

BEIS: Smart Data Research

Report: Authentication and Trust

Prepared by Raidiam Services Limited

August 2020



Acknowledgements

With thanks to all who have set the foundations for secure and safe data sharing in the UK through the formation of the Open Banking Implementation Entity...

...and to the pioneers who will stand on their shoulders.



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit <u>nationalarchives.gov.uk/doc/open-government-licence/version/3</u> or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: <u>psi@nationalarchives.gsi.gov.uk</u>.

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at: <u>smartdatareview@beis.gov.uk</u>

Contents

RAIDIAM RESEARCH RESPONSE - AUTHENTICATION	5
About Raidiam	
Abstract	
Background	
EXECUTIVE SUMMARY	
Smart Data and Trust	
Trust Requirements	
Trust Principles and Frameworks	10
Framework Implementations:	
Smart Data Alignment Challenges	
Conclusion	
SMART DATA AND TRUST	
Principles of Smart Data Ecosystems	
Players	
Trust in Ecosystems	
Elements of Trust	
Definitions and Examples	15
TRUST REQUIREMENTS	16
Data Sensitivity	
User Accessibility	17
TRUST PRINCIPLES AND FRAMEWORKS	18
Roles and Responsibilities	18
First Party - Single Service	20
First Party - Separate ID service (SSO / 'login withx')	21
Vectors	
Trust Frameworks	
FRAMEWORK IMPLEMENTATIONS:	23
Options Overview	23
Implementations	
Ecosystem - Provider-centric (OBIE)	25
Ecosystem - Separate ID and AuthN service (Gov.UK Verify)	
Ecosystem - Shared Gateway for ID, AuthN and AuthZ (OfGEM option 1)	27
Ecosystem - Shared Gateway and Separate ID (OfGEM option 2)	28

29
29
30
31
31
31
32
34
35
35

RAIDIAM RESEARCH RESPONSE -AUTHENTICATION

About Raidiam

Raidiam is delighted to respond to this request from BEIS to provide policy research support to help shape the work on Smart Data. We understand that this work is focussed on the key objectives of putting consumers in control of their data, and enabling innovation, which is entirely aligned with the principles that have led to the successful open banking ecosystem implementation in the UK.

Raidiam has been involved with the design, development and delivery of open banking in the UK, and is the only consultancy involved with the Open Banking Implementation Entity from the start. We are directly responsible for the design and delivery of the UK's trust framework and services and enhance that experience through our hand-picked global associate network of acknowledged experts. We believe that there are valuable learnings and experiences (not to mention technology) that can be leveraged to ensure the success of any secure, open data sharing ecosystem irrespective of country or sector.

Raidiam is a member of a number of organisations concerned with the development, promotion and implementation of standards and frameworks for secure data sharing globally, including being a member of the OpenID Foundation¹ (a not-for-profit committed to enabling, promoting and protecting OpenID technologies), the Open Identity Exchange², a founding member of IDPro³ (professional body for identity and authentication specialists), and Chair of the Technology Working Group of FDATA⁴ (Financial Data and Technology Association - working with governments, regulatory authorities and the financial services industry in a mission to open up the financial sector globally).

These memberships are not passive: Raidiam's CTO is one of only 16 individuals globally recognised as an author of the Financial grade API (FAPI) security profile as well as the global standards for "redirect" and "decoupled" authentication and authorisation standards.⁵ These standards now form the cornerstone of the UK, Australian and New Zealand standards, and Raidiam is in global demand from central banks and industry bodies to help design and deliver workable open data sharing ecosystems.

Raidiam continues to donate its time and resources to ensuring that all industries globally have workable frameworks and standards that offer the highest degree of protection for themselves, their customers and other partner organisations. Raidiam has been in conversation with both OfGEM and the Pensions regulator regarding their respective implementations of data sharing, and is listed on G-Cloud as a Provider of an Identity, API and Authentication accelerator platform⁶, as well as a Digital Outcomes Specialist.⁷

⁵ <u>https://openid.net/wg/fapi/</u>

¹ <u>https://openid.net/foundation/</u>

² <u>https://openidentityexchange.org/</u>

³ <u>https://idpro.org/</u>

⁴ <u>https://fdata.global/</u>

⁶ https://www.digitalmarketplace.service.gov.uk/g-cloud/services/561026363225214

⁷ <u>https://www.digitalmarketplace.service.gov.uk/buyers/frameworks/digital-outcomes-and-specialists-</u> 4/requirements/digital-outcomes

We are delighted to support the BEIS research on this area and believe we bring an unique set of credentials, experiences and connections that allow us to provide high-quality, wellevidenced views. In addition, our views on suggested next steps are grounded in the real-world experience of delivering these capabilities over the past 3 years and which we would be happy to continue in conversations with BEIS.

Abstract

The key question asked for this BEIS research is:

"What are the key challenges to encouraging the design of common authentication mechanisms across sectors for smart data in a way that minimises friction and provides sufficient levels of security? How do these challenges and any risks vary with different types of data?"

Overall, there are many challenges associated with the design of authentication mechanisms which Raidiam has identified. In carrying out our research, we have identified a key challenge in that the term "authentication" ("AuthN") is used interchangeably (and inconsistently) with the terms "authorisation" ("AuthZ") and "identification" ("ID"). All of these terms are used to support the levels of trust in an ecosystem.

The Cambridge dictionary defines "authentication" as "the process of proving that something is real or true", and so authentication is intrinsically linked with what that "something" is (identification). Authentication is usually carried out for a purpose, which necessarily leads to authorisation and the principles of trust.

Therefore, we aim to focus on the principles and elements of trust frameworks, including authentication, to provide further context and clarity around these definitions and to highlight options for implementation of those frameworks. We also offer suggestions for further work that we believe is necessary to develop this research, and which we would be very happy to help carry out.

Background

At the basic level, providers of online services generally offer a bespoke, bilateral authentication between consumer and provider. The 'username' / 'password' pair is a well-understood and widely adopted mechanism which provides minimal friction but only moderate security. It is also not transferable or even consistently applied with password policies, complexities, length and reset times being different.

The security issue is heightened when the data is highly sensitive such as with financial information, leading to most financial institutions adopting a second factor (e.g. standalone PIN device and/or SMS one-time-passcode (OTP)). This provides increased security, albeit is balanced by an increase in friction.

Extending this bank-level authentication within the same organisation from current accounts to other bank services such as mortgages, savings and investments is facilitated by the introduction of a 'Single Sign On' (SSO) mechanism which allows federated access: i.e. re-use of the same credentials. Broadening that principle to make an authentication mechanism common within a sector requires agreement of standards between participants in that sector. Making this mechanism common across sectors is one step further in alignment for the SSO principle and requires a further level of technical and policy standardisation.

Friction for users and participants must be balanced with the regulatory and reputational requirements to provide appropriate security. Starting with the top level of security and data sensitivity is an advantage in terms of federation but may impact the User experience for other applications. Security and friction are typically proportional, with low friction being of low security and high security requiring high friction in the user journey. A truly versatile, usable, interoperable common standard should be flexible enough to accommodate differing requirements for all levels of security as well as types of data.

We have seen from our research that the key question needs to be broken down into a number of sub-questions which will be addressed over the course of this response:

- What is authentication? Who needs to be authenticated? Why is it needed?
- What mechanisms exist for authentication?
- How do these mechanisms differ with different types of data or sectors?
- What common features do these mechanisms have?
- How to standardise across sectors?
- How to consider implementation?

EXECUTIVE SUMMARY

Smart Data and Trust

Smart Data at heart is a data sharing ecosystem which requires at its foundation the same fundamental characteristics as any other data sharing ecosystem. Trust is at the heart of all of this. As far back as 2011, the World Economic Forum identified the need for trust as key to unlocking the full potential of what it called a 'new asset class'.⁸ More recently, in 2018, Chatham House published some key principles for sharing data - albeit in a public health setting the cross-sector application is clear: "Trust facilitates successful data sharing ... Trust is built when ... those involved in the process know each other...and carry out the commitments as agreed."⁹

Trust is required both ways between all the participants of a data sharing ecosystem, namely: the Providers of the data, the Third Parties making use of that data and the end-Users. This boils down to the 'Who', the 'What' and the 'How'. The end-Users (Consumers) are legally the owners of their data. They need to know who the Providers/ Third Parties are, what they are allowed to do with the User's data, and how that data will be provided and secured. Conversely, the Providers need to know who the Users/ Third Parties are, what they are allowed to do with the provided data, and how that data will be provided and secured. And to complete the picture, the Third Parties need to know who the Users Providers are, what they are each allowed to do with the data, and how that data will be provided and secured. Trust is therefore made up of a number of elements, of which Authentication is just one.

Trust Requirements

Different ecosystems have different requirements for providing and validating the 'Who', the 'What' and the 'How', based primarily on the sensitivity of the data, but also on the User accessibility requirements. The key research question includes the requirement to "minimise friction and provide sufficient levels of security". There is a general view that more sensitive data requires more security, which may increase the friction for the User. However, there is a level of visible friction that provides more User confidence in the security of the whole system, so the aim should be to achieve a 'friction right' rather than a 'frictionless' experience.

Data Sensitivity levels can be defined by the risks of mis-use of that data. The subsequent requirements for identification, authentication and authorization determine which attributes and credentials are captured: what they are, how they are collected, who verified them, and when any actions were carried out.

The User accessibility point is addressed by looking at the customer journey. There are multiple ways, with significantly different experiences, of engaging with Users which all require different technical services.

⁸ <u>https://www.weforum.org/reports/personal-data-emergence-new-asset-class</u>

⁹ https://datasharing.chathamhouse.org/guide/principles/trust/

Trust Principles and Frameworks

There are a number of roles required to tie the system of Identification, Authentication and Authorisation together, irrespective of sector. All these roles are required, but multiple roles may be held by each participant. In general, the end User ("Subject"), is giving a system ("Client") a pass ("Access Token") to access a protected resource held by the Provider ("Resource Server"). This requires the User to be Identified and Authenticated, and for the Authorisation to be confirmed.

The attributes, credentials, and the level of validation required can be captured as a set of Vectors which can be tailored for each ecosystem. This contains specific definitions of categories of information ("Vector Components") and values ("Vector Component Values") that make up the required data structure ("Vector") in that sector. The starting point for these vectors should be the levels of identity Proofing, the strength of the Credentials, the management of those Credentials and the security of the Assertion as it travels over the network. In an ecosystem, this proof requirement should apply to authentication of all parties.

The exact rules and legal requirements for each role in a specific sector forms a "Trust **Framework**". Each ecosystem requires a standardised set of rules and legal requirements that covers all the roles and vectors described above. The combination of who provides which role(s), and the levels to which they must carry out those roles can be captured in a sector-specific "Trust Framework".

Framework Implementations:

Different Trust Frameworks will have different implementation options, but a common Trust Framework is a prerequisite to turn a 'sector' into an 'ecosystem'. A common trust framework significantly reduces complexity and hence costs, increases scalability and interoperability within the sector as well as opening up options for the type of cross-sector standardisation that Smart Data is pursuing.

Different implementations can be defined for sectors, which have different pros / cons and costs associated for different participants. Each of the proposed implementations could be used for any sector if the right prerequisites are in place. The right solution will depend on the appetite and alignment of each set of participants.

Smart Data Alignment Challenges

Implementation of a common mechanism for Smart Data will require a commitment to symmetry across sectors to build sector-specific details into the Trust Framework principles described earlier. At a starting point, symmetry within sectors should be confirmed for User experiences and TPP/Provider regulatory responsibilities.

Federation of credentials can support alignment between sectors. This may include identity, regulatory permissions or other authorisation credentials and will be codified in the Trust Framework.

Technical choices need to be made to ensure that any implementation provides a strict and consistent base to be credible, but retains the flexibility to adapt to multiple sectors. This implies open-source standards which are widely available, widely understood, and have been tried and tested. In addition, there are a choice of partners who could manage any technical build, meaning the commercial market is maintained.

The biggest challenge in encouraging the design of common cross-sector mechanisms for Smart Data is that the sector-specific frameworks are not clearly standardised or understood. We believe there is a great benefit from increasing the visibility of these overarching frameworks to ensure common starting points.

Further investigation and discussion with different sectors is now required to increase visibility of the Trust Framework model and then determine the required Trust Frameworks. Only then can the sector-specific details be developed successfully, and commonalities confirmed. Examples such as Australia highlight the delays and confusion that can arise from not confirming the foundations up front.

Conclusion

Authentication is one part of a Trust Framework which is required for a successful data sharing ecosystem. Alignment on the principles comes before capturing sector-specific requirements, but then facilitates agreement to deliver a common mechanism.

We recommend the following next steps:

- Further sector-specific research and documentation of the required Trust Frameworks / Vectors,
- A technical Proof of Concept of these Trust Framework options in action,

and would be delighted to continue discussions.

SMART DATA AND TRUST

Principles of Smart Data Ecosystems

Smart Data at heart is a data sharing ecosystem which requires at its foundation the same fundamental characteristics as any other data sharing ecosystem. Trust is at the heart of all of this. Authentication is a key part of Trust.

As far back as 2011, the World Economic Forum identified the proliferation of personal data from financial and medical records to employment data as one of the most valuable resources of the 21st century. It forecast that the global volume of digital data would grow more than 40-fold in the decade to where we are now in 2020. The Personal Data report described the existing personal data ecosystem as fragmented and inefficient, but painted a picture for success that highlighted interoperability and trust as the keys to unlocking value:

"Current technologies and laws fall short of providing the legal and technical infrastructure needed to support a well-functioning digital economy" "The rapid rate of technological change and commercialisation in using personal data is undermining end user confidence and trust" "Greater mutual trust can lead to increased information flows, value creation, and reduced litigation and regulatory costs" "win-win-win' outcomes will come from creating mutually supportive incentives, [and] reducing collective inefficiencies"¹⁰

More recently, in 2018, Chatham House published seven key principles for sharing data. These principles are intended to help create the right environment for data sharing, achieve good practice in data and benefits sharing and ensure that data sharing is conducted in a fair and ethical manner for all those involved. The parallel with Smart Data is clear:

"Trust facilitates successful data sharing, which in turn reinforces trust. ... trustbuilding measures between stakeholders, at the personal or organizational level, help create an environment conducive to data sharing. Trust is built when the purpose of data sharing is made clear, and when those involved in the process know each other, understand each other's expectations, and carry out their commitments as agreed. Trust increases the likelihood of equitable benefit sharing and further collaboration, and improves core surveillance capacity through the creation of surveillance networks. It can be very hard to build trust, but very easy to lose it."

¹⁰ http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Players

In the consumer-focused Smart Data ecosystems we are considering, we have three main players:

the User (Consumer), the Provider (offering the core sector Service) and a Third Party Provider (TPP, offering the Smart Data proposition):



In all the cases that follow, we assume:

- A User holds an account for a core service or set of resources from the Provider
- A Third Party offers the User a proposition enabled through Smart Data sharing
- The User provides consent to the Third Party for the purposes of delivering that proposition
- The Provider has obligations to safeguard the User data, but also to share it when instructed.

Trust in Ecosystems

In order to be successful, all participants in an ecosystem need to have a shared definition and understanding of trust:

USERS:

PROVIDERS / TPPs:





Consumers must be able to find and trust the propositions they are being offered;



Companies offering those propositions must be capable of finding and trusting the connections;



COMMUNITY:

needs to be clearly defined, secured and checked to increase trust and facilitate usage.

The end-Users (Consumers) are legally the owners of their data. They need to know who the Providers/ Third Parties are, what they are allowed to do with the User's data, and how that data will be provided and secured. Conversely, the Providers need to know who the Users/ Third Parties are, what they are allowed to do with the provided data, and how that data will be provided and secured. And to complete the picture, the Third Parties need to know who the Users / Providers are, what they are each allowed to do with the data, and how that data will be provided and secured.

Elements of Trust

As can be seen from the diagram above, the question of trust is consistent in all applications. In fact, our research helped us to identify the key questions that each participant will be asking of the others:

- Who are you? (Identification)
- What are you allowed to do? (Authorisation)
- How sure am I of those points? (Authentication)

So, Authentication is a key part of Trust, but is also intrinsically linked to Identification and Authorisation. Taken together with ongoing Validation, and Data Security, these elements support, inform and must deliver the Consent and Liability frameworks that are vital to ensure the Trust in the overall ecosystem:



Definitions and Examples¹¹

identification noun, UK /aɪ den.tɪ.fɪ keɪ.ʃən/: proof of who someone or something is.

authorisation noun, UK /,o:.0ər.aɪ'zeɪ.ʃən/: the act of giving someone permission to do something.

authentication noun, UK /ɔː, θen.tɪ'keɪ.ʃən/: the process of proving that something is real or true.

It is worth noting that these items are independent although closely linked:

- *Identification is possible without Authentication:* e.g. the provision of an email address gives identity that has not been authenticated. In fact, Authentication may not be required, depending on use-case.
- Authentication is possible without Identification: e.g. a proof of age card showing a photo can Authenticate you to buy (e.g.) alcohol but does not need to say anything further about who you are.
- *Identification does not guarantee Authorisation:* e.g. identification of an individual does not in itself provide Authorisation to access a certain bank account or floor in a secure building.
- Authentication is done for a reason to confirm identity and/or authorisation.

Example Credentials:

- Drivers License: Provides authZ to drive, also used as authN ID.
- Cash Machine Card: Provides authZ to access accounts ID is the PIN
- Online (non-bank) service Typically does not need 2FA Username/PW works
- Online Bank Account: Typically uses 2FA PIN device or SMS

Authentication is typically a two-step process¹²:

Step 1: Authenticate the credential itself:

- Was the credential issued by a trusted organisation? e.g. is the Driver's License valid?
- Has the credential expired?
- Has the credential been revoked, voided, or tampered?

Step 2: Authenticate the identity of the the individual - i.e. ensure that the individual the credential was issued to is the same individual that is presenting it:

- Does the photo and height/weight on the driver's license match the person who presented it?
- Does the person know the PIN for the card that was presented?
- Does the person have the private token required to access the website?

¹¹ <u>https://dictionary.cambridge.org/dictionary/english/</u>

¹² <u>https://arch.idmanagement.gov/services/access/</u>

TRUST REQUIREMENTS

Different ecosystems have different requirements for providing credentials and validating the 'Who', the 'What' and the 'How'. This is based primarily on the sensitivity of the data, but also reflects the User accessibility requirements.

Data Sensitivity¹³

The sensitivity of the data can be assessed by considering the impact of loss or compromise of that data across core categories. Mapping the worst-case scenarios in this way allows a consistent classification of sensitivity:

Data Sensitivity Level	Non- sensitive	Sensitive / Has	Very sensitive	Extremely sensitive
Category of impact		monetary value	/ Large monetary value	
Inconvenience / Reputational loss	L	М	Μ	н
Financial Loss	L	М	Μ	н
Public Interest Harm	n/a	L	Μ	н
Unauthorised release of data	n/a	L	Μ	н
Personal Safety	n/a	n/a	L	Μ
Civil Violation	n/a	L	М	н

There is a general view that more sensitive data requires more security, which may increase the friction for the User. However, there is a level of visible friction that provides more confidence in the security of the whole system for Users, so completely minimising friction may not always be desirable.

The subsequent requirements for Trust, around identification, authorisation and authentication then determine which attributes and credentials that are captured: what they are, how it was collected, who verified it, and when any actions were carried out.

¹³ <u>https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf</u>

User Accessibility

It is equally important that the User journeys involved in providing credentials and validating the 'Who', the 'What' and the 'How' are considered across all of the three main ways14 of carrying out authentication and obtaining authorisation:

- **Redirection**: This is primarily User-driven: the TPP will redirect a User to go and get a credential (letter, token, seal) from the Provider to confirm the User gives authorisation (consent) to the TPP. This credential also identifies the User in a way that the Provider will recognise when the TPP brings it back to them. This works well when a User is able to interact with both parties and especially when this happens via the same channel or device. Redirection was the first method implemented by open banking in the UK and is by far the most widely adopted. There are however significant challenges if the Provider and TPP use different channels or devices, or if the User is not digitally connected.
- **Decoupled**: This involves more work on behalf of the Provider: the User only needs to provide the TPP with an Identity which the TPP then uses when it contacts the Provider. It is then up to the Provider to carry out authentication and authorisation checks with its User, and to provide the TPP with an access token once those checks are complete. The Decoupled flow has significant benefits over the Redirect flow in that the checks are fully in the control of the Provider, and they could be performed via digital (e.g. push to mobile), telephony (e.g. phone call or SMS) or other non-digital (e.g. letter or 'come to branch') contact. This is more inclusive and opens up more use cases and sectors.
- Embedded / Impersonation: This method involves the authentication process being 'embedded' in the TPP's User journey and is used by 'screen scrapers'. In effect, the User no longer has control of the credentials and the TPP is now impersonating the User. This creates significant security concerns and makes it difficult for a Provider to tell the difference between a real User / customer and a Third Party (whether an authorized TPP or not). Controlling access of the Third Party to other resources or for other purposes is impossible without invalidating all of the User (shared with Third Party) credentials. For all these reasons it is not recommended.

¹⁴ <u>https://standards.openbanking.org.uk/customer-experience-guidelines/authentication-methods/latest</u>

TRUST PRINCIPLES AND FRAMEWORKS

Roles and Responsibilities

Before we look at the options for implementation of the Trust Requirements, we need to define the roles in the system as a whole for Identification and Authentication¹⁵ and Authorisation¹⁶. There are a number of roles required to tie the system together, irrespective of implementation. The majority of these roles are required, even for apparently simple cases, but multiple roles may be held by each participant:

Category	Role	Туре	Responsibility
AuthN	ldentity Subject	Person	The individual ("user") engaging in the identity transaction, being identified by the Identity Provider to the Relying Party.
AuthN	Primary Credential	Credential	The means used by the Identity Subject to authenticate to the Identity Provider.
AuthN	ldentity Provider	System	A system that manages identity information and is able to assert this information across the network through an identity API.
AuthN	ldentity Proofing	Process	The process of verifying and validating that a set of identity attributes belongs to a real-world Identity Subject
AuthN	ldentity Federation	Protocol	A protocol (or implementing system) in which an Identity Provider asserts a User's identity information to a Relying Party through the use of a cryptographic assertion or other verifiable mechanism.
AuthN	Federated Credential	Credential	The assertion presented by the Identity Provider to the Relying Party across the network to authenticate the User.
AuthN	Relying Party	System	A system that consumes identity information from an Identity Provider for the purposes of authenticating the User.
AuthZ	Resource owner / End-User	Person	An entity capable of granting access to a protected resource. When the resource owner is a person, it is conceptually the same as the User.

¹⁵ <u>https://tools.ietf.org/html/rfc8485#section-1.2</u>

¹⁶ https://tools.ietf.org/html/rfc6749

Category	Role	Туре	Responsibility
AuthZ	Client	System	A system making protected resource requests on behalf of the resource owner and with its authorization. This is conceptually the same as the Relying Party.
AuthZ	Authoriz'n server	System	The server issuing Access Tokens to the Client after successfully authenticating the Resource Owner and obtaining authorization. The Authorization Server usually contains an Identity Provider service to allow Access tokens to be issued with Identity assertions to the Client / Relying Party.
AuthZ	Resource server	System	The server hosting the protected resources, capable of accepting and responding to protected resource requests using Access Tokens.
AuthZ	Access Token	Credential	Access tokens are credentials used to access protected resources. and represents an authorization issued to the Client.

There are many roles and responsibilities listed here which at first sight seem quite daunting. This is partly because of the inconsistent definitions that abound for these terms, and also because the whole process of trust is a very natural and instinctive human activity that occurs without us ever really thinking through the different elements. Our daily lives contain countless interactions with people and services and that we need to assess who they are, whether to trust them, if so, what for. Then we need to carry out certain processes designed to capture that trust.

Looking at the definitions above, we see that in general, the end User ("Subject"), is giving a system ("Client") a pass ("Access Token") to access a protected resource held by the Provider ("Resource Server"). This requires the User to be Identified and Authenticated, and for the Authorisation to be confirmed.

In the Identification and Authorisation flow, the end User ("Subject"), provides (e.g.) a username/password ("Primary Credential"), to an identification service ("Identity Provider"), who checks both identity ("Proof") and passes on that information ("Federated Credential") to the service Provider ("Relying Party") in order to authenticate the User. The Identity Provider is responsible for verifying and validating the link ("Identity Proofing") between a set of identity attributes and a real-world Identity Subject. The Relying Party typically then uses the authentication to confirm Authorisation for that particular User.

Although the example of username/password pair is given above, we will see that splitting out the roles of the Username (Identification) and Password (Authentication) can occur when looking at different frameworks. As mentioned above, most of these roles are required in any framework, but multiple roles may be held by each participant. The structure of who performs which role(s) is a key part of defining the Trust Framework that will be discussed later.

To see how this works in practise, we will provide examples or the roles in a first party transaction. An extension to the Third Party Access required for an ecosystem model will be given later.

First Party - Single Service



This model shines a light on what happens in many online service flows, as a way to demonstrate all of the background roles. In this case all roles are performed and controlled by the Provider: capturing the initial approach, Identity Proofing, Authorisation process, issuing and reliance on credentials and provision of appropriate resources.

It is a straightforward, familiar transaction for a User, but is limited by the requirements of the Provider, which are typically unique to that use-case: I.e. Users require a different set of Credentials to Identify and Authenticate at each service gateway. Authorisation is then provided through the same connection.

This leads to a proliferation of username/password, PIN validation and reset requirements and is certainly not scalable.

First Party - Separate ID service (SSO / 'login with ... x')



This model starts to address the proliferation of credentials problem, through the inclusion of an external Identity Provider for Authentication. To initiate the contact, the User will typically only need to provide a method of Identity to the Service Gateway.

The User will then need to Authenticate its Identity at the external Identity Provider, which will be passed back to the internal servers for Identity and Authorisation at the service Provider. The Authorisation consent is captured directly from the User. The service Provider is still responsible for all Identity Proofing including linking the federated credential to a real world identity / customer, and the Access Token, Relying Party, and Resource Server are all still within the domain of the Provider.

This is familiar to many Users of Single-Sign-On (SSO) mechanisms within corporate IT environments, or the widely available *"Login with Facebook / Google etc"* function in the consumer space. This typically redirects a User from a service Provider's login page to Facebook / Google etc and captures both Identity (*"Please provide your Facebook / Google details."*) as well as authorisation (*"[service] wants to use your details. Is this ok?"*).

This significantly reduces friction for Users, and allows for User interoperability wherever the Client / Relying Party Authorisation Server and Resource Server are within the same domain. In a full data sharing ecosystem however, the Client / Relying Party (TPP) is different to the Resource Server (Provider), which limits scalability.

Clarifying these Roles and Responsibilities is the first part of defining a Trust Framework.

Vectors

The second part of defining the concept of a Trust Framework is to define the components which need to be followed by whoever is carrying out the roles given above, and to what level they need to be applied¹⁷.

These components are called Vectors Components, and the levels are called Vector Component Values.

The starting point for defining these Vector Components is to look at the specific sector requirements:

- 1. How strong a **proof** is the link between the real world and the virtual identity?
- 2. How safe are the **credentials** from attacks such as theft, takeover or brute-force (guessing)?
- 3. How well is a given credential **managed** or revoked, or whether it expires at all?
- 4. How securely is the assertion protected as it passes over the network?

The general-purpose definitions are set out below. It is important to note that each of these components can be re-defined (or additional components can be added) in a way that is tailored for each sector, but this structure allows the overall approach to be consistent between sectors.

Trust Frameworks

Each ecosystem requires a standardised set of rules and legal requirements that covers all the roles and vectors described above. The current terminology may not be standardised even within a certain sector, but the roles and levels will be - even if they differ by Provider. In general then, the combination of who provides which role(s), and the levels to which they must carry out those roles can be captured in a sector-specific "Trust Framework".

¹⁷ <u>https://medium.com/@justinsecurity/vectors-of-trust-ed52a57fe025</u>

FRAMEWORK IMPLEMENTATIONS:

Options Overview

Following on from the definition of Trust Frameworks in the previous section, we now come to the implementation options that exist for different ecosystems. The key differences between each potential implementation are the existence and scope of any centralisation - i.e. whether there is a shared Identity, shared Authorisation, or both, and where the Proofing requirement sits.

The implementation options that exist for each Trust Framework depend on the capabilities and requirements of that sector. For example, non-regulated industries will not have a central authorisation requirement, so a shared authorisation service will not exist. If they are nonregulated it implies that the data sensitivity may be lower which may in turn facilitate a shared identity being used. Regulated industries may have the central authorisation requirement, but may not offer any way to Authenticate that authorisation.

We have already covered general examples in the Trust Principles section, in the cases of a single User and a single Provider. As a quick aside, we now show that a Trust Framework is essential when the number of Users (both individuals and TPPs) and the number of Providers multiplies.

Although each sector may not yet have a common Trust Framework, there is no ecosystem without one, just a collection of connections in the same sector. A common trust framework significantly reduces complexity, increases scalability and interoperability within the sector as well as opening up options for the type of cross-sector standardisation that Smart Data is pursuing:





Note that the number of connections increases by 1 in this case for each additional Provider or User, but that it increases by 6 in the first case. This demonstrates the complexity and cost benefits. In the OBIE implementation, each TPP still needs to carry out onboarding to each of the Providers (ASPSPs) due to the lack of federated identity (i.e. banks will only trust themselves), and has been estimated at £50k per integration, per TPP, per Bank.

Centralised frameworks shift some of the liability away from the participants, and may require more central set up costs, but massively reduce the complexity of scaling the ecosystem and ultimately reduce ongoing costs for participants. If there is no central framework at all, then the initial set up costs are distributed across the ecosystem, but scaling and ongoing costs are higher, as is the risk of eventual fragmentation.

As a final point, in the fully centralised model, the Authorisation Servers and Identity providers could be unique for each sector, further illustrating how the same framework can be applied across sectors.

Implementations

We have described a number of different implementation frameworks in discussion with OfGem, and will evaluate them in the following section. In a level of additional complexity from the previous diagrams, there are now two parties - the User and the TPP - that need identifying, authorising and authenticating.

Ecosystem - Provider-centric (OBIE)



This model looks at the options for authentication across an ecosystem where the roles of the Client / Relying Party and Resource Server are held by different participants: the TPP and the Provider respectively.

The TPP needs to have a pre-existing relationship with the Authorisation Service, which is unique to each Provider. The Ecosystem depends on each Authorisation Service having a relationship with each TPP, and each TPP having a relationship with each Authorisation Service, hence becomes exponentially more complex with each additional participant.

In the Open Banking / OBIE case, this was the only legally acceptable framework under PSD2 and the only one that the CMA9 were willing to consider. In order to reduce the complex onboarding requirements and authorisation validations processes for Banks (Providers) and TPPs, the OBIE also created a set of B2B identity services that are not shown here. These services are run centrally to reduce economic wastage, improve time to market for new TPP entrants and lower costs for new participants.

Key issues with this model include that Users need to authenticate and authorise for every Bank/Provider that holds their data, and every TPP needs to onboard to every Provider. This requires a significant technical commitment from Providers, as it requires Providers to manage the account details and credentials of all of their Users and the associated TPPs. However it is also the simplest in terms of liability as the majority of actions remain in the domain of the Provider.

Ecosystem - Separate ID and AuthN service (Gov.UK Verify)



This model also looks at the options for authentication across an ecosystem where the roles of the Client / Relying Party and Resource Server are held by different participants: the TPP and the Provider respectively. It is very similar in view to the previously described model, with the main difference being that the external ID Provider now carries the requirement for Proofing. However, there is a much bigger change when looking at implementation from a legal, regulatory and User impact perspective.

The Provider needs to be confident in the external Identity Provider's proofing capabilities, which requires a strong legal framework. The TPP needs to have a pre-existing relationship with the Authorisation Service, which is still unique to each Provider. The Ecosystem depends on each Authorisation Service having a relationship with each TPP, and each TPP having a relationship with each Authorisation Service, hence becomes exponentially more complex with each additional participant.

The principle is familiar to any Users of Gov.UK's Verify service, where Verify is the external Id Provider with responsibilities for Proofing. (In Verify, elements of the Identity provision are further outsourced to one of a number of ID providers). Legislation is still required to extend this beyond the public sector. The EU is also reviewing options for shared eKYC.

Ecosystem - Shared Gateway for ID, AuthN and AuthZ (OfGEM option 1)



This model looks at the options for scaling authentication and authorisation across an ecosystem.

This centralises Authentication and Authorisation so that Users have a single starting point for all of the ecosystem services and is one of the options discussed with the Pensions Dashboard and midata/OfGem over the past 18 months. It does not rely on an explicit relationship between the TPP and the Provider, and does not rely on an explicit relationship between the User and the Provider. In the OfGem case, the premise was that many Users may not even know who their Provider is.

As in the previous model, the Provider needs to be confident in the external Identity Provider's proofing capabilities but now also needs to be confident in the Authorisation. The TPP still needs to have a pre-existing relationship with the Authorisation Service, but now so does the Provider. Each of these relationships only need to be established once for each TPP or Provider so the system is highly scalable. The Authorisation on-boarding could be achieved for the Provider through the same mechanism as the TPP on-boarding.

Although this does solve many problems within an ecosystem, the cross-sector implementation is limited unless there is a shared gateway for authentication that can identify ALL Users. OfGem were considering an SMS authentication mechanism to perform universal authentication of Users although this requires an a sector-specific identifier (e.g. address for OfGem) which may not be transferable to other use-cases such as Pensions.



Ecosystem - Shared Gateway and Separate ID



This model combines features from previous models and aims to deliver a solution that is scalable both within and across sectors. It brings together the Shared Gateway model, but adds an option for external Identity to be incorporated.

From a User perspective this should be very clear and could rely on existing Provider IDs (or Bank IDs, or Verify) as the Identity service. It is technically the least complex method and will be the cheapest to implement. However it will also require a solid legal framework for the shared gateway service, investment in the standardisation of technical digital identity standards in the UK, and a suitable commercial incentive for participants.

Several of the CMA9 banks are however looking to deliver digital identity propositions within the next 12 months. This means that these Identity provision elements can be added to the previous model when they become available.

Note that all of these models are still concerned with the framework that needs to be implemented. There are still technology choices that need to be made, but these can only happen once the framework is agreed.

SMART DATA ALIGNMENT CHALLENGES

In this section, we will look at the key principles required when aligning sectors. We will then consider the technology options that exist and finally suggest a way to bring all of this together across sectors.

Symmetry

Implementation of a common mechanism for Smart Data will require a commitment to symmetry across sectors to build sector-specific details into the Trust Framework principles described earlier.

The levels of user assurance and requirements of regulation differ across sectors. To avoid any asymmetry in services and responsibilities, TPPs carrying out equivalent services should be regulated to the same level as the appropriate Providers.

Challenges in encouraging common cross-sector mechanisms for Smart Data are underpinned by the differences in mechanisms that exist within sectors. This is primarily driven by the considerations covered in the Trust Requirements chapter. High High Low Low High Provider Regulatory Requirements

TPPs need equivalent regulation to Providers for the relevant services.

Symmetry Principle 1: User Experience

The authentication experience for Users should be equivalent whether they go direct to the Provider or via the Third Party.

Symmetry Principle 2: TPP Regulation

TPPs need equivalent regulation to Providers for the equivalent services, not more or less.

On the User experience, there is still a challenge in ensuring adequate security where Users are using the same identification and authentication processes across sectors. Official advice from the National Cyber Security Centre¹⁸ suggests that the sector with the most stringent

¹⁸ <u>https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management</u>

requirements should be taken as the base model. This could impact the User experience at a sector level where requirement are very different and mean there is a potential asymmetry between sectors - i.e. Bank-grade secured login could be used for Online Groceries, but not the other way around. Principle 1 stands to ensure that symmetry should be preserved within each sector.

The TPP regulatory point is similar: Open Banking TPPs should be regulated more strongly than Open Grocery TPPs, but for cross-sectoral regulations it may be that an Open Banking license can provide much or all of the required approvals for Open Grocery. This principle of federation is explored more below.

Any cross-sectoral authentication mechanisms needs to be capable of capturing those differences in TPP regulatory roles and User experiences. We believe that the Trust Framework construction can meet these needs.

Federation

One of the key ideas to consider when looking at cross-sector usage of credentials is that of Federation. This involves a shared usage of credentials for all or part of the authentication flow, which may be enhanced by additional local checks. A local example of federation is Single Sign-On for business applications.

Federation can occur at different points within the User journey.¹⁹ Examples include:

An organisation can accept credentials issued by another organisation, but still authenticate and authorise the individual locally:

• A passport issued by one country is accepted as a valid credential by a foreign country, but that second country's immigration office still authenticates the holder and may also require a visa (authorisation).

An organisation can accept specific characteristics (attributes) describing an individual from another organisation:

- Your bank will request your credit score from one of the credit reference agencies, rather than maintaining all that information itself.
- Your credit reference agency in turn relies on different attributes sourced from other sources such as banks and utilities in order to build up the credit score.

An organisation can accept an authorisation decision from another organisation:

- A driver's license authorising you to drive in one country is accepted by another.
- It may be only partly equivalent e.g. the full driving license from your home country may only authorise driving an automatic transmission vehicle when on holiday, or may only be valid for a period of time before a local driving test needs to be taken.

¹⁹ <u>https://arch.idmanagement.gov/services/federation/</u>

Technology

Technical choices need to be made to ensure that any implementation provides a strict and consistent base to be credible, but retains the flexibility to adapt to multiple sectors. This implies open-source standards. These standards are widely available, widely understood, and have been tried and tested. In addition, there are a choice of partners who could manage any technical build, meaning the commercial market is maintained.

We will first look at the options for the foundation layer - the authorisation framework, then the identity layer, then the security layer:



The Base layer needs to provide a strong foundation, so is driven toward wide availability.

The Identity layer and Security requirements depend more on the policies and Trust Frameworks required by the individual sectors.

Base Layer

At the foundation layer, there is an industry standard protocol for **authorisation** (not authentication) called OAuth2.²⁰ This is used by Apple and Google among others and provides a framework for the authorisation of delegated, limited access to data resources owned by Users. The framework defines many of the roles and responsibilities necessary to grant authorisation but it does not specify to any great extent either operationally or technically how those roles need to be performed.

Crucially it also does not specify, or really care, WHO is granting or being given that authorisation. It certainly does not cover what the level of proof needs to be, nor specify how that proof should be given. It is authorisation without identification.

This means that OAuth2.0 is flexible and applicable to a wide range of applications, or, in a Smart Data context, to a wide range of sectors. However, this very flexibility can lead to interoperability problems because it does not profile implementation-specific details such as the technical requirements for token contents or encryption mechanisms.²¹

Identity Layer

So, the next layer on top of the base is concerned with confirming WHO the participants in the authorization chain are, and what the level of confidence is in those claimed identities. This layer adds to the authorisation by capturing Who the User is, How they were authenticated and When that authentication occurred.

²⁰ <u>https://tools.ietf.org/html/rfc6749</u>

²¹ https://www.gluu.org/resources/documents/articles/5-reasons-you-need-openid-connect-and-uma/

There are two widely available blocks for this layer, which both extend OAuth2.0:

- OpenID Connect (OIDC)²²: This adds an ID Token and further defines technically how participants in the OAuth2.0 framework need to perform their functions. It is widely considered as the identity protocol for the internet. OpenID Connect supports Customerto-Business (C2B) data and Identity information sharing, and is the protocol underpinning "Login with Facebook / Google / Microsoft" etc.
- User Managed Access (UMA)²³: This is a more recent standard that supports Personto-Person sharing via Businesses (C2B2C) amongst other extensions. Implementation requires the authentication of both individuals and therefore deployment of a common authentication and authorization service for those individuals. This does not exist in the UK at present.

Of the two options given above, OpenID Connect is the more widely deployed: it has been used in the successful reference implementations of open banking in the UK, New Zealand and Australia and is actively being adopted by FDX in the United States. Coupled with the Financial-Grade API security profile, this is rapidly becoming the gold standard for open banking around the world.

UMA in theory provides greater granularity of control in that it allows a specific user to make demands of the requesting side in order to test their suitability for receiving authorisation. This could include restricting access to a specific individual, not just a specific system. UMA has been successfully deployed within a single authorisation domain to enable scenarios such as the sharing of bank account information between accounts held at the same bank or enabling parent/child access to services or data held by the same service provider.

Implementation of UMA requires more granularity and centralisation of User Identification systems, which introduces additional complexity. However, given that UMA is a profile of OAuth2.0, it is possible to introduce this capability to a wider OAuth2.0 ecosystem should person to person data sharing be required and the ability to authenticate both individuals be available.

Security Layer

To ensure appropriate security for the sensitivity of the data being shared, we need to agree Profiles that confirm what mechanisms and options are available to participants. This has a double benefit in that it both increases security AND increases interoperability for the ecosystem.

Several different OAuth2.0 profiles exist including the Financial-Grade Profile (FAPI)²⁴, the HEART profile²⁵ for the healthcare sector and Core²⁶ which is used by social media companies. These profiles are managed by industry-specific representatives as well as security and data sharing subject matter experts.

Raidiam's CTO is a recognised significant contributor to the FAPI Security Profile which is currently considered to be the gold standard for all OAuth2.0 data sharing ecosystems globally.

²² http://openid.net/connect/

²³ <u>https://kantarainitiative.org/confluence/display/uma/Home</u>

²⁴ https://openid.net/wg/fapi/

²⁵ <u>https://openid.net/wg/heart/</u>

²⁶ <u>https://openid.net/specs/openid-connect-core-1_0.html</u>

The security characteristics of the FAPI profile have been formally proven and independently verified by Cornell University Security research.²⁷

Profiles do need active management to remain relevant and facilitate innovation. This means that an Ecosystem needs to plan potential changes into its roadmap. Thanks to efforts of Open Banking in the UK and the Consumer Data Right in Australia, FAPI is widely supported by the technology industry and so can easily be implemented for any sector or company.

²⁷ https://arxiv.org/abs/1901.11520

Visibility

The biggest challenge in encouraging the design of common mechanisms for Smart Data is that the sector-specific frameworks are not clearly standardised or understood. We believe there is a great benefit from increasing the visibility of these overarching frameworks to ensure common starting points.

Without alignment of principles, the likelihood of aligning the outcomes will be very low:

- If the task is "Draw a vehicle", there will be many different outputs.
- If the task is "Draw a sports car", you are much more likely to get initial alignment.

Further investigation and discussion with different sectors is now required to increase visibility of the Trust Framework model and then determine the required Trust Frameworks. Only then can the sector-specific details be developed successfully and commonalities confirmed.

This focus on the Trust Framework is now the approach being adopted in Australia as part of their implementation of the Consumer Data Right (CDR). The legislation launched in November 2017 with an ambition to give consumers in all sectors greater access to and control over their data²⁸. The Australian government proposed starting with the banking sector followed by the energy sector, with telecoms in scope further down the line.

The initial start date was supposed to be February 2020 but his was pushed back to July 2020 by the Australian regulator, citing challenges which refer to the trust framework:

"Robust privacy protection and information security are core features of the CDR and establishing appropriate regulatory settings and IT infrastructure cannot be rushed."

- ACCC Commissioner Sarah Court, Dec 2019²⁹

The UK implementation started with the design of a Trust Framework, and launched the technical directory and supporting services realising that framework and ecosystem within 13 months.³⁰ In contrast, the Australian implementation plans are still ongoing after nearly 2.5 years with detailed technical commentary highlighting the lack of agreed fundamentals of authentication, authorisation and consent from the Australian banks as a major contributing cause of delay and calling on the industry to build out from the successful implementation in the UK.³¹ In parallel with this, the Australian energy sector has recently flagged concerns that cross-sector application of standards will not work unless all sectors are included in the detailed consultation process.³²

²⁸ <u>https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0</u>

²⁹ <u>https://www.accc.gov.au/media-release/consumer-data-right-timeline-update</u>

³⁰ <u>https://www.openbanking.org.uk/about-us/</u>

³¹ https://github.com/ConsumerDataStandardsAustralia/standards/issues/99

³²https://github.com/ConsumerDataStandardsAustralia/standards/files/4484079/AGL.submission.concurrent.cons ent.target.state.-.9.April.pdf

CONCLUSION

Authentication is a key part of a Trust Framework. Trust is at the heart of all smart data sharing implementations. Alignment on the definitions and principles is required before alignment on the authentication mechanisms can occur.

Different sectors have different roles, regulations and requirements, but there is a framework of vectors that can be used to capture all of these consistently. From that baseline, agreement on the implementation requirements can be developed. Authentication mechanisms can be developed to fit those frameworks and technology choices can be made.

Recommended Next Steps

Review of Usability / Implementation experiences (with suggested contacts)

- Alignment and combination of the current research pieces to complete the requirements for a Trust Framework from a Consumer (User), Legal and Technical point of view.
- Further detailed review of existing framework models focussing on usability and implementation:
 - Open Banking via OBIE
 - Verify.Gov via GDS
 - o midata via OfGEM
 - CDR via ACCC / Data61
- Apply this to all Smart Data implementation target sectors and map out requirements for consultation, discussion and agreement.

Deliver a Technical Proof of Concept to understand the presented Trust Framework options in action.

 Delivery of a high-level technical proof of concept for a flexible trust framework that can be used for live testing of Authentication and Sign-up processes, plus a sample Accreditation Hub / Directory. (This step proved decisive for unlocking stakeholder agreement in the original Open Banking Working Group)

Proposal: Raidiam has unique global experience in designing, developing and delivering a trust framework for a thriving ecosystem, and would be very pleased to offer further support to BEIS on the next steps recommended above.

This publication is available from: www.gov.uk/beis

If you need a version of this document in a more accessible format, please email <u>enquiries@beis.gov.uk</u>. Please tell us what format you need. It will help us if you say what assistive technology you use.