIBA)	Per authentication open items, **adopt this flow** once is it more established and once clearer use cases (and implementation details) are both defined and security reviewed, and provided it is adopted for the authentication flow.
CDR specific mechanism (full authorisation flow)	**Adopt this flow,** until such time that CIBA is available.

CONSENT OPEN ITEMS

Defer inclusion of a Consent API until a requirement exists	**Defer until a requirement exists,** given difficulties in developing and certifying API products without clear specifications. With respect to future revisions of the CDS: Fine grained requirements may arise (e.g. when extending to other sectors), at which point there may be a higher level of complexity involved in introducing a Consent API due to semantic mismatch with the current specifications
Include a Consent API as an optional mechanism	
Include a Consent API as a mandatory mechanism	

8. REVIEW OF CDS

THIS REVIEW HAS EXAMINED VERSION 0.9.3 OF THE CDS AND THE INFORMATION SECURITY PROFILE AND OTHER ELEMENTS RELATED TO SECURITY. IT HAS IDENTIFIED 21 SECURITY-RELATED OBSERVATIONS, OF WHICH:

- Two have **Positive** security implications;
- Ten are **Neutral** and have neither a positive nor negative security implication, but are worth noting; and
- Nine are **Security Risks** and contain recommendations that aim to address the risk.

The detailed review of the CDS is contained in **Appendix D**.

Below is a list of all security risks identified along with recommendations to resolve them.

#	DESCRIPTION	RISK	RECOMMENDATION
OBS-01	**IP Address Forwarding**	Data Holders do not have a means to inform Data Recipients that a known bad IP address is in use.	It is recommended that the CDS use the 403 forbidden response code with an error payload detailing the reason for authorisation failure.
OBS-02	**Browser Metadata**	Data Holders do not receive browser metadata and therefore cannot block or alert on potential malicious activity, e.g. sudden change in browser type in a session hijack.	It is recommended that the CDS be extended to forward browser headers to the data holder. A solution could be to Base 64 encode all inbound headers and forward them to the data holder with a custom X-Originating-Agent header. This will permit banks to continue use of tools that detect malicious end-user behaviour.

8. REVIEW OF CDS CONT.

#	DESCRIPTION	RISK	RECOMMENDATION
OBS-05b	**JARM response types**	Response flow from the Data Holder is not digitally signed or encrypted, so it is exposed to tampering attacks.	Consider implementation of JARM. It is noted that JARM was introduced in October 2018, so may not have been specified in the original development of the CDS.
OBS-06	**Hybrid flow and phishing attacks**	Hybrid flow redirection approach introduces opportunity for phishing attacks.	It is recommended that: • Product certification must ensure that Request Objects are digitally signed, but also that there is no way to disable such a feature. This is important to note as many solution providers are building on top of existing, less secure OIDC implementations. • The CDR Register must restrict redirects to known endpoints that have been previously registered, and this must likewise be assured in product certification. • Stronger authentication mechanisms (e.g. FIDO) should be considered as another method to counter phishing risks.
OBS-09	**Consent – broad access to data**	Account authorisation gives access to all accounts, which therefore increases risks as all accounts are impacted in the event of a security incident arising.	It is recommended that the CDS be updated to note that the competitive space will find solutions for authorisation of individual accounts.

8. REVIEW OF CDS CONT.

#	DESCRIPTION	RISK	RECOMMENDATION
OBS-11	**Consent – rich access to data**	Account authorisation gives access to account detail that some banks may use in phone channels for customer authentication – a malicious or compromised Data Recipient may be used for attacks against the phone channel.	It is recommended that banks review the use of transaction data for end-user authentication at the phone channel. Banks that use make use of 'rich data' for phone-based authentication may choose to move to alternate approach in advance of Open Banking deployment.
OBS-16B	**Integrity control of APIs**	API responses are not signed, which exposes them to tampering attacks if transport security is bypassed.	Consider inclusion of Detached JWT Headers (x-jws-signature). This has been introduced by UK Open Banking as a standardised control for API response integrity.
OBS-17	**Scope and linkage to intent**	Scope definitions do not convey intent – Developers may therefore request more scopes/access than required.	The CDS should define scope labels that better convey intent. An example is: *'account.details.readonly'*
OBS-18	**Consent – non-repudiation**	Consumers can challenge their lodgement of consent, and the Data Recipient's right to use their data.	Guidance should be provided to Data Recipients to record the following each time consent events occur, including: Username (consumer's ID at the Data Recipient), Timestamp, IP, Consent Scopes.

9. APPENDIX A THREAT MODELLING

9.1 APPROACH & METHODOLOGY

THE FOLLOWING STEPS WERE UNDERTAKEN AS PART OF THE THREAT MODELLING METHODOLOGY:

1. Examination of each of the key actors in the ecosystem, with a focus on those that are in scope for the Information Security Profile;
2. Examination of how information is sent and received by each actor, including personal information and security credentials (including tokens);
3. Consideration of how each threat category may affect each of the actors and the data flows throughout the ecosystem;
4. Correlating these threats with the controls specified in the Information Security Profile; and
5. Developing observations and/or recommendations related to these relationships.

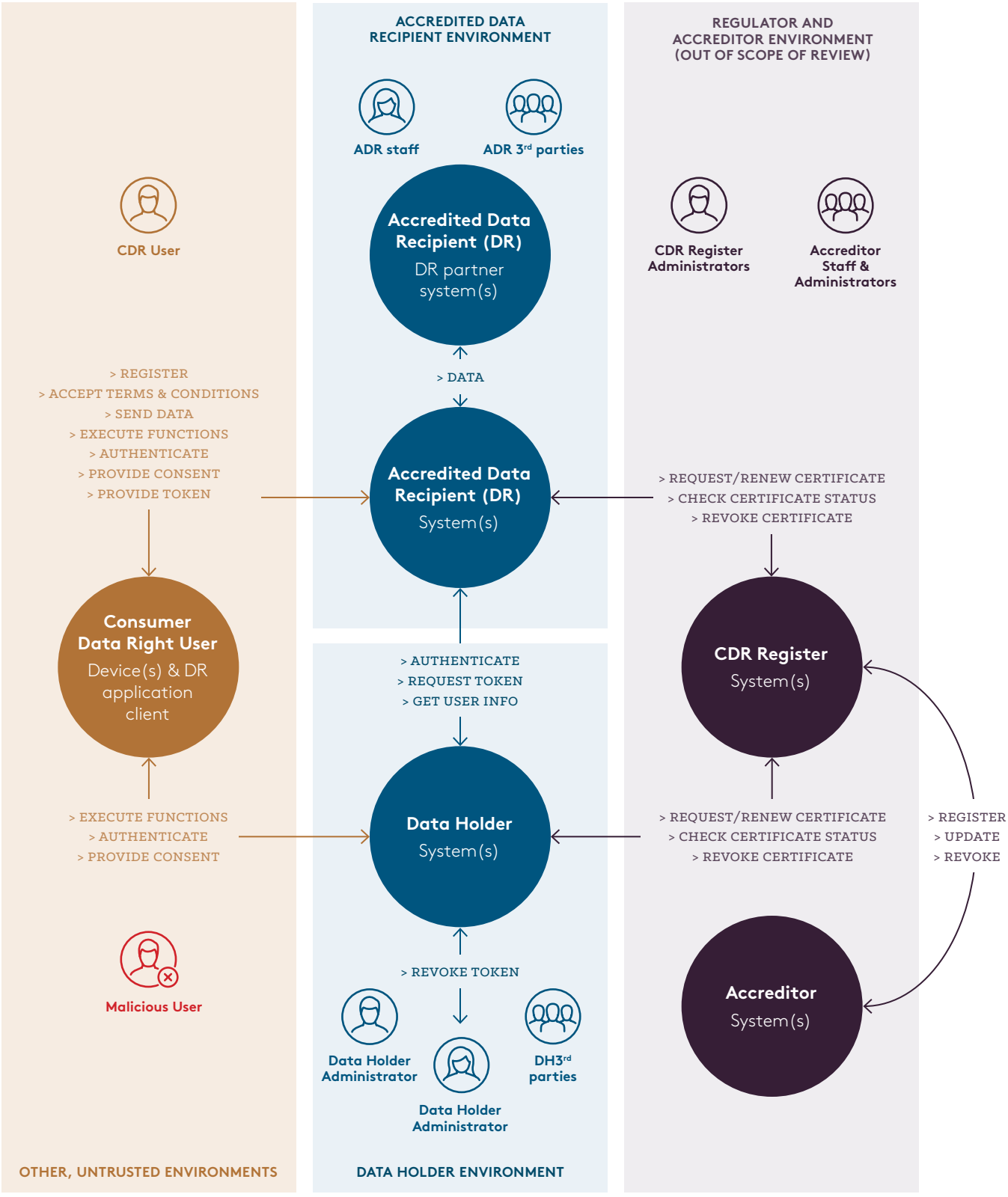
The threat framework used to conduct the threat modelling (and to ensure comprehensiveness) is the Microsoft STRIDE model, which focuses on the following threats:

THREAT	DESCRIPTION	DESIRED PROPERTY
Spoofing	Where a system, device or human actor impersonates another.	**Authenticity**
Tampering	Modification or sabotage.	**Integrity**
Repudiation	A dispute as to the authenticity of data sent between actors.	**Non-repudiability**
Information disclosure	Theft or loss of data where it can be obtained and/or read by an unintended party.	**Confidentiality**
Denial of Service	Where a system is made unavailable to users or unable to perform its assigned task.	**Availability**
Elevation of privilege	Where an actor obtains permissions within a system to perform unauthorised operations.	**Authorisation**

9. APPENDIX A - THREAT MODELLING CONT.

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY

THE FOLLOWING CONTEXT DIAGRAM AND EXPLANATORY TABLE SUMMARISES THE SYSTEMS, ACTORS AND DATA FLOWS IN THE OPEN BANKING ECOSYSTEM.



9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

#	NAME	DESCRIPTION
1	**CDR User**	• The end user or resource owner who provides consent for the Data Holder to provide their information (resource) to the Data Recipient. • The CDR User possess the device(s) used to participate in the ecosystem.
2	**Data Holder System**	• The Data Holder System processes and stores the CDR User's information (resources). They will make this information available to Data Recipients through the Open Banking API scheme.
3	**Data Recipient system**	• The Data Recipient maintains systems or applications to obtain the CDR User's information from the Data Holder. • The Data Recipient, depending on their architecture, could provide multiple ways for CDR Users to interact with their system such as mobile applications, single page applications, web applications and desktop applications. These different technologies may be susceptible to different types of threats.
4	**CDR Register**	• The ACCC as the governing body of the CDR will maintain a registry of Data Holder and Data Recipient actors and a centralised Public Key Infrastructure for use by the actor's systems. • **Note that this component is out of scope of this review.**
5	**Accreditor systems**	• The accreditation of entities in the CDR ecosystem may be supported by various information systems. • **Note that this component is out of scope of this review.**

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

Threat Assessment and Mitigants

The following sections describe by actor (Data Recipient, Data Holder, CDR User), threats considered for each threat category (STRIDE) as well as threat mitigation measures including where they are considered in this review.

Data Recipient

STRIDE CATEGORY	DATA RECIPIENT THREAT	COMMENTS	REFERENCE
Spoofing	Data Recipient is socially engineered into directing legitimate users to a fake/ malicious Data Holder (e.g. Data Recipient is tricked to set the Data Holder's redirection URL to a website they control).	Due to the CDR's closed ecosystem this information is provided only by the CDR register rather than any out of band mechanism.	Addressed in the CDR Register design (outside the scope of this review).
	Malicious/compromised Data Recipient attempts to forge an access token in order to gain access to additional user's data.	Entropy requirements for Data Holder authentication responses make token guessing impractical. Token signing by Data Holder prevents forged tokens from being accepted.	Entropy requirements are specified in FAPI1 5.2.2 (outside the scope of this review). Token signing is specified in FAPI2 and OIDC 6.3 (outside the scope of this review).
	Session is hijacked between the CDR User and Data Recipient - Intermediary is now sending traffic.	The standard does not define any security controls related to sudden change in IPs, User Agents etc. It is recommended that additional endpoint metadata be forwarded to the Data Holder for risk scoring.	Recommendations in OBS-02 address this threat.
	Key material used for a Data Recipient's CDR CA hierarchy certificates (MTLS) stolen, allowing an attacker to impersonate the Data Recipient for connections to Data Holders.	Signing keys for private_key_jwt's are also required to successfully impersonate a Data Recipient to a Data Holder. These should not be stored on the same systems as the MTLS key material. Security design and secure implementation of Data Recipient systems should be required through the Data Recipient certification process.	This threat must be addressed in Data Recipient system implementation and needs coverage in the Data Recipient certification process (outside the scope of this review).

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

STRIDE CATEGORY	DATA RECIPIENT THREAT	COMMENTS	REFERENCE
Tampering	Attacker at Data Recipient attempts to modify access/ refresh tokens to change what they can access.	Token signing by the Data Holder prevents modified tokens from being accepted. This mechanism is provided by the OpenID Connect standard as extended by FAPI.	Addressed in OIDC 6.3 (outside the scope of this review).
	Attacker is modifying parameters in client-side redirects - Examples would be redirect_uri, scope, nonce, state etc.	These general risks in OpenID Connect are addressed in the FAPI-RW profile, which moves these parameters into the signed Request Object as noted in OBS-06.	Noted in OBS-06.
Repudiation	Consumer claims they have not granted access to data.	Access grants are actioned through the Data Holder rather than the Data Recipient. While beyond the scope of this review we recommend these events should be logged at the Data Recipient for auditability as noted in OBS-18.	Recommendations in OBS-18 address this threat.
Information Disclosure	Leaked access or refresh tokens, which can then be used to access customer data.	Tokens are bound to the intended bearer's CDR Register-issued MTLS certificate via HoK, preventing reuse by other parties.	Noted in OBS-07.
	Leaked identifiers (such as URI components stored in logs).	Where identifiers are used in URLs, they are required to be arbitrary and carry no inherent meaning as specified in CDS section "ID Permanence". If full messages are logged then PI may be retained, appropriate design and implementation of Data Recipient systems should be required through the Data Recipient certification process.	Identifier arbitrariness is addressed in CDS section "ID Permanence". Logging detail is outside the scope of this review.
	Interception of CDR User data between CDR User and Data Recipient.	TLS requirements inherited from the FAPI specification provide best-practice mitigation of transport level data interception.	FAPI1 7.1 (outside the scope of this review).

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

STRIDE CATEGORY	DATA RECIPIENT THREAT	COMMENTS	REFERENCE
Denial of Service	DoS attacks against Data Recipient systems.	The Data Recipient is expected to have availability and resiliency responsibilities outside of this particular standard and the scheme as mandated through other regulating entities.	This should be addressed in the system NFRs (outside the scope of this review).
Denial of Service	Data Holder rejection of end-user requests based on risk scoring is indistinguishable to the Data Recipient from authentication failure or application errors.	Support for richer error reporting is required for Data Recipients to adequately manage system availability and end-user error reporting.	Noted in OBS-01. Recognised in current draft CDS under "Known Issues".
Elevation of Privilege	Data Recipient attempts to access data not consented to by the user.	Tokens are scoped to their intended actions and signed by Data Holder so that they can't be modified.	Token scoping is specified in OAUTH2 3.3 (outside the scope of this review). Token signing noted in OBS-07.

Data Holder

STRIDE CATEGORY	DATA HOLDER THREATS	COMMENTS	REFERENCE
Spoofing	Attacker attempts to pretend to be a Data Recipient to gain access to customer information (i.e. a fake 'budget app' is trying to convince users it is part of the ecosystem).	A spoofed Data Recipient will not be part of the ecosystem without registering its keys into the CDR Register. This stops it being part of the 'ecosystem'.	These is addressed in the CDR Register design (outside the scope of this review).
Spoofing	Attacker attempts to masquerade as a CDR User in order to get access to customer data.	Required assurance levels of CDR User authentication by a Data Holder is specified in the CDS by reference to the Trusted Digital Identity Framework.	Controlled by strength of Data Holder authentication process of CDR Users (outside the scope of this review).
Spoofing	Identity provider mix-up attack.	Use of OIDC Hybrid Flow includes Data Holder issuer identifier in returned code which is used by Data Recipient to find the valid Data Holder's token endpoint.	Noted in OBS-05.

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

STRIDE CATEGORY	DATA HOLDER THREATS	COMMENTS	REFERENCE
Tampering	No finding pertinent to the Security Profile.		
Repudiation	Consumer claims they have not granted access to data.	While authentication and logging of access grants is beyond the scope of this review, we recommend these events should be logged at the Data Holder for auditability as noted in OBS-18.	Recommendations in OBS-18 address this threat.
Information Disclosure	Leaked access or refresh tokens, which can then be used to access customer data.	Tokens are bound to the intended bearer's CDR Register-issued MTLS certificate via HoK, preventing reuse by other parties.	Noted in OBS-07.
	Leaked identifiers (such as URL components stored in logs).	Where identifiers are used in URLs, they are required to be arbitrary and carry no inherent meaning as specified in CDS section "ID Permanence". If full messages are logged then personal information may be retained, appropriate design and implementation of Data Holder systems should be required through the Data Holder certification process.	Addressed in CDS section "ID Permanence". Logging detail is outside the scope of this review.
	Leakage or loss of customer data.	The Data Holder is expected to have data protection responsibilities under the scheme outside of this particular standard as well as mandated through other regulating entities.	This threat must be addressed in Data Holder system implementation and needs coverage in the Data Holder certification process (outside the scope of this review).
	Data Holder Server Certificate Lost, allowing MITM against Data Holder/Data Recipient traffic.	private_key_jwt signing prevents active tampering with data, but CDR User data can be collected in transit. Security design and secure implementation of Data Holder systems should be required through the Data Holder certification process.	Signing noted in OBS-07. Data Holder implementation certification is outside the scope of this review.

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

STRIDE CATEGORY	DATA HOLDER THREATS	COMMENTS	REFERENCE
Denial of Service	DoS attacks against Data Holder systems.	The Data Holder is expected to have availability and resiliency responsibilities outside of this particular standard and the scheme as mandated through other regulating entities.	This should be addressed in the system non-functional requirements (outside the scope of this review).
Elevation of Privilege	Attacker (man-in-the-browser or similar) attempts to modify consents as the user submits them.	The CDS requires authentication at LoA 3/CL2 (i.e.: requiring MFA) for write operations, but a compromised CDR User device can modify consents transparently to the user.	Authentication level requirements are specified in CDS section "Levels of Assurance (LoAs)". CDR User endpoint security is outside the scope of this review.
	Attacker with some access to Data Holder systems is able to gain additional access or move laterally to other Data Holder systems to gain access to the data of CDR Users.	There is a range of general security practice guidance the Data Holder could consider when building their applications. In this instance, the OWASP guidance around building access control as well as ensuring security testing occurs. The Data Holder is expected to have data protection responsibilities under the scheme outside of this particular standard as well as mandated through other regulating entities.	This threat must be addressed in Data Holder system implementation and needs coverage in the Data Holder certification process (outside the scope of this review).

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

Customer (end-user)

STRIDE CATEGORY	CUSTOMER THREATS	COMMENTS	REFERENCE
Spoofing	Phishing.	Partly controlled with MFA for write transactions. User education with respect to Data Recipients and Register-provided list of Data Recipients.	Authentication level requirements and user education are outside the scope of this review.
Spoofing	Inadvertent installation or use of fraudulent Data Recipient application or website.	Partly controlled with MFA for write transactions. User education with respect to Data Recipients and Register-provided list of Data Recipients.	Authentication level requirements and user education are outside the scope of this review.
Spoofing	Authorisation request parameter injection attack. (Compromised browser attempts to modify or inject authorisation request parameters).	Use of signed request object prevents tampering with parameters.	Request object content and validation is specified in FAPI2 8.4.2 (outside the scope of this review).
Spoofing	Attacker impersonates a CDR User or their device (stolen credentials/credential stuffing).	There is a range of general security practice guidance the Data Recipient and ADH should consider when building their applications. In this instance, the OWASP guidance around building authentication and session management.	Data Holder and Data Recipient system implementation needs coverage in the participant certification process (outside the scope of this review).
Tampering	Malware has access to consumer data presented on the device.	Similar to existing systems - endpoint (desktop/mobile device) security.	CDR User endpoint security is outside the scope of this review.
Repudiation	No finding pertinent to the Security Profile.		

9. APPENDIX A - THREAT MODELLING

9.1.1 OPEN BANKING ECOSYSTEM SUMMARY CONT.

STRIDE CATEGORY	CUSTOMER THREATS	COMMENTS	REFERENCE
Information Disclosure	Auth code stolen from browser or mobile device.	AppSec guidance to Data Recipients.	Data Holder and Data Recipient system implementation needs coverage in the participant certification process (outside the scope of this review).
	ID token stolen from browser or mobile device.	Attacker could gain access to data in ID token, but by itself an ID token does not represent authentication, and Access Tokens are MTLS HoK-bound.	Token MTLS HoK binding noted in OBS-07. Use of distinct ID and Access tokens is specified in OAuth 2 (outside the scope of this review).
	Data Recipient retains CDR User data beyond the consent period granted.	The Data Recipient is expected to have responsibilities to honour CDR User expectations for data retention under the scheme outside of this particular standard as well as mandated through other regulating entities.	This must be addressed in Data Recipient systems and process implementation and needs coverage in the Data Recipient certification process (outside the scope of this review).
	More CDR User data is disclosed to a Data Recipient than is required to meet a specific product need.	Lack of a fine-grained permission scheme currently requires Data Holders to provide broad, rich, and deep access to CDR User data without filtering, which will result in more data being provided to Data Recipients than may be required for some product scenarios.	Noted in OBS-09, OBS-10, and OBS-11. Recommendations in OBS-09 and OBS-11 address some consequences of this design. Policy/legislative requirements are outside the scope of this review.
Denial of Service	No finding pertinent to the Security Profile.		
Elevation of Privilege	No finding pertinent to the Security Profile.		

10. APPENDIX B DETAILED COMPARISON BETWEEN THE CDS AND INDUSTRY STANDARDS

10.1 FAPI READ-WRITE PROFILE

THE TABLE BELOW COMPARES THE CDS AGAINST THE FAPI-RW PROFILE.

ELEMENT	FAPI-RW	CDS (V 0.9.3)	SECURITY IMPLICATIONS OF DIFFERENTIAL
Authentication Flow	• Hybrid flow. • CIBA flow.	• Hybrid flow with restricted grant types. • Proposal for CIBA. • Proposal for custom flows.	CDS is adopting the Hybrid flow, but with proposal for CIBA and alternate custom flow. **Security can be degraded with some of the CDS proposals.** This is addressed in Appendix C – Detailed Review of Open Topics under "Authentication Flows".
Authentication Flow (Hybrid)	• Hybrid flow. • JARM profile introduced as separate FAPI specification (Oct 17, 2018).	• Hybrid flow with restricted grant types.	Hybrid flow - CDS has restricted the options available to implementers, which **reduces the attack surface and therefore has a positive security impact**. However, CDS has not adopted the additional security controls that JARM makes available for Hybrid flow responses (JARM may have been defined only after initial CDS development).

10. APPENDIX B - DETAILED COMPARISON BETWEEN THE CDS AND INDUSTRY STANDARDS

10.1 FAPI READ-WRITE PROFILE CONT.

ELEMENT	FAPI-RW	CDS (V 0.9.3)	SECURITY IMPLICATIONS OF DIFFERENTIAL
Client Types	• Confidential client support. • Public client support.	• Confidential client support.	CDS has opted not to support public clients. **This reduces the potential attack surface and therefore has a positive security impact.**
Client Authentication	• MTLS with *private_key_jwt* client authentication.	• MTLS with *private_key_jwt* client authentication.	Parity with the FAPI-RW standard.
End-user identification	• Content of subject identifiers is undefined and may identify account or customer numbers. • Provision of profile information (name, gender, &c) is optional.	• Subject identifiers are required to be *PPIDs* (Pairwise Pseudonymous). • Provision of profile information (name, gender, &c) is required. • Requires LoA exchange.	CDS requires extra claim elements to satisfy end user identification. The result is that the data recipient is guaranteed to know the LoA at which the CDR User is authenticated. **No significant security impacts.**
Transaction Security	• Adopts MTLS with HoK.	• Adopts MTLS with HoK.	Parity with the FAPI-RW standard.
Reauthorisation	• CIBA support.	• Proposes to adopt CIBA • Proposes a custom defined flow	Addressed in Appendix C – Detailed Review of Open Topics under "Re-Authorisation".

10.2 UK OPEN BANKING

THE TABLE BELOW COMPARES THE CDS AGAINST UK OPEN BANKING.

ELEMENT	UK OPEN BANKING	CDS (V 0.9.3)	SECURITY IMPLICATIONS OF DIFFERENTIAL
Coarse-grained authorisation	• Limited scopes: *account*, *payment*.	• Multiple additional scopes: *bank_basic_accounts*, *bank_detailed_accounts*, *bank_transactions*, *bank_payees* (and more).	The CDS only supports a coarse-grained approach to authorisation. This allows for increased disclosure of user financial information to data recipients. **At a high level, this potentially increases the risk that the data can be exploited.** See "OBS-11 Consent – rich access to data" for an example.
Fine-grained authorisation	• The UK provides 21 permissions *(ReadOffers, ReadTrannsactionsCredit* etc.) and the ability to constrain the duration available for a transaction history.	• Not implemented.	
Payment authorisation	• The UK defines a consent API based on the FAPI Lodging Intent pattern.	• Not implemented. Not required at this stage (i.e. no support for payments).	n/a
Consent duration	• A consent duration that is associated with each set of permission grants.	• A single consent duration, defined as a custom claim.	At initial request, the claim is exchanged within the Request Object payload which is a FAPI pattern and the object is signed and encrypted. At reauthorisation a custom endpoint is called to extend consent. These are standard patterns which have been widely reviewed for security and which do not have security concerns. **No negative security impacts.**

10. APPENDIX B - DETAILED COMPARISON BETWEEN THE CDS AND INDUSTRY STANDARDS

10.2 UK OPEN BANKING CONT.

THE TABLE BELOW COMPARES THE CDS AGAINST UK OPEN BANKING.

ELEMENT	UK OPEN BANKING	CDS (V 0.9.3)	SECURITY IMPLICATIONS OF DIFFERENTIAL
Headers	• Cross Origin Request Sharing (CORS) headers to be used to give API access to JS clients (based on FAPI-Read profile).	Not specified.	CORS is browser-side control that prevents malicious JavaScript from communicating across domains. Using CORS and specifying implementation guidance in future revisions of the CDS can reduce risk if additional client types become supported. **This currently has no negative security impact, but may need to be specified in future if browser-side access is required, at which point cross-domain security attacks can emerge.**
	• Detached JSON Signatures are to be used for non-repudiations.	Not specified.	Detached Signatures (x-jws-signature) may not have been specified as the CDS currently supports low risk, read only APIs. Signatures can be used to ensure API responses have not being tampered with. **This has a negative security impact as there is no ability for detecting tampering of API responses.** See "OBS-16B Integrity control of APIs" for an example.

11. APPENDIX C DETAILED REVIEW OF OPEN TOPICS

11.1 AUTHENTICATION FLOWS

THERE ARE FIVE AUTHENTICATION FLOWS STILL UNDER CONSIDERATION. THESE ARE SET OUT BELOW, ALONG WITH COMMENTS / ANALYSIS AND RECOMMENDATIONS.

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Standard Redirect Flow: *Username and password are captured in a redirected web page and consent is then obtained in the redirected web page.*	• This is the standard authentication flow, which is well understood and widely used. • OpenID Connect (OIDC) redirection can present a phishing risk, which is inherent to the use of OIDC redirect protocols. • This is partly mitigated by the FAPI-RW, specifically the *redirect _uri* is digitally signed as noted in OBS-06.	**Adopt this flow.** • This flow is established and resilient, and with known patterns to support various implementation scenarios that will arise. • The flow is a traditional submission of credentials, which is considered relatively low friction for end-users. • There is an inherent security risk from phishing which is acknowledged, and which could be reduced through end-user education and product certification.

11. APPENDIX C - DETAILED REVIEW OF OPEN TOPICS

11.1 AUTHENTICATION FLOWS CONT.

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Redirect with OTP Flow: *Username is captured in a redirected page. The Data Holder then provides a one-time password via another channel, which is then captured in the redirected page to authenticate the customer. Consent is then obtained in that same web page.*	• This is a variation of the standard flow, with the user being prompted for a username and OTP token. • The flow does not require any password exchange, which retains its use solely within the data holder. • This flow presents a user experience, which is different to the bank logon. • It increases the work effort for any malicious actor, as a spoofing of the user experience (phishing-type attack) must also generate an OTP. • **This flow does have issues largely relating to the likelihood that SMS would be used for the OTP.** • The use of SMS increases the risk of 'localised attacks', which are attacks by people with physical proximity to the user – for example - it is possible for someone with physical proximity to the user to gain access to both a username and an SMS token (displayed on the lock screen on many phones). • Many companies also support only password and SMS authenticator factors, which leads to a scenario where either SMS is used to access all APIs, or SMS is used for read-only APIs and a password step-up for write APIs. • SMS is vulnerable to attacks such as SIM porting (albeit, this will affect other options too, which will likely use SMS for step-up authentication).	• While there are known risks related to use of SMS as a delivery mechanism for One Time Passwords, these risks are understood and currently accepted in the banking sector where SMS OTP is already in wide use. • Migrating to more secure OTP delivery mechanisms would reduce the risks associated with this flow. • Notification to CDR Users of newly authorised Data Recipients through some other channel (e.g.: along with regular banking statements) will also mitigate risks associated with using SMS OTP to enable ongoing access to data.

11. APPENDIX C - DETAILED REVIEW OF OPEN TOPICS

11.1 AUTHENTICATION FLOWS CONT.

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Redirect with Known Channel: *Username is captured in a redirected page. Customer then proceeds to a known digital channel, authenticates and provides consent.*	• This intent of this flow is to direct the user to a known channel, and only that channel is responsible for both username and password capture (unlike other flows, even a username is not needed outside of the Data Holder environment). • The flow involves authentication at the known channel and then authorisation of the involved party. • The flow's intent is to serve all authentication and authorisation directly from a trusted channel. • However, the flow is not based on established protocols, which will could lead to difficulties in implementation. • Edge cases that need addressing could include session timeouts (multiple browser windows are involved), securely acknowledging authorisation back to the requestor and potentially challenging scenarios (such as sending acknowledge from a web known channel back to a mobile app solution provider).	• This flow is not based on established protocols and would require more definition to provide security assurance.

11. APPENDIX C - DETAILED REVIEW OF OPEN TOPICS

11.1 AUTHENTICATION FLOWS CONT.

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Client Initiated Backchannel Authentication (CIBA): *A decoupled and asynchronous authentication flow that is defined by FAPI.*	• With this flow, a screen will be presented for entry of a username. • This will trigger a message to the Data Holder to request user authentication. The mode of authentication is flexible, so it can be a mobile push message, scanning of a QR code or email with a link. • CIBA is an innovative protocol and enables a range of innovative authentication mechanisms. • CIBA should be considered an emerging protocol. The latest standard is in draft and published in January 2019. It is effectively a toolkit, so the security posture is highly dependent on implementation details.	**Recommend adopting this flow, once it is considered more established**, and once clearer use cases (and therefore implementation details) are defined and security reviewed.
CDR Specific Decoupled: *A decoupled flow proposed by a community member where a one-time identifier is obtained from a known digital channel and then provided to the data recipient with consent being completed afterwards in an experience provided by the Data Holder.*	• This is a decoupled flow, whereby a one-time identifier is obtained from a known channel and provided to the Data Recipient with consent being completed afterward in an experience provided by the Data Holder. • This is the only flow that requires no sharing of the username with the Data Recipient. The mechanisms that support this flow will need to be defined.	• It is a non-standard approach that is not associated with common protocols.

11.2 RE-AUTHORISATION

CONSENT IS GRANTED FOR A TIME DURATION. RE-AUTHORISATION IS REQUIRED TO EXTEND CONSENT BEFORE IT EXPIRES. THERE ARE TWO OPTIONS FOR REAUTHORISATION CURRENTLY UNDER CONSIDERATION:

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Client Initiated Backchannel Authentication (CIBA). *FAPI defines a protocol for an asynchronous and de-coupled mechanism for a data recipient to request authentication from a data holder known as Client Initiated Backchannel Authentication (CIBA).*	CIBA can trigger re-authorisation as a backchannel request. It can be used for re-authorisation in the same way as it is used for authentication.	**Adopt once more established.** Use of CIBA for re-authorisation is encouraged, but only if it is also introduced for the authentication flow. Per the authentication flow, recommend adopting CIBA flow once it is considered more established and once clearer use cases (and therefore implementation details) are defined and security reviewed.
CDR Specific Mechanism. *An alternative option is to define a CDR specific mechanism for reauthorisation. This mechanism would be specific to the CDR regime and would not be supported by an external standard implementation.*	The CDR Specific Mechanism uses one additional endpoint to request an extension of *sharing_duration*, and existing introspection and token refresh mechanisms to communicate successful extension.	Whilst non-standard, this is a simple mechanism which can be securely implemented with one additional endpoint. The Access Token must be mandatory to call this endpoint. **Recommend adopting the CDR Specific Mechanism** for the initial CDS specification, until such time that CIBA mechanisms are available.

11.3 CONSENT

CONSENT IS THE MEANS BY WHICH A CONSUMER AUTHORISES ACCESS TO THEIR DATA. IT IS IMPORTANT TO NOTE THAT CONSENT CAN BE EITHER:

- **Coarse-grained** – This is granting consent to a resource, for example to allow transaction history to be retrieved.
- **Fine-grained** – This is granting consent to a resource, but with the addition of detailed constraints. Such constraints could include transaction types, start and end dates, inclusion and exclusion of certain data fields (e.g. merchant identifiers, payment description) or the specification of a consent duration.

With respect to future revisions of the CDS: A Consent API may be useful for both of the above and will be needed for future payment authorisation. However, it is understood that there is not an existing requirement for fine-grained authorisation, nor is there existing support for a Payment API.

The review makes recommendation as below.

NAME / DESCRIPTION	ANALYSIS / COMMENT	RECOMMENDATION
Defer inclusion of a Consent API until a requirement exists. *In this option the inclusion of a Consent API will be deferred until a later date when a specific requirement is introduced that requires such a pattern to be adopted.*	Deferring inclusion of a Consent API is a pragmatic option – Without requirements it is difficult to articulate specifications and to certify products.	**Defer until a requirement exists**, given that it is difficult to develop and certify API products without clear specifications. However, note that fine grained requirements will likely arise (e.g. when extending to other sectors), at which point there may be a higher level of complexity involved in introducing a consent API due to semantic mismatch with the current specifications.
Include a Consent API as an optional mechanism. *In this option the specifics of a CDR Consent API would be defined but would be defined as optional.*	If implemented, a consent API would be a core feature of the CDS. Optionality will likely raise issues with costs, product certifications and inter-operability.	
Include a Consent API as a mandatory mechanism. *Equivalent to option 2 except that the implementation of the Consent API would be mandatory.*	A consent API would be a core feature of the CDS, so needs detailed requirements and will need to be supported by conformance tests. Without these, it cannot be made mandatory.	

12. APPENDIX D DETAILED REVIEW OF THE CDS

12.1 INTRODUCTION

THE CDS IS DIVIDED INTO:

Standards

Defines the core conventions for APIs built on the CDS, such as key principles, the structure of API URLs and the definitions of response codes.

Schemas and APIs

This section defines a limited set of read-only bank APIs that will be available in the initial version of the API standard. This section will be extended over time to support additional banking needs, as well as the energy and telecommunications industries.

Security Profile

Defines the overarching approach to security. This information security profile is based on OIDC and the FAPI-RW profile, overlaid with specific directives from Data61 as to how to implement specific components of FAPI-RW.

Authorisation Scopes

Defines the OpenID scopes that allow access to the consumer data APIs provided by Data Holders.

This review focuses on version 0.9.3 of the CDS and largely on the Information Security Profile and other elements related to security. The review is written in alignment with the defined CDS sections. Where security observations have been made, the prefix "OBS-[ID]" has been used.

Observations are classified as:

- Positive – these have a positive security implication.
- Neutral – these have neither a positive nor negative security implication but are generally worth noting.
- A Security Risk – these observations highlight a security risk along with a **recommendation** as to how to address these risks.

12.2 STANDARDS

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Security Risk	OBS-01	IP Address Forwarding	Many banks source IP threat intelligence feeds and use it to block access to known malicious IP addresses. The standard has no response code to convey such an event to the calling system. Banks are therefore put in a position of either permitting malicious traffic, or responding with an alternate code, which inevitably will be construed as a 'service issue'. This type of issue is likely to arise when payments are added to the CDR profile, as many banks include velocity checks and will likewise need a means to communicate a velocity breach to the data recipient.	**It is recommended** that the CDS use the 403 forbidden response code with an error payload detailing the reason for authorisation failure.
Security Risk	OBS-02	Browser Metadata	Bank security risk engines make use of browser metadata, to either fingerprint calling agents or to detect malicious behaviour. This additional metadata is not being forwarded to the data holder. This could impact the effectiveness of such tools.	**It is recommended** that the CDS be extended to forward browser headers to the data holder. A solution could be to Base 64 encode all inbound headers and forward them to the data holder with a custom X-Originating-Agent header. This will permit banks to continue use of tools that detect malicious end-user behaviour.
Neutral	OBS-03	Permanence	ID Permanence is introduced as a mechanism to ensure resource identifiers (e.g. accounts) are immutable. For example, a call to "Get Accounts" will respond with account identifiers that are meaningless when transferred across organisations. However, in practice, any volume of data from a call to APIs such as "Get Transactions" will provide sufficient information to 'de-anonymise' and permit data linkage across client organisations and providers.	**No recommendation.**

12.3 SECURITY PROFILE

12.3.1 CDR FEDERATION

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-04	CDR Register	The CDR register is fundamental to the security posture of the Open Banking ecosystem as a whole, but as supporting processes are to be defined outside of the CDS it is not in scope for this review.	**It is noted** that the "Register Design Specification" is currently in review and defined in documentation available from the ACCC.

12.3.2 AUTHENTICATION FLOWS

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Positive	OBS-05	Hybrid flow restrictions	Hybrid flow is restricted in a manner that improves the security posture of the system. It supports only the restrictive *'code id_token'* flow type. Using the Hybrid flow can aid in the reduction of threats such as 'identity provider mix-up' attacks that can otherwise arise.	**No recommendations.**
Security Risk	OBS-05b	JARM response types	JARM enables the signing and encryption of server responses. This reduces the risk of tampering of server responses.	Consider implementation of JARM. It is noted that JARM was introduced in October 2018, so may not have been specified in the original development of the CDS.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Security Risk	OBS-06	Hybrid flow and phishing attacks	Phishing risk could be introduced due to: • Use of the *redirect_uri* flag as an unauthenticated URI parameter. • Changed user experiences can be leveraged by attackers as a means to trick users to enter credentials into unfamiliar sites. The use of FAPI-RW counters the issues with unauthenticated URI parameters, as they are now in a signed Request Object. The risk of phishing due to changed user experiences is inherent to the use of OIDC redirect protocols.	**It is recommended that:** • Product certification must ensure that Request Objects are digital signed, but also that there is no way to disable such a feature. This is important to note as many solution providers are building on top of existing, less secure OIDC implementations. • The CDR Register must restrict redirects to known endpoints that have been previously registered, and this must likewise be assured in product certification. • Stronger authentication mechanisms (e.g. FIDO) should be considered as another method to counter phishing risks.

12.3.3 CLIENT AUTHENTICATION

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Positive	OBS-07	Client Authentication	The standard sets two directives for Client Authentication: • Clients are to use the *private_key_jwt* authentication method. • Clients are to use MTLS with Holder of Key (HoK). These patterns are in line with the FAPI-RW profile.	No recommendation.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

12.3.4 OIDC CLIENT TYPES

No observations.

12.3.5 CONSENT

See also the open items section for discussion of options.

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-08	**Consent – Privacy Notices**	From a review of the UX stream materials a screen was defined to accept a privacy notice. Display and acceptance of privacy notices is not currently specified in the CDS profile.	The Data Holder and Data Recipient will have obligations on privacy outside of the CDS which may influence how notices are displayed and acknowledged. If not, potentially the CDS should consider specific guidance to present privacy notices and store acknowledgement of their acceptance. Additional specific guidance may be required regarding the display and storage of consent for legal statements – though this will likely be resolved in the competitive space.
Security Risk	OBS-09	**Consent – broad access to data**	Consent grants 'broad access' to data, making all the consumer's accounts available for use. Consumers are not able to select which account to make available to Data Recipients. Security risks could arise in the event of a data compromise. Should this occur, more accounts are impacted than would otherwise have occurred. This could be a more significant risk when payment APIs are introduced. A lack of account selectivity will mean that all accounts may potentially be vulnerable to financial (payments) exploits.	**Update (2/7/2019):** It is recommended that the CDS be updated to note that the competitive space will find solutions for authorisation of individual accounts. [This update has been made after the risks was discussed with the CDB]. Original recommendation: A mechanism should be developed to allow consumers to select the individual accounts they wish to authorise.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-10	**Consent – deep access to data**	Consent grants 'deep access' to data, as there is no limitation to the amount of historical data that will be made available.	**No recommendations.**
Security Risk	OBS-11	**Consent – rich access to data**	Consent grants 'rich access' to data, as there is no limitation to the type of information returned. For example, there is no means to provide a transaction amount (not sensitive) without also providing a transaction description (potentially sensitive). Some banks make use of detailed transaction data to authenticate phone users, especially for password resets ("e.g. tell us your last transaction and the business where it was made"). A compromised Data Recipient may have more transaction data than necessary, and this could have ramifications for banks that use such data for phone-based authentication.	**It is recommended** that banks review the use of transaction data for end-user authentication at the phone channel. Banks that use make use of 'rich data' for phone-based authentication may choose to move to alternate approach in advance of Open Banking deployment.
	OBS-18	**Consent – non-repudiation**	A CDR User can consent to authorising access to their data and at a future time claim they have not approved such an action – due to the CDS not specifying that adequate logging is needed to provide event traceability. This may be a minimal risk for read-only APIs but could be more problematic when payments are introduced.	Guidance should be provided to Data Recipients to record the following each time consent events occur, including: Username (consumer's ID at the Data Recipient), Timestamp, IP, Consent Scopes.

12.3.6 SCOPES AND CLAIMS

No observations.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

12.3.7 TOKENS

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-12	Token Timeout	CDS aligns use of tokens to both OIDC and FAPI-RW profiles. Access Tokens are fixed at 10-minute expiry, whereas Refresh Tokens are permitted a value greater than 28 days and less than the consent duration. Selection of a 10 min Access Token timeout appears to balance operational trade-offs. A shorter timeout reduces the utility of a 'stolen' token, but can also lead to increased traffic and potential cost ramifications (e.g. some commercial authorisation server vendors charge a per-token usage fee and/or if run on a consumption-based cloud computing model, additional processing load could increase costs). A longer timeout can be more useful in scenarios such as long running batch activities but can also degrade security. Use of 10 min timeout appear to be a mid-point of operational trade-offs.	No recommendations.
	OBS-12B	Token revocation	The CDS does not address token revocation, and the need for Data Holders to ensure that revoked tokens are not accepted. There may be an underlying assumption that these controls are in place.	CDS should consider explicitly noting that token revocation checks are required at the Data Holder.

12.3.8 IDENTIFIERS AND SUBJECT TYPES

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-12C	Subject Consistency	The subject ('sub') field in the tokens is a unique identifier. Without further specification, an implementer could use one identifier in the Access token and a different one in the ID Token. In the event of an incident, it could become difficult to reconcile activity due to use of multiple identifiers.	CDS should consider specifying that subject identifiers are made consistent across tokens.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

12.3.9 LEVELS OF ASSURANCE

No observations.

12.3.10 TRANSACTION SECURITY

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-13	**Use of TLS 1.2+**	CDS specifies TLS 1.2 or higher. This merits consideration of mandating sole use of the newer TLS 1.3 standard. Per review of support: *Front-end channels:* TLS 1.3 is supported in both Chrome (release 66) and Firefox (starting with release 60) and is in development for Safari and Edge browsers. *Backchannels:* OpenSSL has only just adopted TLS 1.3, whilst Secure Channel Provider (security library used by Windows) is still limited to TLS 1.2.	The specification for TLS 1.2+ remains valid but merits another review when future CDS updates are made.
	OBS-15	**Permitted cipher suites**	Current CDS wording specifies that: "only the following cipher suites shall be permitted.... [with a list of endorsed ciphers]" This may hinder use of stronger ciphers in the future.	**It is recommended** that wording should be amended to "the following cipher suites *or stronger* shall be permitted". This avoids coupling of ciphers to contemporary best-practices. The list of 'acceptable ciphers' should be reviewed each time the CDS is updated.

12.3.11 REQUEST OBJECT

No observations.

12.3.12 REQUESTING SHARING DURATION

No observations.

12. APPENDIX D - DETAILED REVIEW OF THE CDS

12.3 SECURITY PROFILE CONT.

12.3.13 END POINTS

No observations.

12.3.14 REAUTHORISATION MECHANISM

Refer to the open items section for discussion of options.

12.4 BANKING APIS

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Neutral	OBS-16	Unmasked account numbers	The "Get Account Detail" API will reply with a BSB and account number. Some banks have a policy that this data element must be masked when presented on their systems. The practice of masking account numbers may have been security related at one time but appears to be maintained at this stage for privacy.	No recommendations.
Security Risk	OBS-16B	Integrity control of APIs	API responses are not signed, which may expose them to tampering attacks.	Consider inclusion of Detached JWT Headers (x-jws-signature). This has been introduced by UK Open Banking as a standardised control for API response integrity.

12.5 COMMON APIS

No observations.

12.6 SCHEMAS

No observations.

12.7 ADMIN APIS

No observations.

12.8 AUTHORISATION SCOPES

CATEGORY	#	DESCRIPTION	ANALYSIS	RECOMMENDATION / COMMENTS
Security Risk	OBS-17	**Scope and linkage to intent**	Authorisation scope names do not readily convey purpose. As the CDS extends (i.e. additional APIs, additional industry sectors) it may become more difficult for developers to readily understand the mapping between scopes, APIs and level of permissions (e.g. read vs write). This possibly increases the risk that developers will request more scopes/ access than is necessary for the task.	The CDS should define scope labels that better convey intent. An example is: *'account.details.readonly'.*

13. GLOSSARY

API	Application Programming Interface
CA	Certificate Authority
CDR	Consumer Data Right
CIBA	Client Initiated Backchannel Authentication
DH	Data Holder
DR	Data Recipient
FAPI	Financial-grade API
FAPI-RW	FAPI Read/Write Profile
HOK	Holder-of-Key
JSON	JavaScript Object Notation
JWK	JSON Web Key
LOA	Level of Assurance
MTLS	Mutual Transport Layer Security
OIDC	OpenID Connect
PPID	Pairwise Pseudonymous Identifier
TLS	Transport Layer Security

FORTIAN
Security | Privacy | Risk

Fortian Pty Ltd
ABN: 33 164 874 695