Department for
Business, Energy
& Industrial Strategy

Smart Data Research

Report: Third Party Accreditation

BEIS Research Paper Number 2021/029

Prepared by Raidiam Services Limited

RAIDIAM

Authors: Faith Reynolds, Tim Johnson

June 2021

Acknowledgements

With thanks to all who have contributed directly and indirectly to the delivery of this report.

In particular, those pioneers who have worked to set the foundations for secure and safe data sharing in the UK through the formation of Open Banking Implementation Entity; to those who created the original blueprint for Smart Data through the creation and operation of the UK's open banking ecosystem; and to those already working on the applications for Smart Data principles in practise around the world.

Any enquiries regarding this publication should be sent to us at:
enquiries@beis.gov.uk

Contents

Introduction

The overarching aims of Smart Data are to ensure that individuals, business and society can get reliable value from sharing their data through vibrant, sustainable and competitive markets where potential harms are mitigated. By combining consumer data with appropriate product and performance data, and by providing a seamless and interoperable framework for data sharing, innovators will be empowered to develop new ways for consumers to benefit from their own data. [1]

Smart Data initiatives exist to "facilitate the secure sharing, upon request by the customer, of customer data with Third Party Providers (TPPs), who use this data to offer innovative services for the customer." [2]

The UK's data protection laws already give consumers the right to request that businesses provide their data to TPPs in a commonly used format - this is known as the right to data portability. 'Smart Data' represents a logical extension of this right and provides an enhanced framework for sharing consumer data that allows for further innovation[3].

This enhanced framework includes the use of API Standards to allow consumers to share their data swiftly and securely with TPPs. It also includes adherence to common technical standards, data formats and definitions to ensure interoperability and to minimise barriers for TPPs, ensuring that the Data Providers can trust any of the TPPs within the accreditation regime[4].

Trust is the foundation of all data sharing. Options for implementing trust in bi-party digital transactions have been around for many years. However, implementing Trust across a distributed, secure, data sharing ecosystem is a challenge that has only been tackled in the past few years in the wake of technological and regulatory changes.

There are a number of Smart Data and data portability initiatives in different sectors including Open Finance, the Pensions Dashboard, the nascent Open Communications as well as voluntary initiatives like Open Energy, Open Savings, Investments & Pensions (OSIP) and Open Insurance.

This research aims to support the development of policies to enable and coordinate these initiatives, which should facilitate individual sector implementation as well as set strong foundations that can be applied on a cross-sector basis. There are a number of steps that government, regulators and participants need to take to implement and realise the benefits of

[1] "Smart Data Consultation": https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808272/Smart-Data-Consultation.pdf
[2] This research invitation: BEIS CR21008 ITQ
[3] "Smart Data Consultation": https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808272/Smart-Data-Consultation.pdf, page 11
[4] Ibid.

Smart Data in any sector, with this paper focussing on the Accreditation of Third Party Providers.

The key questions BEIS asked for this research are:

- *What conditions may TPPs need to meet in order to be accredited; deeming them appropriate to handle customer data?*
- *How do these conditions vary across sectors (e.g. lessons from Open Banking and other existing or planned sector accreditation schemes) and where could these be standardised?*

Raidiam is delighted to deliver this research, which builds on the 2020 Research Paper on Authentication and Trust in Smart Data ecosystems[5]. We look forward to demonstrating how the experiences and expertise developed and delivered firstly for open banking in the UK have been modified and adopted for open banking in Brazil and Australia, and how they may further extend for implementation into other sectors.

Note on terminology

The terms ‘Smart Data’ and ‘Open X’ are used interchangeably in this report to reflect both the government focus on ‘Smart Data initiatives’ and the increasing global naming convention for such implementations to be called ‘Open X’. In both cases, we focus on the secure sharing, upon request by the customer, of customer data with TPPs.

We acknowledge that this may be inconsistent with the definitions and the use of the word “Open” by the Open Data Institute (ODI).

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909365/Raidiam_Authentication_Research_Response.pdf

Executive Summary

The definition of accreditation is simply "the action or process of officially recognizing someone as having a particular status or being qualified to perform a particular activity." However, the challenge is to define the principles and concepts of the "official" regulation role, of "status" or "qualification" and also to consider the dimensions of "activities" that they may undertake.

In practice, accreditation is a very broad church, encompassing the high level regulations that exist in GDPR, the sector-specific regulations that confer access to the regulated roles, and the technical conformance that may accredit the actual technology implementation.

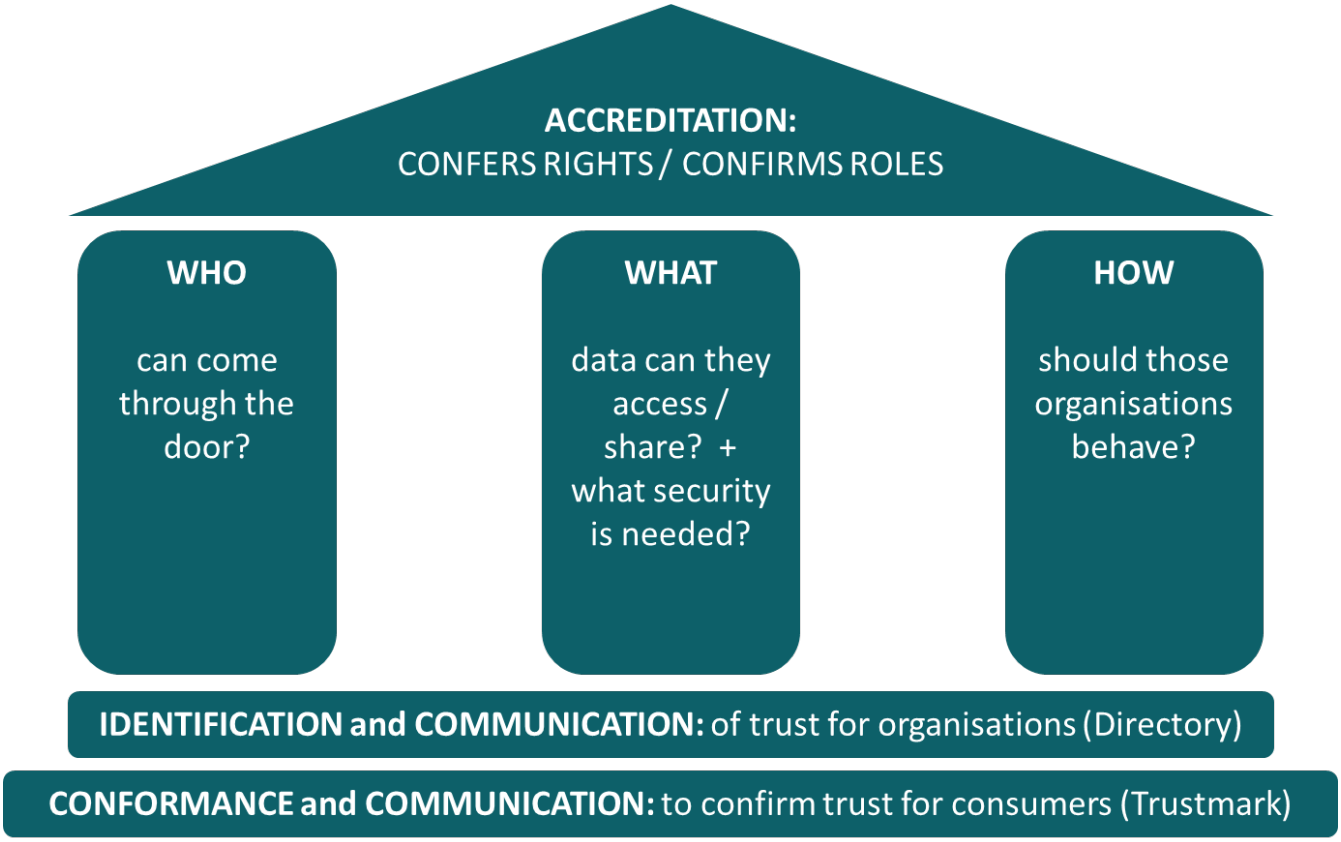


Figure 1: Three Pillars of Accreditation. Underpinned by Communication Benefits.

An accreditation framework helps create trust in the data sharing ecosystem by:

- **conferring rights** on participants to engage in the ecosystem;
- improving transparency between participants by making providers **identifiable**
- enabling providers to **communicate** their trustworthiness
- monitoring their **conformance** with the requirements of accreditation.

BEIS asks two research questions:

- *What conditions may TPPs need to meet in order to be accredited; deeming them appropriate to handle customer data?*
- *How do these conditions vary across sectors (e.g. lessons from Open Banking and other existing or planned sector accreditation schemes) and where could these be standardised?*

Before answering what conditions TPPs may need to meet in order to be accredited or how these may be developed across sectors, it is important to first understand what a TPP is being accredited for.

Data sharing is not yet standardised across initiatives. Accreditation regimes are still being developed. Options exist even within similar sectors to implement accreditation of similar roles in different ways, depending on existing regulation, validation and infrastructure. The need for more or less onerous accreditation depends on the risks associated with the data being accessed. It also depends on the extent to which other legal or regulatory drivers interact. For instance, the strength of an accreditation regime may be offset through a more or less stringent monitoring and enforcement regime.

The UK's Open Banking initiative has broken new ground and provides a useful blueprint for how Smart Data might develop. It points to a series of decisions government and regulators need to make to underpin accreditation and ensure Smart Data is a success. These include:

- Classification of data and the risks associated with sharing data an accreditation framework may seek to mitigate
- The definition of participant roles in the data chain and associated responsibilities
- The rights of access to data TPPs may have
- The scope and ownership of the accreditation framework
- Conduct rules for the fair treatment of consumers and access to redress

Case studies from the implementation of accreditation show that there is no standardised way to implement an accreditation regime. They highlight the interaction between different layers of accreditation from high level regulation to low level technical conformance. But they also demonstrate the universal requirements for validation of identities and roles, and the communication of those identities and roles in a secure manner.

Analysis demonstrates that there are similarities to conditions for accreditation across sectors and these could be standardised for Smart Data. However, it is likely that standardisation of accreditation can only feasibly be introduced for 'read' access at this point. 'Write' access for TPPs is higher risk and is more likely to be sector specific and less open to standardisation.

Once TPPs have met accreditation requirements in one sector, they could be granted a 'passport'. This passport would 'fast-track' a TPP's application to access data from another sector and if successful provide them with a 'visa stamp' for the additional sector. This reduces

friction for a TPP. However, it would still ensure sector regulators have oversight and can mitigate risks of TPPs from other sectors entering their ecosystem.

Communicating accreditation securely between participants can be achieved through a Smart Data Directory, similar to an Open Banking Directory. As participants become accredited for new sectors, this can be reflected on the Directory. A single Directory is preferable to multiple directories, to reduce friction for all participants, maintain interoperability and support market efficiencies.

There are also opportunities to standardise aspects of monitoring, enforcement and reporting to reduce the regulatory burden of supervision. Such automation and centralisation of repeatable aspects will free up regulators to focus on problem areas or new developments.

Supervision, enforcement and reporting functions are required to ensure that the accreditation regime is robust and delivers the trust needed to facilitate cross-sector data sharing.

In Part 1 we explore what accreditation is, what TPPs might be accredited for, and the key elements of accreditation that need to be decided upon in a Smart Data regime.

In Part 2, we outline a number of existing and emerging accreditation approaches in the UK and internationally. We summarise key areas for the standardisation of cross-sector data sharing and the types of conditions TPPs may need to satisfy to be accredited.

Finally, in Part 3 we summarise our recommendations.

PART 1: Accreditation

BEIS asks two research questions:

- *What conditions may TPPs need to meet in order to be accredited; deeming them appropriate to handle customer data?*
- *How do these conditions vary across sectors (e.g. lessons from Open Banking and other existing or planned sector accreditation schemes) and where could these be standardised?*

Before answering what conditions TPPs may need to meet in order to be accredited or how these may be developed across sectors, it is important to first understand what a TPP is being accredited for.

In Part 1, we define what accreditation is, the objectives of accreditation, what it should achieve, the differing approaches to accreditation in the ecosystem and the key functional requirements of accreditation BEIS must decide on in delivering an accreditation framework. We finish by concluding a series of design principles that accreditation for Smart Data should deliver.

Definitions

The dictionary definition of 'accreditation' is:

> ***accreditation***[6] */əkrɛdɪˈteɪʃ(ə)n/*
>
> *(noun) the action or process of officially recognizing someone as having a particular status or being qualified to perform a particular activity.*

At first sight, this appears to be a straightforward definition. However, challenges arise when trying to work out what that definition means in reality, and how to put that into practise:

- *"The Action or Process"*
  implies there is/will be a process, which can/should be documented
- *"Of officially recognizing"*
  requires there to be an official entity that can carry out that process
- *"Particular status/qualification"*
  requires definitions of roles (and possibly responsibilities)
- *"Particular activity"*
  further detail on the actual activity to be carried out (i.e. end user use case)

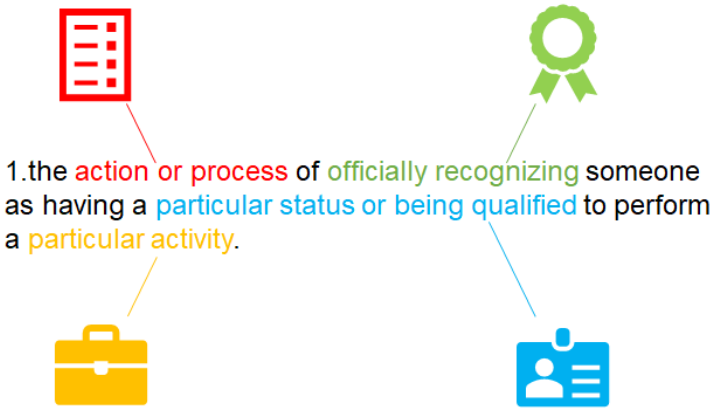


Figure 2: The dictionary definition of 'accreditation' highlighting each element in the list above.

As part of its own enquiries into Smart Data, BEIS has identified that an accreditation framework should establish the requirements and ongoing conditions for third parties to access data with the consent of the data subject, and the process for becoming accredited by meeting those requirements. It should include a mechanism or 'official party' which monitors compliance with such requirements, and revokes accreditation if required.

Creating, maintaining, and sharing a record of accredited TPPs is a further aspect of an accreditation framework BEIS has identified. Accreditation itself should communicate to all parties in the system that the TPP has met these requirements.

[6] Source: https://www.lexico.com/definition/accreditation

In practice, an accreditation framework helps create trust in the data sharing ecosystem by:

- **conferring rights** on participants to engage in the ecosystem;
- improving transparency between participants by making providers **identifiable**
- enabling providers to **communicate** their trustworthiness
- monitoring their **conformance** with the requirements of accreditation.

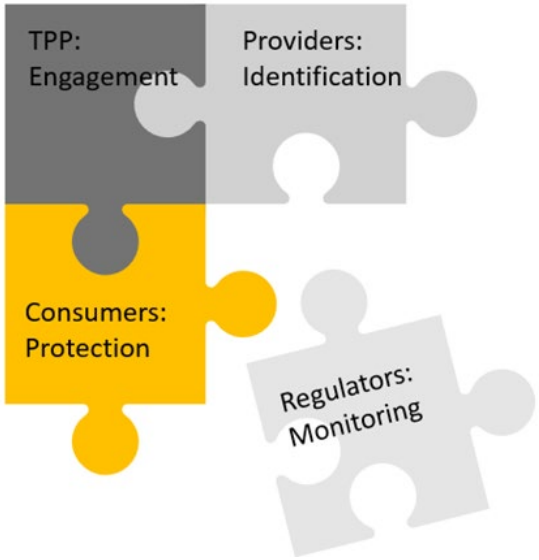


Figure 3: Puzzle pieces containing concepts in the list above - showing that accreditation provides benefits for all parties in the ecosystem.

Purpose of accreditation

Accreditation should support market integrity, reduce friction between parties in the data sharing chain, create a protective layer for consumers and facilitate easier oversight of the data sharing ecosystem by government and regulators. We explore these themes below.

Accreditation gives participants equal access to the ecosystem which facilitates 'a level playing field' for competition. It provides protection for all parties by ensuring the roles and responsibilities of participants are known in advance, and can be verified throughout the lifecycle of the relationship. Accreditation helps form the basis for liability arrangements which regulators or participants can put in place. It creates certainty in the market about governance, security and conduct requirements of firms which in turn facilitates operational resilience and sustainable markets. Firms that do not meet the standards of accreditation are required to improve, or to leave the market.

Additionally, in the context of the wider Smart Data initiative, accreditation should make it possible for participants to share data not just within sectors but also across sectors.[7] Cross-sector accreditation allows for a standardised approach to access data from different sectors. This supports efforts to deliver cohesion and interoperability in data-driven markets.[8] Cross-sector accreditation is important because reducing the friction associated with onboarding to different regulatory authorisations and accreditation schemes enables TPPs to access data from a wider range of markets more easily. The potential for innovation grows when datasets are combined, so facilitating TPP's access should increase innovation and competition leading to better outcomes for individuals, businesses and society.[9]

Simultaneously, accreditation also forms a layer of protection for consumers: providers have had to meet certain robust criteria before selling consumers a product. Where providers are accredited, consumers can also much more easily enforce their own right to recourse in the event something goes wrong. This reduces the likelihood and impact of 'privacy shocks'[10] (episodes which reduce consumer trust or make them less willing to buy some companies' products). The experience of Open Banking in the UK highlights that consumer confidence is key to acceptance of any new service, and that a vibrant ecosystem will ultimately be driven by the consumer.

Likewise, accreditation provides for easier oversight by regulators and government. It allows them to set requirements for accreditation which promote the public interest and well-functioning markets. Combined with sectoral regulation, accreditation should ensure that the way data is used by third parties is transparent, does not abuse the trust of users, and does not lead to negative or harmful practices for consumer or business users. The process of

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/965687/KalifaReviewofUKFintech.pdf page 26
[8] https://www.fca.org.uk/publication/documents/cohesion-interoperability-advisory-group-open-finance-advice-note.pdf
[9] https://theodi.org/article/innovation-using-old-ideas-to-create-new-ones/
[10] Ibid.

accreditation facilitates levy raising (to fund data sharing bodies) as well as measurement of the market and how data sharing is contributing to the needs of both society and the economy.

Consistency in approaches to accreditation then will help TPPs access multiple markets and could boost customer confidence and trust.

Accreditation ecosystem

There are a number of bodies within the data sharing ecosystem that can and do take responsibility for accreditation. In this section we explain how those different bodies have operated within our most advanced data sharing ecosystem, Open Banking. We extrapolate from this the key pillars of accreditation that must be addressed and how these are dealt with when there is no regulatory mandate to share data.

Hierarchy

Data sharing ecosystems are typically governed by two ostensibly opposing forces: one, the requirement to share and the other the need to secure. Implementation of a fully functional, vibrant ecosystem requires many layers of validation, with each layer needing to address the two needs.

By way of example, this is achieved in Open Banking through the framework legislation that exists at European level in PSD2 and GDPR, and at a UK level through the CMA Order.

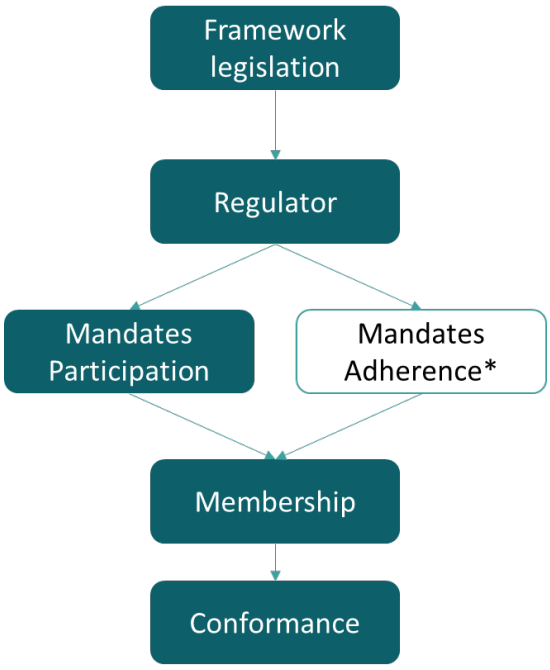


Figure 4: Hierarchy of accreditation bodies within an ecosystem.

PSD2 mandates that TPPs have access to consumer data (with consumer consent) held at data providers and is brought into legislation in the UK through the Payment Services Regulations 2017 governed by HM Treasury and the FCA. The CMA Order requires that data sharing is done in a standardised way. GDPR requires that the data is secured.

The CMA Order is then enacted through the 'membership'[11] of the Open Banking Implementation Entity and conformance is achieved through the technology (the Directory). As long as a TPP has been authorised or registered at the FCA they can onboard to the Open Banking Directory and access data from data providers without the need for any bi-lateral, multi-lateral or scheme contract involving other participants. PSD2 legislation sets out the data

[11] We use Membership here in the broadest sense, rather than legal. No TPP is required to sign up to a 'membership' at Open Banking Limited. However, they are required to onboard and sign Terms and Conditions with Open Banking Limited.

TPPs can access, how they can expect data providers to provide it, and the majority of liability arrangements.[12]

Pillars

Open Banking and PSD2 provide a helpful and holistic example of how data sharing can be effectively enabled. However, other Open X initiatives do not have the benefit of legislation or regulation in the same way and are having to scope out how they will achieve the same aims through different means. Our analysis demonstrates there are three key pillars these initiatives have to address:

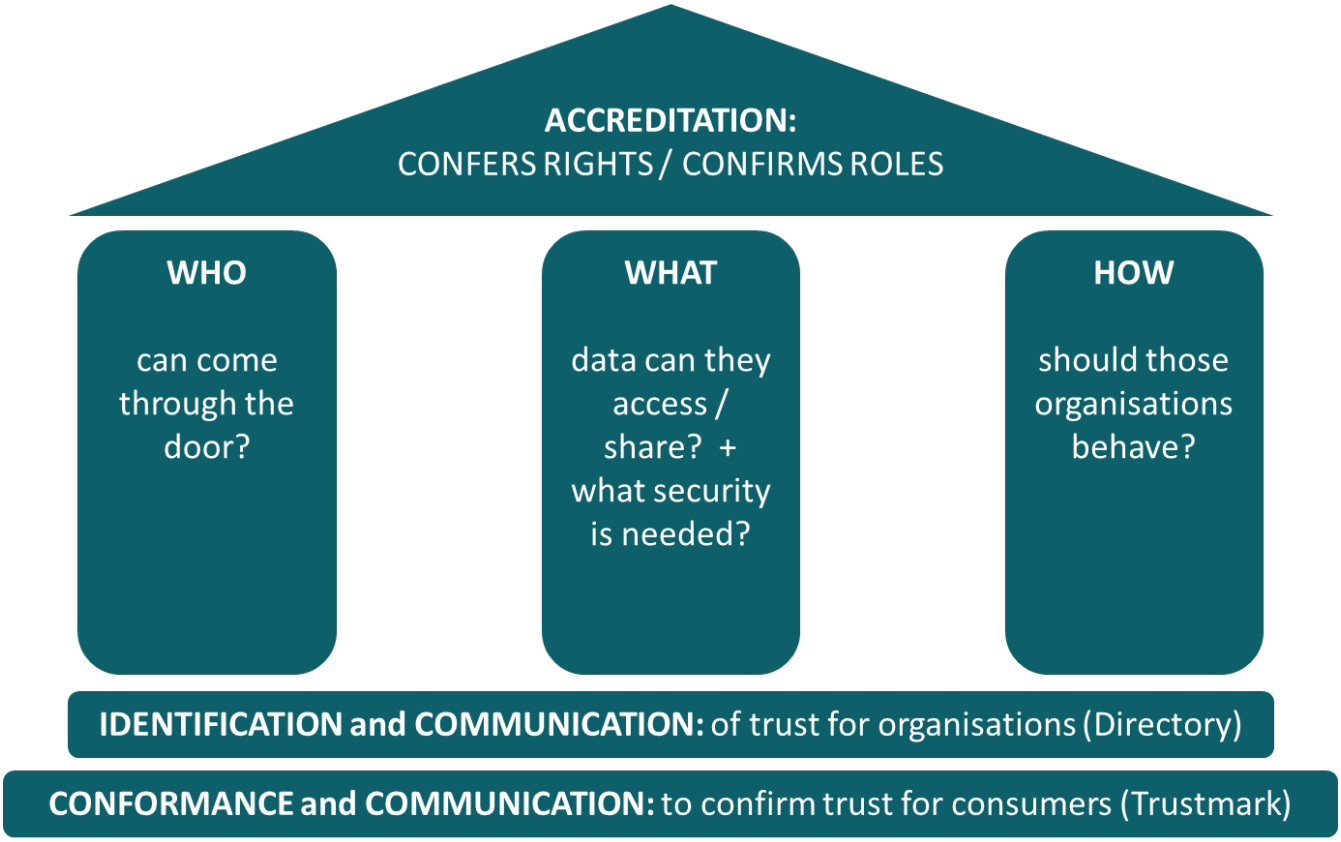


Figure 5: Three Pillars of Accreditation. Underpinned by Communication benefits.

- *Who can come through the door?* i.e. what requirements are there on a participant to prove itself fit and proper and to whom should it prove itself fit and proper?
- *What data can a participant access or share? And what security is needed to do so?* i.e. what needs to be in place to secure the data, and to secure the transmission of data?
- *How should organisations behave with regards the data?* i.e. what can they do/not do with the data they access, what services they must provide to the data subject and what responsibilities do they have if/when something goes wrong?

[12] Please see BEIS research on Liability and Redress which highlights outstanding issues in relation to liability in data sharing scenarios. https://www.gov.uk/government/publications/smart-data-research-on-consent-liability-and-authentication

Although those three pillars hold up the roof of accreditation, they are also underpinned by the foundations required to communicate trust across the ecosystem, namely:

- How participants identify other participants, and communicate trust that they have met the 'fit and proper' requirements for accessing the data *(via Directory)*
- How participants conform to the standards, and communicate that conformance, both to other participants *(via Directory)* and to consumers *(via Trustmark)*.

Voluntary approaches to accreditation

Where there is no regulatory mandate on a data provider to share data (and therefore no right of access for a TPP), the agreement to share data has to be agreed through consensus between data providers and TPPs. In a very limited way this can be achieved through a bi-lateral contract. The legal contract sets out who the TPP is, what data it may access, how it may access data from the data provider, and where liabilities apply. This is possible today but is not a scalable solution, is costly both for the TPP and the data provider and does not promote innovation or competition.

Alternatively, data providers and TPPs can form a group which is bound by a single contract or series of contract templates.[13] This group determines the rights of access to data, the basis for who can access the group and the liability arrangements. This approach reduces the friction but voluntary governance has weaknesses. Governance may exclude certain legitimate parties from entering the membership or the cost of joining may exclude smaller participants, creating an anti-competitive framework. It may also struggle to enforce the requirements on participants where there are no legislative requirements on firms to share certain data, behave in certain ways or make good certain arrangements (e.g. timely transfer of data).

Again alternatively, a group of data providers and TPPs may agree to share data in a standardised way and conform to certain technical requirements but agree the individual access rights, liabilities and responsibilities on a bi-lateral basis. This approach creates some security but increases friction. It may also suffer with similar governance issues outlined above.[14]

In all scenarios, there is a scaling benefit to agreeing not just the standards, but also the communication mechanism for confirming how well participants meet those standards. This is best exemplified by the use of a Trust Platform such as the UK's Open Banking Directory. This Directory securely communicates identity and authorisation attributes for all participants. Without a single centralised Directory, each participant would need to agree, communicate and validate each and every other participant separately in order to guarantee security.

[13] This is the approach adopted by TISA for the TISA Exchange (TeX) initiative: https://tisaexchange.co.uk/
[14] For instance, the Open Banking Implementation Entity is facilitating the development of a data sharing Standard for Extended Customer Attributes for a group of Data Providers. However, the Standard has not identified the requirements for participants to access the data (which is governed by GDPR only) or set out the liabilities. Data Providers currently (March 2021) expect to mitigate the security risks through bi-lateral contracts.

There is a variety of options for accrediting Smart Data and the approach the government takes will determine the extent to which its accreditation regime addresses the who, the what and the how of our accreditation framework above.

Functional requirements of accreditation

Where accreditation is mandated, key decisions are required of government about both the functional and supervisory requirements. However, the different pillars of accreditation can be focused in different ways to achieve the desired outcomes.

Functional requirements	Supervisory and policy requirements
• **Classification of data** and what data should be made available to share • Definitions of **Roles of participants** that provide, access and use data • **Rights of access** to data by TPPs (and/or conversely requirement for Providers to share data) • **Requirements for accreditation** that all participants need to meet (by role) • **Validation process** for accreditation requirements having been met	• **Monitoring** (and extent of monitoring) of accredited participants • **Enforcement** against participants that do not meet the standards of accreditation • **Reporting** on the accreditation framework, effectiveness and market development

In the table above, note the relationships between the burden of sign up for the TPP and how this might relate to the level of ongoing supervision and scope for enforcement. For instance, GDPR places a very low barrier to entry for firms at sign up. However, it has strong enforcement powers should it identify a participant that is not acting in line with the regulation. The focus is on credible deterrence rather than pre-approval to participate. However, in other markets, such as financial services, there is a higher bar for accessing the market as well as the credible deterrence.

In both approaches, supervision is always a challenge given the resources of the regulator and the size of the market. Therefore, finding technological ways to ensure participants comply can reduce the burden of supervision, for instance, through ‘technical conformance’ (see our appendix, Conformance, for more detail).

A harmonised approach to accreditation for TPPs across sectors is needed to ensure a successful ecosystem and to inspire confidence across different regulators.

Below, we explore other key decisions that are required to create an effective and harmonised scheme: the classification of data, the definition of participant roles, the rights of access to data and ownership of an accreditation entity.

Classification of Data

The strength of an accreditation regime depends on the risk associated with the data it seeks to mitigate. The risks of data being accessed or used illegally are aligned to the sensitivity of the data. Sensitivity may be defined by the extent to which it identifies an individual person; the commercial nature of the data; or even the extent to which releasing the data would have an impact on national security. Such sensitivities can be used to define whether data is made open to all, shared among a group of accredited parties, or is closed to all but very limited parties through bi-lateral contract.[15]

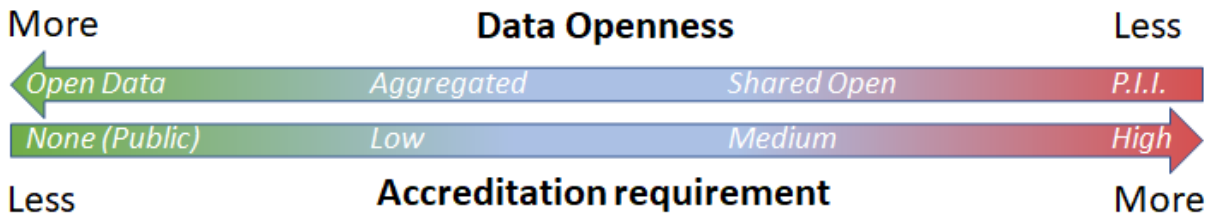


Figure 6: Graduated arrow showing the relationship between Data Openness and Accreditation Requirement - "More" Open Data requires "Less" accreditation and vice-versa.

[15] By way of example, at the point of writing, Open Energy is consulting on its data classifications: https://docs.google.com/document/d/1A9Aj7uW5DEkhZjdBw5JI6t7qi_ojMIeKrBxyDWhD2n8/edit#

The definition of participant roles

As we saw in our paper on Authentication and Trust[16], in any data sharing transaction, there is a number of consistent roles of participants that provide, access, manipulate and use data:

One authorised party will hold and provide the data ("Provider" role) to another authorised party who will request and access that data ("Accessor" or "Third Party" role). Where Smart Data or sensitive data is involved, then the "Consent Provider" (under GDPR, the 'data subject') should be required to provide consent.

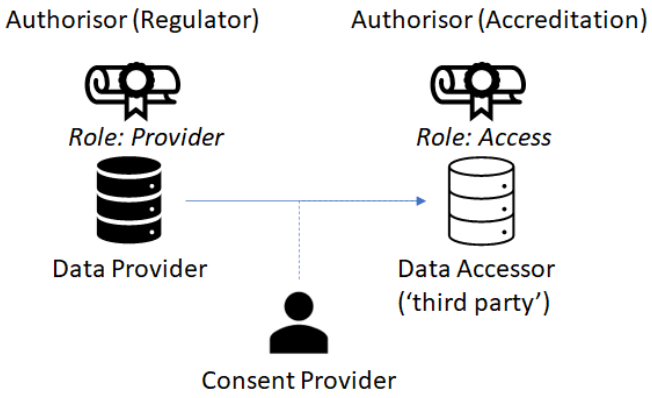


Figure 7: Blocks showing the typical roles in any Smart Data sharing ecosystem.

In an ecosystem, the challenge comes when trying to map those roles across the different actors that exist in that sector. Some sectors have many more participants than others, and every actor may play one or more roles.[17]

For example:

- Participants vital to the function of the ecosystem or use-case may not fit neatly into regulatory definitions of roles (e.g. Technical Service Providers in Open Banking, or Price Comparison Websites in the telecoms sector), or
- Participants may adopt multiple roles during the course of a data sharing use-case or scenario (e.g. where TPPs access data from a Provider, but in turn become a Provider when they share it to a Fourth Party).

Of particular importance in the data chain is the recognition of which participant is the 'consumer-facing party'. The consumer-facing party should show the data subject/consumer how their data has been aggregated and categorised[18], provide tools to enable the consumer to manage and revoke their consent or the access granted to their data, and facilitate an easy point of complaint and access to redress. In practice, the most recognisable brand to the consumer may not be the TPP but the Fourth Party.

For Smart Data to facilitate a wide range of use cases, it is important that the accreditation regime clearly:

- Identifies all the potential parties in a data chain, including Technical Service Providers and Fourth Parties

[16] BEIS Smart Data Research: Authentication and Trust: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909365/Raidiam_Authentication_Research_Response.pdf
[17] "As You Like It", Act II, Scene VII; Shakespeare
[18] https://www.fca.org.uk/firms/agency-models-under-psd2

- Outlines the responsibilities of the different parties and what they must be accredited for. Key responsibilities which warrant consideration include:
    - Recording data, and the accuracy of the record
    - Storing data on behalf of a data subject in a secure and readily accessible format
    - Providing data, within a certain timeframe and using a certain means of electronic and encrypted transfer
    - Accessing the data from a data provider with a data subject's consent
    - Storing consents/access to data granted and revocations of consent/access to data by the consumer
    - Categorising, manipulating or analysing data
    - Providing categorised, manipulated or analysed data as a service to another participant that is not the data subject
    - Providing a consumer facing service using the data
    - Providing a consumer facing interface that shows how a consumer's data has been aggregated and categorised
    - Providing tools to the consumer to enable them to control access to their data
    - Providing a route to complain and access to redress
- Decides whether the consumer-facing party in the data chain (which may not be the TPP) should be accredited
- Decides whether an additional participant role (and rights of access) are required for entities that aggregate Smart Datasets on a anonymised/pseudonymised basis for public research purposes
- Sets out the conduct requirements for participants. For instance, the FCA extended its Principles for Business and parts of the Banking Conduct of Business Sourcebook to TPPs to ensure a level playing field for all firms offering TPP services[19]

As we note above, roles have emerged in Open Banking that do not neatly fit the definitions laid out in PSD2. It has not satisfactorily delineated the role of TPP from a Fourth Party or from a Technical Services Provider (TSP)[20]. TPPs often operate as TSPs on behalf of other TPPs or Agents. Fourth Parties may not be regulated but are often the consumer-facing brand rather than the TPP, which is not the intention of the regulation. This causes considerable confusion for both participants and consumers.

The Icebreaker One initiative, Open Energy[21], has tried to simplify the roles and is exploring placing Data Provider responsibilities onto TPPs where they are passing on data to another

[19] https://www.fca.org.uk/publications/policy-statements/ps19-3-general-standards-communication-rules-payment-services-e-money-sectors

[20] https://www.fca.org.uk/firms/agency-models-under-psd2; also see Appendix Roles (PSD2)

[21] https://energydata.org.uk/

party (see Appendix Roles (Energy)). This shortens the data chain and may help address the liability issues laid out in BEIS report on Liability and Redress.[22]

It may not be practical to accredit all Fourth Parties. However, in cases where Fourth Parties undertake further analysis and manipulation of data provided to them by a TPP, it may be appropriate to identify these parties as TPPs using the services of a TSP to access data. In this case, these Fourth Parties would need to be accredited as if they were a TPP. This should help to avoid regulatory arbitrage where Fourth Parties access data and behave like TPPs but are not accredited.

Where a TPP is providing a holistic service to a Fourth Party and that Fourth Party does not undertake any further analysis or manipulation of the data, it may be helpful to assume they are a genuine Fourth Party and as such do not require accreditation. However, it may be helpful to consider certain requirements for Fourth Parties. These could include:

- Disclosure of access and using Smart Data in the provision of a service to the ICO as part of their ICO registration. This ensures there is some visibility of the company's access to Smart Data which can be monitored and reported to BEIS.
- The responsibility of the Fourth Party as the consumer-facing party to show the data subject/consumer how their data has been aggregated and categorised; provide tools to enable the consumer to view and manage their consents; and facilitate an easy point of complaint and access to redress. (Where the TPP is the consumer-facing party and there is no Fourth Party, the TPP should be required to provide these services).

In conjunction with this approach, requiring TPPs to use technology to improve traceability in the data chain would provide additional operational benefits and address risks outlined in the BEIS report on liability and redress.[23]

Another observation is that in some sectors it may be helpful for aggregated Smart Data to be made available on an anonymised or pseudonymised basis. In financial services this has been achieved through the Global Open Finance Centre of Excellence with data providers sharing data on a voluntary basis. However, in energy there is no central repository of smart meter data in the UK, there is no requirement on supplier to share smart meter data, even at an aggregated level. This may hold back efforts to net zero[24].

22 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909364/Dgen_and_BEIS_-_Smart_Data_-_Liability.pdf

23 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909364/Dgen_and_BEIS_-_Smart_Data_-_Liability.pdf

24 https://energydata.org.uk/data-protection-and-smart-meter-data/

Rights of access

The framework legislation confers the right of access to data for TPPs. This can take a number of forms, whether positioned as a right for consumers to port or transfer the data which they are confirmed to own, as in Canada's 'Consumer Directed Finance', Australia's 'Consumer Data Right', or from the other perspective as in PSD2 where the right of TPPs to access is enshrined as a requirement to share for the data provider, if directed by the Consumer.

An accreditation regime then confirms (or in the case of a voluntary agreement, confers) the right of access to data for TPPs. This means that the accreditation regime must be robust enough to support the sector-specific use cases envisaged by Smart Data. Alternatively, the right of access must be mediated by regulators who define the data which can be accessed.

Under the Smart Data Framework, BEIS has the option to legislate to give powers to regulators to mandate data sharing. To fully support wider Smart Data, BEIS may need to give general access rights to TPPs to access data which the respective regulators dictate should be made available, or which the respective memberships have agreed voluntarily.

Framework and Ownership

As we note above, accreditation affords benefits to the government and regulators and gives them an overview of how the market is shaping up. However, this assumes that the government or regulators own the accreditation regime or have powers to require the owner of an accreditation regime to report to them. An important part of the framework for accreditation is therefore deciding WHO will be responsible for the functional and supervisory items listed previously:

- Classification of data
- The roles of participants that can provide, access and use data
- Rights of access to data
- Accreditation requirements participants need to meet to access the data
- Validation of the requirements having been met
- Monitoring of accredited participants
- Enforcement against participants that do not meet the standards of accreditation
- Reporting on the accreditation framework, market development and effectiveness

The needs of an accrediting body are likely to vary according to the role of regulators (WHO), the legal requirements associated with data sharing (WHAT), and technological conformance (HOW) to standards:

In the Appendix (Responsibilities), we suggest ways in which the different responsibilities between government, regulators and an independent accrediting body might be separated.

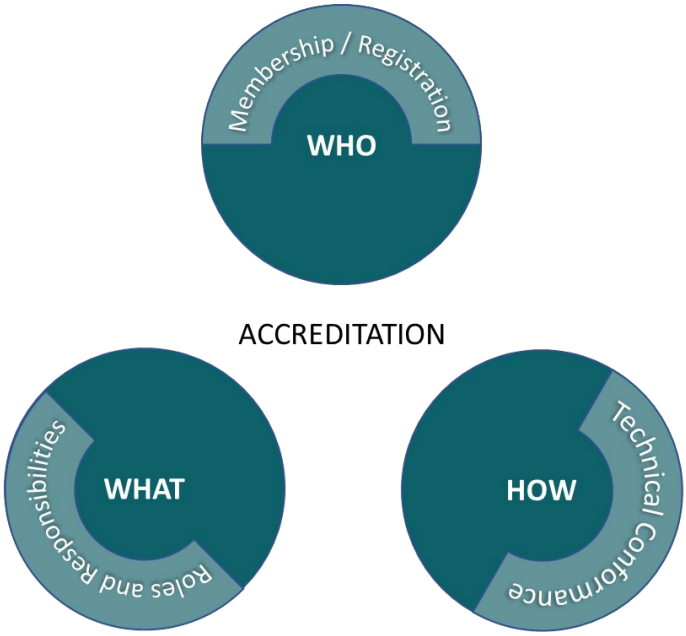


Figure 8: Framework for Accreditation showing WHO, WHAT and HOW.

Design criteria

Based on the previous sections on the aims and objectives of accreditation, we propose a series of design criteria against which to measure any accreditation approach for cross-sector data sharing in the UK:

Beneficiary	Design criteria
Government and regulators	- Promotes cohesion and interoperability within and across sectors - Easy to oversee (with clear responsibilities between government and regulators) - Can be effectively enforced against in a timely manner, including revocation if required. - Is financially sustainable - Simple and avoids fragmentation or entities 'falling through the gaps' - Scalable to other sectors over time - Applicable to a wide range of data sets (both in and out of scope of GDPR or other regulatory boundaries) - Agile to accommodate changing accreditation requirements in keeping with legal and regulatory developments - Enables the swift identifiability of providers in the ecosystem to deliver the benefits of accreditation envisaged above
End-users (Consumers)	- Accreditation and expectations for participants accessing data are consistent across sectors - Ease of access to accreditation is proportionate to the sensitivity of data being shared - Accreditation supports a consistent liability framework that provides reassurance - Accreditation is communicable to build trust
Participants (TPPs, Providers and other roles defined as requiring accreditation)	- Accreditation creates a level playing field - The processes for accreditation and/or regulatory authorisation do not create an unnecessary barrier to accessing data - Government and regulatory expectations and enforcement of accreditation is consistent across sectors - Applicable to a wide variety of use cases - Applicable to a variety of end users (e.g. individuals, small businesses, and other public and private sector bodies) - Enables the swift identifiability of providers in the ecosystem to deliver the benefits of accreditation envisaged above

PART 2: Sector-Specific Examples

In Part 2, we review and highlight the specific conditions for accreditation that exist in current open data sharing initiatives. We note areas for the standardisation of the conditions for accreditation as well as how participants can communicate it.

Open Banking (UK)

As the global reference for successful open data ecosystem implementation, we look first at the accreditation process for the UK's Open Banking Implementation Entity (OBIE).[25]

Preconditions for Open Banking

The OBIE accreditation process first requires roles of *"Payment Initiation Service Provider"* and *"Account Information Service Provider"* defined by European legislation (PSD2)[26], plus the regulatory authorisation provided by one of the National Competent Authorities across the PSD2 region[27] (i.e. any of the EU27 national regulatory authorities for financial services). This in itself demonstrates how multiple bodies can all provide the same level of authorisation if the over-arching regulatory framework is set. Full details of the PSD2 requirements (as listed by the FCA) are included in the Appendix

Key Steps:

Request Regulatory permissions:

a. Apply to the FCA or European equivalent

b. Confirm PSD2 Role and scope of service

c. Gain FCA Approval[28] by confirming type of service. If the only 'payment service' a company is offering is defined as an Account Information Service it will have fewer requirements. If the entity is providing other payment services such as Payment Initiation, then it must become an Authorised Payments Institution:

   i. Business model of proposed service

   ii. Policies and Procedures (for robustness and completeness)

[25] https://www.openbanking.org.uk/providers/third-party-providers/
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223
[27] https://www.eba.europa.eu/supervisory-convergence/supervisory-disclosure/competent-authorities
[28] See Chapter 3: https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

iii. Compliance with all “relevant regulations” e.g. Anti-bribery etc.

iv. Insurance levels: i.e. hold professional indemnity and initial capital

v. Data Security and Privacy measures are in place.

Enrol with OBIE:

d. The OBIE onboarding team will check and confirm:

i. identity and verification (ID&V) for the Individual

ii. identity and verification (ID&V) for the Company

iii. PSD2 role of Company via NCA register check.

iv. Linkage between Company and Individual via Company Director authorisation.

Test the service:

e. Build and test the service in a sandbox environment using dummy data

f. Use the Open Banking Directory Sandbox to confirm how to share the identity, authorisation and service details securely with other participants.

Finalise and Go-live:

g. Confirmation of regulatory permissions (see Step 1)

h. Confirmation of full identification and validation checks (see Step 2)

i. Launch full service

j. Use the Open Banking Production Directory to share the identity, authorisation and service details securely with other participants.

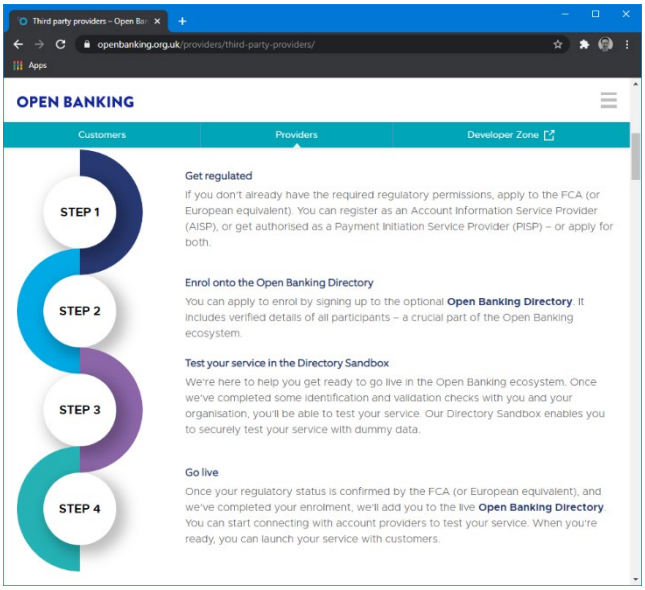


Figure 9: Screenshot of the Open Banking accreditation process:

Open Energy (UK)

Energy will be the next sector in the UK to deliver a live data sharing ecosystem through Icebreaker One's Phase 3 work[29] on the MEDA Programme[30]. Energy is also the next sector in line under the Australian Consumer Data Right.[31]

Preconditions for Open Energy: Licensing

Roles in the Energy sector are far more varied than those in the Banking sector, leading to huge potential complexity of data sharing options. In addition, there exist both *'Licences'* and *'Codes'* for participants in the Energy sector.

Ofgem administers a number of different licensing schemes:[32]

The Gas Act (1986):

- Transport Licence

- Interconnector Licence

- Shipper Licence

- Supplier Licence

The Electricity Act (1989):

- Transmission Licence

- Distribution Licence

- Interconnector Licence

- Generation Licence

- Supply Licence

Ofgem:

- Smart Meter Communication Licence

[29] https://energydata.org.uk/
[30] https://www.gov.uk/government/groups/modernising-energy-data
[31] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr/cdr-in-the-energy-sector
[32] https://www.ofgem.gov.uk/licences-industry-codes-and-standards/licences/licensable-activities

The Ofgem Licence application process is intended to confirm:

- The applicant has the appropriate resources for their proposal to enter the market
- The applicant understands their regulatory obligations and has appropriate plans in place to meet these
- The applicant is fit and proper to hold a supply licence

Part of the Licence agreements include the requirement to adhere to an Industry Code which defines the terms under which participants can access the appropriate networks. The Codes are all overseen by Ofgem, but administered by Code Administrators.[33] Reform of these Codes is also under consideration, via consultations to be conducted in 2021.[34]

There are a number of accreditation schemes run by Ofgem under the *"Renewables and CHP register"*[35]

Key Steps:[36], [37]

1. Apply for the appropriate Licence:
    a. Tier 1 questions - Core information required
        i. Company - ID&V, Solvency, Companies House
        ii. Individuals - ID&V, Suitability, Solvency
        iii. Link Individual and Organisation
        iv. Business Plans - Previous licence history,
        v. "Licence-specific" information
    b. Tier 2 questions - Additional verification for applications deemed high-risk
        i. Certified copies of official documents
        ii. Substantive contact with Industry Code Administrators
        iii. Evidence of Services: bank, solicitors, auditors
        iv. Personal interview

Apply to the appropriate Industry Code[38]

    c. Company details

[33] https://www.ofgem.gov.uk/licences-industry-codes-and-standards/industry-codes
[34] https://www.gov.uk/government/consultations/reforming-the-energy-industry-codes
[35] https://www.ofgem.gov.uk/environmental-programmes/information-renewables-and-chp-register
[36] https://www.ofgem.gov.uk/system/files/docs/2019/07/applying_for_a_gas_or_electricity_licence_-_2019_guidance_document_1.0_0.pdf
[37] https://www.ofgem.gov.uk/system/files/docs/2017/01/register_user_guide_-_how_to_create_an_account.pdf
[38] e.g. https://www.elexon.co.uk/reference/market-entry

d. Individual details

e. Sign the appropriate Code

f. Confirm (technical) adherence to Code

g. Confirm funding

The codes define the terms under which industry participants can access the electricity and gas networks. The table below lists the codes and contact details for them.

Code	Type	Code Administrator	Website
Balancing and Settlement Code (BSC)	Electricity	Elexon	www.elexon.co.uk
Connection Use of System Code (CUSC)	Electricity	National Grid	https://www.nationalgrideso.com/industry-information/codes
Distribution Use of System Agreement (DCUSA)	Electricity	Electralink	www.dcusa.co.uk
Master Registration Agreement	Electricity	Gemserv	www.mrasco.com
Grid Code	Electricity	National Grid	https://www.nationalgrideso.com/industry-information/codes
Distribution Code	Electricity	Energy Networks Association	www.dcode.org.uk
System Operator - Transmission Operator Code (STC)	Electricity	National Grid	https://www.nationalgrideso.com/industry-information/codes
Uniform Network Code (UNC)	Gas	Joint Office of Gas Transporters	www.gasgovernance.co.uk
Independent Gas Transporter UNC (iGT UNC)	Gas	Gemserv	www.igt-unc.co.uk
Supply Point Administration Agreement (SPAA)	Gas	Electralink	www.spaa.co.uk
Smart Energy Code (SEC)	Gas and Electricity	SECAS	www.smartenergycodecompany.co.uk
Retail Energy Code (REC)	Gas and Electricity	REC	https://www.retailenergycode.co.uk/

Figure 10: Table of Energy Sector Codes and Administrators[39].

[39] https://www.ofgem.gov.uk/licences-industry-codes-and-standards/industry-codes

Open Communications (UK)

Ofcom carried out a consultation exercise in the Autumn of 2020, to examine the case for Open Communications[40]. The consultation questions aimed to draw parallels from the implementation of open banking and to consider how that could be applied to Open Communications.

Ofcom already operates a voluntary Digital Comparison Tool (DCT) accreditation scheme, which requires members to confirm they meet certain standards. Ofcom notes that

> *"We do this to help build trust in the service [DCTs] offer to customers"*

This sector is already starting to move towards a more open data approach. From June 2022, providers will be required to conform with an updated set of General Conditions which will mandate digital access to generic product information, to third party Digital Comparison Tool (DCT)s who meet similar criteria to the voluntary scheme.[41]

Application for accreditation requires submitting a short description of the services, its ownership, business model and comparison calculator.

To be eligible for membership of the scheme, comparison tools must:

- provide users with information on the quality of services they compare;
- make clear who owns them and be independent from the providers whose services are being compared, to ensure unbiased search results;
- set out clear and objective criteria on which comparisons are based;
- deliver services to a high standard and comply with relevant legislation;
- provide information that is accurate, accessible and up to date, and present that information in plain and clear language;
- show offers covering a significant proportion of the market and be open to any provider that wishes to make their products available for comparison; and
- have effective procedures in place to handle consumer complaints and to allow users to report incorrect information.

Further detail on each of the accreditation steps is provided online.[42] Where a comparison tool is certified it can display the scheme logo on its website and other public materials. To ensure robustness, accredited bodies are monitored regularly. In addition, they must pass a technical audit, are subject to spot checks and may be required to provide evidence or declare compliance.

[40] https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications
[41] Para 6.71: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/204980/statement-eecc-revised-proposals.pdf
[42] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/204982/statement-digital-comparison-tools.pdf

Open Banking (Brazil)

Although built on the same principles and technology approach as the UK's open banking ecosystem, the accreditation flow for open banking in Brazil differs due to the presence of national IDs (*"CPF"* for Natural Persons, *"CNPJ"* for Legal Entities), and the ability to use them electronically.

Preconditions for Open Banking, Brazil

Open Banking in Brazil has adopted a very similar implementation approach to the UK. This includes the foundation of the Brazilian equivalent to GDPR for data privacy, the LGPD[43]. The roles and responsibilities set out in Europe under PSD2 are however captured directly by the Central Bank in the Open Banking legislation.[44]

This simplifies the validation processes significantly compared with the UK model, and hence open banking in Brazil can be operated more autonomously without additional manual accreditation by a regulator:

Key Steps:

1. Open Banking Brasil Directory firstly takes central bank input:
    a. For all regulated companies - identified by CNPJ
    b. For regulated roles - via API validation feed from the Central Bank
    c. For associated individuals - identified by CPF.

Individuals carry out registration[45]:

    d. Individual User validation - SMS / Email and 2FA set-up
    e. Digital Signing of the Terms and Conditions and Privacy Policies (which set out what you can/cannot do - i.e. self-attestation)
    f. Confirmation of individual role within company
    g. Responsible individual then signs participant Terms of Adhesion for the Company.

[43] https://gdpr.eu/gdpr-vs-lgpd/
[44] https://www.bcb.gov.br/content/config/Documents/BCB_Open_Banking_Communique-April-2019.pdf
[45] https://openbanking-brasil.github.io/areadesenvolvedor/documents/Open_Banking_passo_a_passo_cadastro_v05.pdf - TPP version is in production.

Open Banking and Energy (Australia)

As a final live example, we can highlight the 'Contract club' approach, process and questions required for the Australian Consumer Data Right (CDR), which has banking and energy in its initial scope:[46]

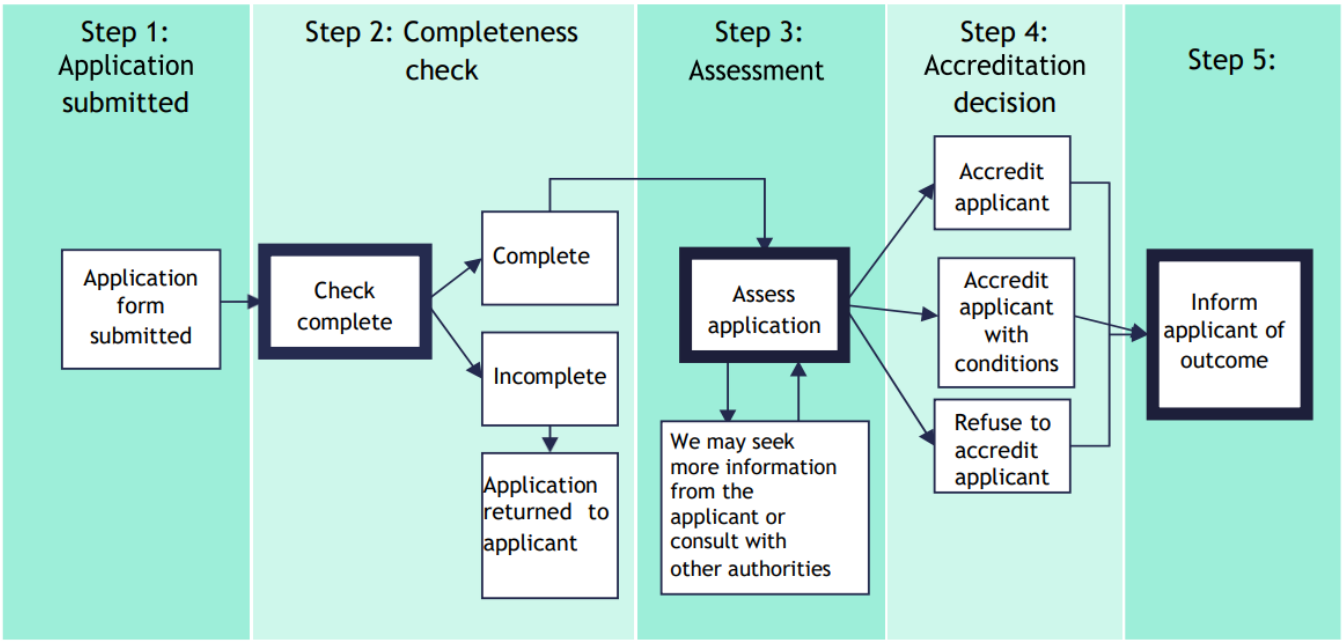


Figure 11: ACCC CDR Accreditation Process

Application to CDR Data Environment	
Part 1 (governance)	**Part 2 (control requirements)**
Step 1: Define and implement security governance in relation to CDR data	Limit the risk of inappropriate or unauthorised access to CDR data environment.
Step 2: Define the boundaries of the CDR data environment	Secure network and systems within CDR data environment.
Step 3: Have and maintain an information security capability	Securely manage information assets over their lifecycle.
Step 4: Implement a formal controls assessment program	Implement formal vulnerability program to identify, track and remediate vulnerabilities within the CDR data environment.
Step 5: Manage and support security incidents	Limit, prevent, detect, and remove malware. Implement formal security training and awareness program for all personnel interacting with CDR data.

Figure 12: ACCC Data Governance and Control requirements

[46] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-accreditation-guidelines

Open Savings, Investments and Pensions (UK)

In the UK, an alternative model already active within the financial services sector is that of the membership or 'contract club', as exemplified by The Investing and Savings Alliance (TISA).

The process and agreements behind the membership of TISA have opened the way for successful data sharing frameworks such as the TISA Exchange (TeX)[47], built on consistent legal agreements.[48]

This legal framework is intended to be the baseline for a long-term vision for Open Savings, Investments and Pensions (OSIP)[49], which proposes to deliver similar standards approaches to governance, APIs and development as have been seen with open banking and open energy.

The Pensions Dashboard Programme is also preparing for a voluntary onboarding phase during the course of 2021[50].

47 http://www.tisaexchange.co.uk/
48 https://tisaexchange.co.uk/library/tex-legal-documents/
49 https://www.tisa.uk.com/tisa-groups-projects/osip/
50 https://www.pensionsdashboardsprogramme.org.uk/2021/03/12/building-an-onboarding-strategy/

Standardising conditions for accreditation

Accreditation conditions are determined according to risk. Regulators offer different routes to authorisation dependent upon identified risk. Typically they reserve the right to ask individual firms for more information, meaning that while there are standardised aspects for all applicants, each individual applicant's experience may vary. Regulators are rightly protective of the boundaries of sectors and how they take responsibility for risk within them. As such, while accreditation requirements may be similar, they may not be simply transferrable.

Application processes suggest that there are some key information requirements which all applicants are asked to provide. These include:

- Proof of company
- Disclosure of past activities (authorisations and revocations)
- Directors of the company, controlling persons, their fitness and propriety
- Address of head office and locations of services provided
- Operations: the products and services in scope, contracts with additional parties etc
- Business plan or proof of business readiness
- Structure of the organisation
- Governance requirements, internal controls, risk management, adherence to GDPR
- Security management: from IT readiness to managing security-related customer complaints

In addition to these, the FCA requires the following information for Registered Account Information Service Providers (with rights to 'read' data only) which seem pertinent for Smart Data[51]. These include:

- How sensitive data is dealt with
  (in the case of financial services, 'sensitive payments data')
- Business continuity arrangements
  (data sharing typically creates chains of parties relying on the provision of data)
- Audit arrangements
- Professional indemnity insurance

As we note above, where risk is higher additional information is requested. For PSD2, participants must provide more documentation where they become an Authorised Payment Institution and can initiate payments from a consumer's account. This type of access is called 'write' access.

The accreditation requirements for 'write' access are very specific to the activity being undertaken, e.g. requirements to have financial crime controls in place. One of the design

[51] A more detailed list of PSD2 requirements is outlined in the Appendix

principles we highlight in Part 1 is that cross-sector accreditation must be applicable to a wide range of datasets (both in and out of scope of GDPR or other regulatory boundaries).

Given the range of potential activities which could constitute 'write' access and how these may vary between sectors, it may not be possible to harmonise requirements for 'write' access across sectors.

It may be easier to create a harmonised set of requirements all applicants must provide for 'read-only' access. Depending on the type of sensitivity of data accessed (see 'Classification of Data' above), more or less information may be required. The Federated Services Qualification System is an example of how requirements can be tiered.

Federated Services Qualification System

The FSQS (Financial Services Qualification System)[52] is a community of financial institutions including banks, building societies, insurance companies and investment services, collaborating to agree a single standard for managing the increasing complexity of third and fourth-party information needed to demonstrate compliance to regulators, policies and governance controls.

This is a good example of standardising where possible to reduce friction in a highly sensitive sector. It removes significant repetition, whilst also ensuring a minimum level of robust data collection. However, it allows the individual banks to retain complete individual control over who they allow to access their systems.

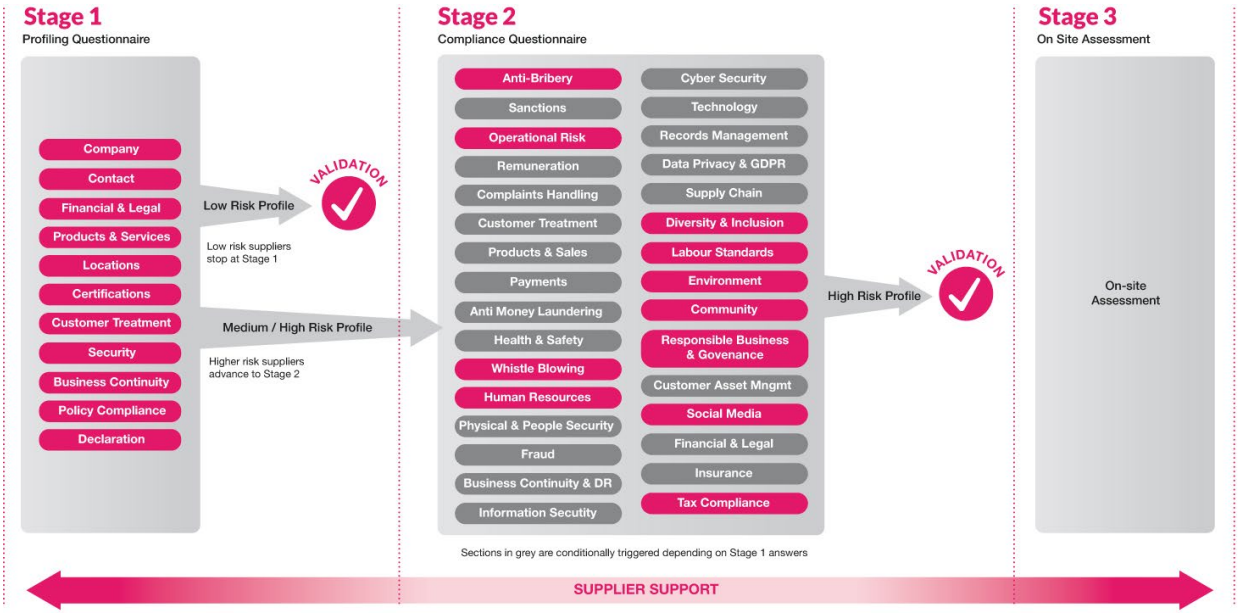


Figure 13: Screenshot from https://hellios.com/fsqs/ showing the three stages of accreditation required for the FSQS: Profiling, Compliance and Assessment.

[52] https://hellios.com/fsqs/

Standardising cross-sector data sharing

As noted above, regulators are rightly protective of their perimeters and how they authorise, supervise and enforce against participants within their ecosystem. Cross-sector accreditation by an external party reduces the control regulators have over the risks they are duty-bound to mitigate.

Accreditation of cross-sector data sharing must balance the needs of participants and regulators. The process for accreditation and/or regulatory authorisation should not create an unnecessary barrier to accessing data for participants. But regulators need sufficient control to easily identify and oversee participants in their ecosystems[53].

A potential approach for cross-sector accreditation is to establish the same applicant requirements for all Smart Data sharing for 'read' access only. BEIS can draw on the consistent set of information participants in any sector are usually asked in relation to their ownership, fitness and propriety, operations (including financials, legal, security and adherence to GDPR) and governance. Applicants can apply to a single sector regulator for access to that sector's data, providing any additional information as necessary. On successful application they receive a 'passport'.

TPPs can then build on this standardised accreditation base, and 'fast-track' or 'passport' between sectors where they have already been fully accredited. Any sector regulator would 'visa stamp' to verify that accreditation conditions have been met for that sector or require additional materials to support the 'visa application'. The 'passport' does not reduce friction entirely but speeds up the process for participants and reduces barriers to access other datasets.

A positive supporting activity would be to require regulators to increasingly improve communication and harmonisation between themselves on the quality of evidence they accept for accreditation, thus increasing the likelihood of transferability of such evidence in the 'passport'. If there is appetite, an independent entity could be responsible for doing the initial accreditation for the passport.

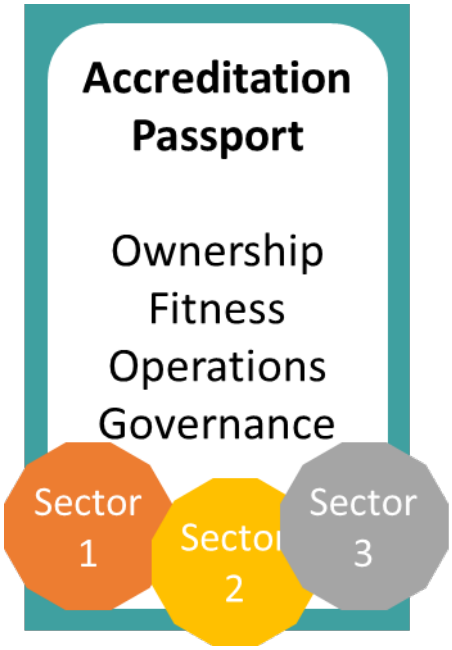


Figure 14: Figure: Accreditation 'passport' graphic with sector-specific 'visa' stamps

[53] See the Design Criteria outlined in Part 1

Communicating the accreditation

The success of Open Banking is founded on the Directory (participant whitelist) which underpins the trust framework. Open Banking Limited relies on the FCA register to check whether entities are accredited and trustworthy. The Directory captures and reflects the outcome of the checks undertaken by Open Banking Limited, allows all participants to trust that the checks have taken place and to prove who they are to each other. The FCA register is checked regularly for updates and revocations.

As suggested above, participants that wish to move between sectors could get a passport and a ‘visa stamp’ from sector-specific regulators. However, once they have a passport with the relevant ‘visa’, they must be able to communicate that they are trustworthy to other participants in a way which is also secure. Participants must be able to trust and validate that the passport and visa(s) are real.

One option to facilitate communication is through a Smart Data Trust Platform, more commonly known as a Directory. Such a Directory would mean cross-sector TPPs were clearly identifiable to other participants. When a participant gets their passport updated with a new sector, this ‘visa’ could be reflected on the Directory. This already happens within the Open Banking ecosystem where different types of accreditation are displayed on the Directory: e.g. Account Information Service (read-only), PIS (write) and Confirmation of Payee.

Taking a single Directory approach would increase interoperability and reduce friction once accreditation is in place, while also maintaining security. To reduce fragmentation and complexity for participants, a Directory should be a single, centralised system (otherwise each participant will need to check each Directory for each TPP). Due to the foundational requirement, this Directory should be offered as a utility service by a central provider (e.g. an existing entity providing a cross-sector service. Following one of the options set out in the BEIS Smart Data Consultation, we would support the idea of creating a Smart Data Function to carry out this activity).

Monitoring, enforcement and reporting

An accreditation regime is only as strong as its enforcement. Where requirements for conduct and reporting are not monitored or enforced, trust in the accreditation process weakens. As noted in Part 1, regulatory supervision is often challenging given the limited resources of regulators and the expanding markets they supervise. Standardisation, automation and centralisation of any repeatable aspects of supervision will free up regulators to focus on problem areas or new developments.

It is possible to standardise and automate aspects of Smart Data:

- **Conformance:** Ongoing accreditation requires conformance to demonstrate how well a service is meeting requirements set out. Technical conformance can be demonstrated objectively through the use of standardised testing tools. Certificates can then be issued and published to increase the positions of trust across the ecosystem.
- **Performance:** There has been a lot of debate within the financial services sector about the correct way to self-report API performance. Having an independent body to monitor and report API availability could harmonise reporting across sectors and reduces the risk of inconsistent self-reporting within and across sectors.
- **Enforcement:** Additionally, an automated schedule of fines and penalties where performance (e.g. unplanned downtime of data provider's APIs) does not meet the standard required may help to reduce the supervisory burden associated with implementation challenges.

It is likely that there will be conduct requirements that can be standardised across sectors, such as the fair treatment of consumers, rules to protect vulnerable consumers and provisions for access to redress. Similarities are demonstrated within both the FCA's principles of business requirements and Ofgem's voluntary DCT scheme. There will also be sector specific rules which TPPs may need to adhere to in addition to those set out for Smart Data.

It is important that regulators are suitably equipped to deal with the conduct challenges that they may be required to monitor and enforce against as part of their role. GDPR is a key cross-cutting regulation and it may be appropriate to give sector regulators concurrent powers for data protection as identified in BEIS report on Liability and Redress.[54]

Supervision, enforcement and reporting functions are required to ensure that the accreditation regime is robust and delivers the trust needed to facilitate cross-sector data sharing.

54 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/909364/Dgen_and_BEIS_-_Smart_Data_-_Liability.pdf

PART 3: Conclusion

Summary

As part of the brief for this research, we identified that before answering what conditions TPPs may need to meet in order to be accredited, it is important to first understand what a TPP is being accredited for.

Once government has made decisions about what TPPs are being accredited for, our analysis shows that it is possible to surmise that conditions for accreditation can be standardised across sectors. However, it is likely that standardisation of accreditation can only feasibly be introduced for ‘read’ access at this point. ‘Write’ access for TPPs is higher risk and is more likely to be sector specific and less open to standardisation.

To support the standardisation of conditions for accreditation, BEIS can draw on the consistent set of information participants in any sector are usually asked in relation to their ownership, fitness and propriety, operations (including financials, legal, security and adherence to GDPR) and governance.

Once TPPs have met accreditation requirements in one sector, they could be granted a ‘passport’. This passport would ‘fast-track’ a TPP’s application to access data from another sector and if successful provide them with a ‘visa stamp’ for the additional sector. This reduces friction for a TPP. However, it would still ensure sector regulators have oversight and can mitigate risks of TPPs from other sectors entering their ecosystem.

Communicating accreditation securely between participants can be achieved through a Smart Data Directory, similar to an Open Banking Directory. As participants become accredited for new sectors, this can be reflected on the Directory. A single Directory is preferable to multiple directories, to reduce friction for TPPs, maintain interoperability and support market efficiencies.

There are also opportunities to standardise and automate aspects of monitoring, enforcement and reporting to reduce the regulatory burden of supervision.

Recommendations

It is important that an accreditation regime identifies the WHO, the WHAT and the HOW of our Accreditation framework. To put it another way, we recommend government identifies:

- *Who can come through the door?* i.e. what requirements are there on a participant to prove itself fit and proper and to whom should it prove itself fit and proper?
- *What data can a participant access or share? And what security is needed to do so?* i.e. what needs to be in place to secure the data, and to secure the transmission of data?
- *How should organisations behave with regards the data?* i.e. what can they do/not do with the data they access, what services must they provide to the data subject and what responsibilities do they have if/when something goes wrong?

To establish a Smart Data regime we recommend government and regulators decide on both the functional requirements of the accreditation framework and how it will be supervised and enforced.

Functional requirements	Supervisory and policy requirements
• **Classification of data** and what data should be made available to share • Definitions of **Roles of participants** that provide, access and use data • **Rights of access** to data by TPPs (and/or conversely requirement for Providers to share data) • **Requirements for accreditation** that all participants need to meet (by role) • **Validation process** for accreditation requirements having been met	• **Monitoring** (and extent of monitoring) of accredited participants • **Enforcement** against participants that do not meet the standards of accreditation • **Reporting** on the accreditation framework, effectiveness and market development

Classification of data and rights of access

To fully support Smart Data widely, BEIS should consider giving general access rights to TPPs as part of the framework legislation. These could enshrine a basic right of access (and/or specify a general requirement to share) whilst still allowing sector-specific discretion as to which data can be accessed on both a ‘read’ and ‘write’ basis. That discretion can be dictated by the respective regulators or agreed voluntarily by the respective memberships.

We recommend that general rights of access (and/or requirements to share) are considered at the framework legislation level.

Roles of participants

With regards the responsibilities of participants, we recommend BEIS include in the legislation:

- The definitions of parties in a data chain
- The responsibilities of the different parties and what they must be accredited for
- The responsibilities for the consumer-facing party. These should include showing the data subject/consumer how their data has been aggregated and categorised; providing tools to enable the consumer to control their data; and facilitating an easy point of complaint and access to redress.
- Set out the conduct requirements for participants (e.g. fair treatment of consumers, especially people in vulnerable circumstances)

Standardising conditions for accreditation

As we note above, BEIS can standardise the conditions for accreditation by drawing on the consistent set of information participants in any sector are usually asked for in relation to their ownership, fitness and propriety, operations (including financials, legal, security and adherence to GDPR) and governance.

We recommend that conditions for standardisation focus on 'read' access only and that 'write' access is determined by sector regulators. Participants should be required to provide more detail to individual sector regulators to access the higher risk 'write' permissions.

Communication of accreditation

We recommend BEIS puts in place a single Smart Data Directory. This will allow TPPs to easily and securely communicate their accreditation and 'visa stamps' to other parties. A single directory will reduce friction, increase interoperability and drive market efficiencies.

Further work is required to consider the benefits of how the trustworthiness of accredited parties is communicated to consumers. For this, initiatives like the Australian implementation of the Consumer Data Right[55] will be useful in demonstrating the value of a Trustmark.

Supervisory and Policy Conclusions

BEIS must determine who is going to be responsible for running the accreditation regime, and who will monitor it, and who will enforce against it.

We recommend BEIS maps out the supervisory, enforcement and reporting requirements and allocates responsibilities across government, regulators and/or an independent accrediting entity. This will ensure that the accreditation regime is robust and delivers the trust needed to facilitate cross-sector data sharing.

[55] https://consumerdatastandardsaustralia.github.io/standards/archive/standards-0.9.3/docs/#scopes-and-claims

APPENDICES

Glossary

- **Smart Data initiatives**: sector specific initiatives aiming to facilitate the secure sharing, upon request by the customer, of customer data with third party providers, who use this data to offer innovative services for the customer.
- **Open** *X* (where *X* is Banking, Energy, Finance, Savings, Investments, Telecoms, Pensions etc): The typical form of naming for a specific Smart Data initiative in a particular sector.
- **Ecosystem**: the collective of the entities involved in defining, operating and using the sector-specific secure, consented data sharing initiative.
- **OBIE**: Open Banking Implementation Entity: the organisation set up to deliver Open Banking (the Smart Data initiative) in the UK
- **Providers**: The organisations in a data sharing ecosystem who provide the data to be shared. In open banking these are the banks.
- **TPPs**: Third Party Providers: The organisations in a data sharing ecosystem who receive the data shared by Providers and who (typically) provide propositions to Consumers.
- **Consumers**: The owners of the data, and the providers of the consent to share that data, and (typically) the users of the services provided by TPPs. Also known as a **PSU**
- **PSD2**: The European Payment Services Directive (Revised) which sets out the requirement for consumer account data to be shared, and which defines the roles of Providers (called ASPSPs in the legislation), and of TPPs (called PISPs or AISPs)
- **PISP**: Payment Initiation Service provider. A PSD2 definition of a TPP who has the right to read AND write data on behalf of a consumer - i.e. to initiate a payment instruction.
- **AISP**: Account Information Service provider: A PSD2 definition of a TPP who has the right to read data on behalf of a consumer - i.e. to read and use Account Information.
- **PSU**: (PSD2 definition): Payment Service User – the end-user of the services provided by TPPs.

Roles (PSD2)

The revised Payment Services Directive (PSD2) is the most obvious example of where the roles of participants in the data sharing ecosystem have already been identified and categorised in legislation: [56]

These Regulated roles include:

- **Data subjects**: these are the people or small businesses (Payment Service Users) that create data which they consent to share with TPPs
- **Data providers**: data providers (banks and building societies[57]) co-create and store data on behalf of the data subject.
- **TPP (Third Party Provider)**: TPPs access the data directly from the bank and provide a service to the end customer - the data subject.

However, in practise, it is not quite that simple. TPPs may rely on other 'Technical Services Providers' to access the data, and may pass the data on to a 'Fourth Party' who then provides a service to the end customer or even a 'fifth party' in the chain.

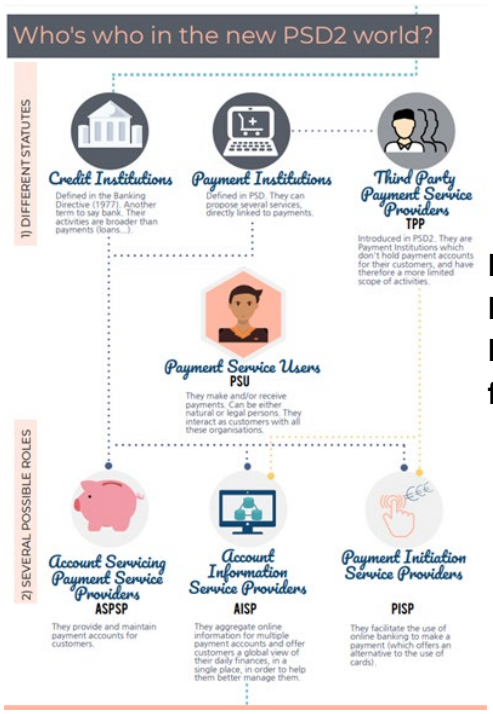


Figure 15: Screenshot of European Payment Council's PSD2 infographic (see footnote for link).

[56] https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-04/EPC_Infographic_PSD2_April%202018.pdf

[57] In PSD2 terms, the data providers are actually "Account Servicing Payment Services Providers" also known as "ASPSPs". To avoid acronyms for the reader we have simplified this to 'banks and building societies' but the term does include a wider variety of payments institutions.

Therefore, we have seen actors emerge within the Open Banking ecosystem that do not fit with the existing regulatory roles:[58]

- **TSP (Technical Services Provider)**: TSPs operate on behalf of the TPP[59] to access the data and pass it onto the TPP, but do not take any direct interest in the data items. Some TPPs operate as TSPs for other TPPs.
- **Fourth Parties:**[60] these parties receive a data service from one or more TPPs and use it to provide a service to the end customer or a fifth party. For example, a lender would use the services of a TPP as part of the credit profiling of a potential customer (the data subject) before providing the end product. You can find out more about data chains in the BEIS Smart Data report on Liability and Redress.

The peculiarities of PSD2 mean that the TPP has responsibility for providing a consumer facing service. However, in practice, where a TPP provides the data to a Fourth Party, the TPP is not the consumer facing brand.

It may therefore be appropriate to simplify the roles for accreditation in a Smart Data context rather than replicate those of PSD2.

[58] In the energy sector, price comparison websites are a similar example of non-regulated actors who are carrying out activities that drive the data sharing ecosystem use cases.
[59] Due to the peculiarities of PSD2, TSPs are not regulated parties. However, there have been calls to extend the regulatory perimeter to include TSPs, especially as some TPPs operate as TSPs for other regulated TPPs.
[60] Again the peculiarities of PSD2 mean that some fourth parties that use the services of a TPP are identified as 'agents' for which TPPs have certain responsibilities; in other cases they are identified as 'Third Parties Not Providing AIS'. See https://www.fca.org.uk/firms/agency-models-under-psd2 for further detail.

Roles (Energy)

The Energy industry in the UK highlights the challenges of adopting roles defined in one sector to another. As part of the Open Energy initiative led by Icebreaker One, an Energy Ecosystem map has been produced which shows the multiple roles, players and regulators that help keep the lights on (among other things):

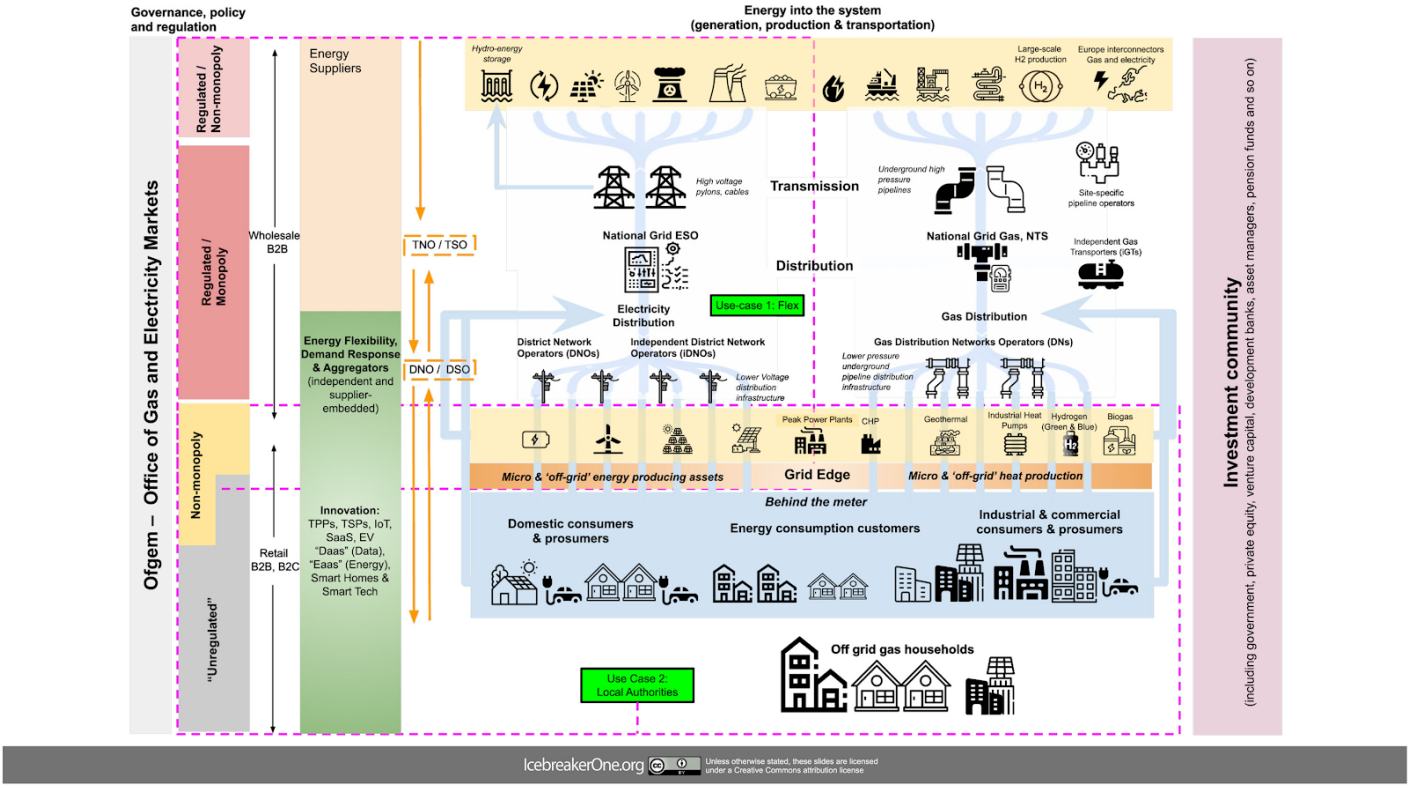


Figure 16: Icebreaker One's Energy Ecosystem Map of multiple roles, players and regulators[61]

In addition, Icebreaker One has sought to extend but simplify the roles of participants by:

- Identifying the potential for the data subject to be different to the data user. For instance, a consumer's data may be shared with their consent to help a local authority undertake planning to retrofit a local housing estate with low carbon technology. The data subject consents to their data being aggregated or used for social benefit rather than in the provision of a direct service they sign up for.
- Simplifying the concept of a TPP to relate to the action of accessing data rather than providing it to a specific Data Subject or Data User. This means there is no separate category of TSP.

[61] https://icebreakerone.org/2020/07/13/the-uk-energy-data-ecosystem/

- Facilitating onward sharing (the 'fourth party' situation within Open Banking), by noting that TPPs providing a service (not just the data) to another organisation (and not the Data Subject/User) becomes a Data Provider in the next step in a new data chain.

This reduces the length of each data chain and also gives the TPP responsibilities to the data subject to ensure the data subject can see how their data has been used and to whom it has been passed on. This might, for instance, put an obligation on the TPP as a Data Provider to offer a dashboard where the consumer can revoke their consent for onward sharing, for instance.

In some more commercial use cases, the data subject may also be the same as the data provider, e.g. one department of a local authority (the data subject) may need to share its data with another department (the data user).

Open Energy Participant Roles	Example	Open Banking / PSD2 equivalent
Data Subject The entity that acts as the source or shared source of the data. An individual or organisation.	Consumer, DNO, Supplier Others - e.g. PV installer, charge-point operator, Local Authority department	PSU
Data Provider The entity that stores the data on the behalf of the data subject.	Energy Supplier Distribution Network Operator (DNO) Smart Meter provider	ASPSP
Energy Data Service Provider (EDSP) The entity that accesses the data for a data user. It may clean, categorise and prepare the data for use and provide 'value add' services to the data user or act as a simple conduit for passing on data.	Construction Services Community Energy Groups New entrants	TPP (+ role as AIS or PIS) TSP
Data User The entity that uses the data to make decisions and act on intelligence enabled through the data.	Local Authority	PSU.

Table: Open Energy Roles described in parallel with an example and an equivalent OB role.

Registration Questions (PSD2)

The core questions required depend on whether the role is low risk (Account Information with 'read only' access), or higher risk (Payment Initiation with 'write access'). Additional questions in the higher risk case are set out in *italics*.

Account Information Service Provider (AISP)[62]

Preconditions:

- UK business for AIS (and only AIS, no Payments)
- Robust governance arrangements and internal procedures and control mechanisms
- A business plan
- Adequate indemnity cover
- Directors and Managers must:
- Be of good repute with appropriate skills to provide the services
- Not have been convicted of any financial crimes

Information required:

- Details of governance arrangements and internal procedures (for example, the structures in place to run a business effectively)
- Details of the people responsible for providing the services
- Details of any agents acting on the company's behalf (if relevant)
- Incident reporting, managing sensitive payment data, business continuity arrangements, principles and definitions used when collecting statistical data
- Details of Security policies

Payment Initiation Service Provider (PISP)[63]

Preconditions:

- *Must be a corporate body (e.g. limited company or partnership)*
- UK business for AIS (and only AIS, no Payments)
- Robust governance arrangements and internal procedures and control mechanisms
- A business plan
- *Must have adequate measures to safeguard payment service user funds*
- Adequate indemnity cover

[62] https://www.fca.org.uk/firms/apply/become-registered-account-information-service-provider
[63] https://www.fca.org.uk/firms/apply/authorised-payment-institution-api

- Directors and Managers must:
- Be of good repute with appropriate skills to provide the services
- Not have been convicted of any financial crimes
- *UK-registered and located business*
- *Must comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*
- *Must ensure anyone having a qualifying holding is 'fit and proper', and that any close links to another person will not prevent effective supervision of the business.*

Information required:

- *Details of the services proposed*
- Details of governance arrangements and internal procedures (for example, the structures in place to run a business effectively)
- *Appropriate initial capital as set out by the FCA*
- *Plans for obtaining a 'safeguarding' bank account*
- Details of the people responsible for providing the services
- Details of any agents acting on the company's behalf (if relevant)
- *Details of people with qualifying holdings representing 10% or more of the capital or voting rights*
- Incident reporting, managing sensitive payment data, business continuity arrangements, principles and definitions used when collecting statistical data
- Details of Security policies
- *Information about the control mechanisms to meet your obligations under the Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*

Layers

We set out below the layers of validation from Framework Legislation, through Regulatory oversight and mandate, via a Membership accreditation body, through to Conformance and Certification levels which could provide a suitable structure for Smart Data generally.

Validation Layers	**Open Banking: Requirement to Share**	**Open Banking: Requirement to Secure**	**Smart Data** *(Options)*
Framework Legislation	PSD2	GDPR	*Smart Data Regime (proposed)*
Regulator	FCA	ICO	*Various*
Mandated by...	CMA	Government	*Regulator*
Membership	OBIE	National Cyber Security Centre (NCSC)	*NCSC*
Conformance	OBIE / OIDF	Cyber-essentials / ISO27001	*To be decided.*

Responsibilities

In the table below, we suggest ways in which the different responsibilities between government, regulators and an accrediting body might be separated:

Functional or Supervisory requirement	Government	Regulator	Accreditation Body[64]
Rights of access to data	General right	Specific rights to types of data Designation of data types by sensitivity	Limits accreditation to what is set out by regulator
Types of participants that can access data	Sets out key data participants roles for all data sharing	Unless specific directives prohibit (as in case of PSD2) follow Government	Relies on Government categorisation of participant roles
Accreditation requirements	Sets our requirement that meets regulatory standard	Regulators set out broad requirements for passporting between sectors relying where possible based on existing regulatory standards	Accredits party against existing regulatory register and requirements. For passporting, provides visa where necessary. In case of entity that is not in regulated sector, does checks and accreditation for the market required. Creates new passport that can be used in relevant sectors (and admitted by regulators onto their register for the activity).

[64] In response to one of the options set out in the BEIS Smart Data Consultation, we would support the idea of creating a Smart Data Function to carry out some of these roles.

Validation of requirements having been met	Set out responsibilities of accrediting body and regulators	Stamp the passport before accrediting body sends to participant. Register the new participants on their Registers/Codes etc where they have accrediting body passport and (if necessary) visa.	Accrediting body validates the requirements have been met. Provides mechanism for identification and communication of that validation (e.g. Trust Platform / Directory)
Monitoring of accredited participants	Set out responsibilities of accrediting body and regulators	Responsible for monitoring the market players.	Holds the register of accredited and passported participants
Enforcing against accredited participants	Set out responsibilities of accrediting body and regulators	Enforces against accredited participants that do not meet rules of accreditation (or other conduct rules set out for the market)	Removes passport/visa of accredited party.
Reporting on accreditation framework, market development and effectiveness	Set out responsibilities of accrediting body and regulators	Confirms relevance of accrediting body actions and processes to support regulatory activities.	Accrediting body reports annually on the framework, take up, potential barriers to cross-sector data sharing, and enforcement challenges.

Conformance

Accreditation is an up-front activity. Ongoing accreditation requires conformance. Conformance can be demonstrated objectively through the use of standardised testing tools. Certificates can then be issued and published to increase the positions of trust across the ecosystem.

Open Banking UK has options for conformance in three areas[65]:

- **Security of APIs -** uses Global Standards (FAPI) - Global OIDF Conformance suite
- **Consent Management** - Uses Global open standards - Global conformance suite.
- **Functional Conformance[66]** – this is specific to Sector data standards, but the testing suite is open-sourced and can be applied to different sector standards with no loss of confidence. Results are self-generated, but are then published online.

In the case of the UK implementation, the OBIE publishes and states:

> *"These Conformance Certificates can be used by Implementers as evidence to the ecosystem (including Regulators) that they have followed the OBIE Standard correctly."* [67]

Open Banking Brazil is expected to follow a similar process to the UK when Brazil reaches Phase 2 of the implementation in June 2021. For Phase 1, a straightforward availability dashboard is published[68]:

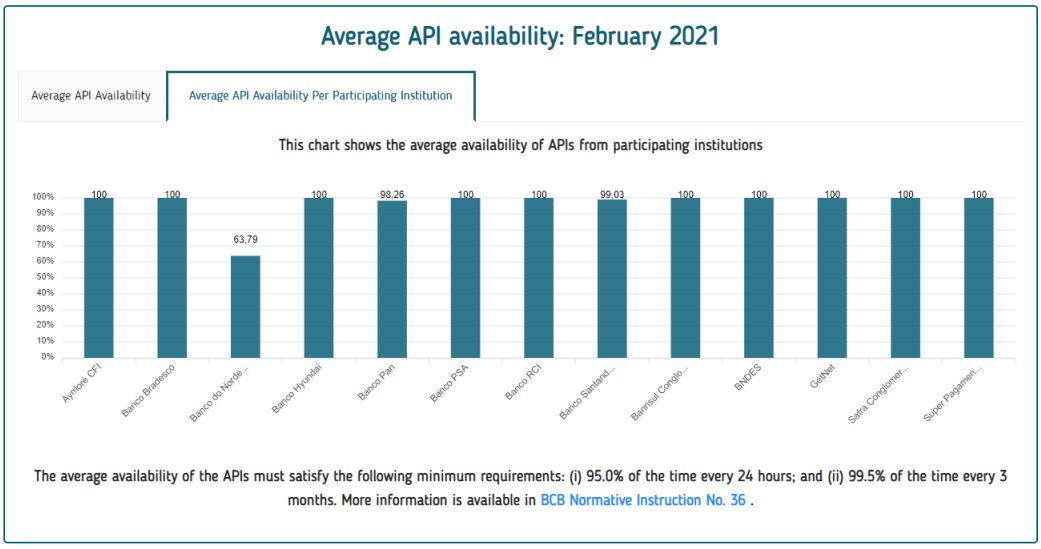


Figure 17: Screenshot: Performance metrics published by Open Banking Brazil

65 https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1061584956/Conformance+Certification+Service
66 https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1061716467/Functional+Conformance
67 https://openbanking.atlassian.net/wiki/spaces/DZ/pages/126321042/Open+Banking+Security+Profile+Conformance
68 https://dashboard.openbankingbrasil.org.br/

ASPSP/Brand	Security Profile Version	Suite Version	Client Authentication Type	Response Type	Date	Submission	Status	#Warning	#Failed	Notes
AIB Group (UK) p.l.c. / First Trust Bank	v1.1.1	v1.1.7	Client secret basic	code id_token	23 Feb 2018	Download	PASSED	1	0	
Bank of Ireland										
Barclays										
Danske										
HSBC	v1.1.2	v1.1.11	Client secret basic	code, code id_token	30 Apr 2018	Download	PASSED	2	0	
First Direct Bank	v1.1.2	v1.1.11	Client secret basic	code, code id_token	06 Jun 2018	Download	PASSED	2		
Marks and Spencer Bank	v1.1.2	v1.1.11	Client secret basic	code, code id_token	06 Jun 2018	Download	PASSED	2		
Lloyds Bank	v1.1.1	v1.1.9	Client secret basic, client secret post	code, code id_token	09 Mar 2018	Download	PASSED	1	1	NB: Platform currently unable to handle query parameters in redirect URI. To be resolved. 1 test still to be run. Non-blocking issue.
Nationwide	v1.1.2	v1.1.9	Client secret basic	code id_token	28 Mar 2018	Download	PASSED	1	1	NB: Platform currently unable to handle query parameters in redirect URI. Incorrect error returned in response to access token sent as a query parameter. Both issues shortly to be resolved. Platform accepts TLS1.0&1.1 connections due to limitations in customer base.
RBS										
Santander	v1.1.1	v1.1.11	client secret basic	code id_toke	25 May 2018	Download	PASSED	1	0	
Ozone (Mock Bank)	v1.1.2	v1.1.7	client secret basic, client secret post, private key	code, code id_token	26 Feb 2018	Download	PASSED	1	0	See O3-Ozone
Forgerock (Mock Bank)	v1.1.2	v1.1.9	Private key	code, code id_token	09 Mar 2018	Download	PASSED	1	0	See https://backstage.forgerock.com/knowledge/openbanking/home
Ostia Solutions (Sandbox Provider)	v1.1.2	v1.1.9	Private key	code	02 Mar 2018	Download	PASSED	0	0	See Ostia Solutions

Figure 18: Original publication of Conformance and Security Certificates by Open Banking (UK)

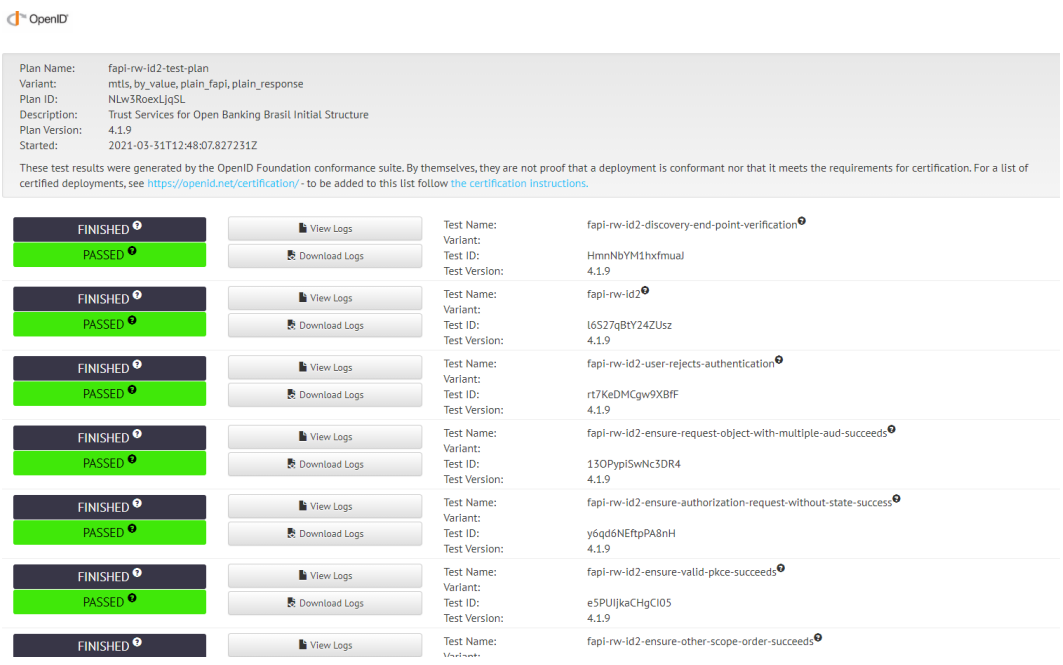


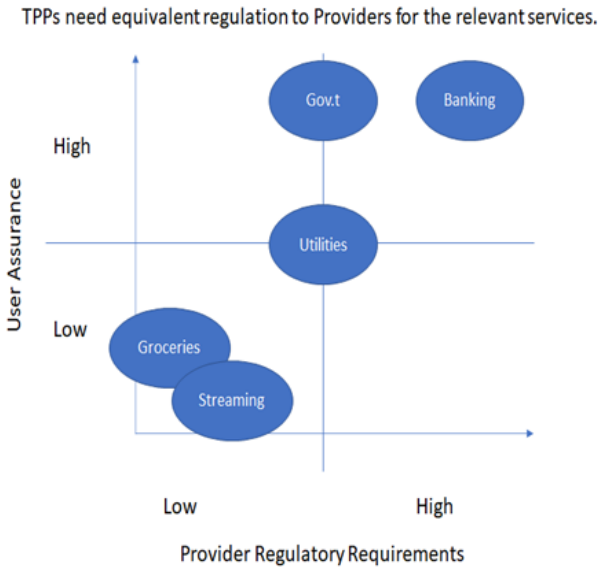
Figure 19: Detailed certification test results from Open ID Foundation to support certification[69]

[69] https://www.certification.openid.net/plan-detail.html?plan=NLw3RoexLjqSL&public=true

Inter-operability and Cross-Sector Symmetries

As we saw in our paper on Authentication and Trust, there were a couple of symmetry principles identified that will aid the cross-sector implementation of Smart Data:

Figure 20: 2-axis plotting of sectors against User assurance and Regulatory requirements.



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.

We see these same principles also applying to accreditation, with a minor modification to apply for Principle 1 as 'TPP Accreditation Experience'

In our 2020 research, we recommended a commitment be made to symmetry by all Sectors. However, our experiences in the past 12 months highlight that implementation is a challenge within any single sector, without trying to consider inter-operability up front.

However, given the similarities in fundamental needs for all sectors, we see opportunities to parallel implementation of essentially the same processes in different sectors leading to the same outcome of increased standardisation and interoperability.

Focus on removing friction for any sector and be deliberate that codifying a standardised approach is required. Once multiple sectors have adopted this approach, we believe that the applications for standardised implementation on a cross-sector basis will become clear.

As a case in point, a number of open banking and open finance initiatives around the world are now using essentially the same standards and approaches, although there is no global coordination.

As a consequence, the UK's Department for International Trade (DIT) is now actively promoting the interoperability benefits for FinTech's operating in those markets to look at the UK, and vice-versa.

List of Figures

This publication is available from: www.gov.uk/government/publications/smart-data-accreditation-and-customer-experience-guidelines

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