Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK:

Is there a need for Certification, Trustmarks and an Independent Authority?

White Paper

written by Ewan Willars, Innovate Identity Ltd

innovate identity™

experts in id

OIX OPEN IDENTITY EXCHANGE

White Paper

CONTENTS

Page

PARTICIPANTS

PROJECT GROUP

- Government Digital Service (GDS)
- The Investing and Savings Alliance (TISA)
- Barclays
- Digidentity
- Experian
- GB Group
- HSBC
- LexisNexis Risk Solutions
- Post Office
- Open Identity Exchange (OIX)
- Innovate Identity

PEER REVIEW GROUP

- Department of Culture Media and Sport (DCMS)
- Financial Conduct Authority (FCA)
- Association of British Insurers (ABI)
- Building Societies' Association (BSA), also representing the Joint Money Laundering Steering Group (JMLSG) Board
- Finance and Leasing Association (FLA)
- Open Banking Implementation Entity (OBIE)
- Gambling Commission
- Remote Gambling Association (RGA)
- Sky Betting and Gaming
- International Airlines Group (IAG)
- Timpson
- tScheme
- Information Commissioner's Office (paper review only)
- FinTech Delivery Panel (FDP), also Onfido

EXECUTIVE SUMMARY

In the UK, where there remains no appetite for a national digital identity scheme, it is envisaged that several schemes will emerge servicing sector and cross-sector opportunities. A market where a consumer can have more than one digital identity, with more than one identity provider (IDP) already exists today. In future, each IDP could belong to more than one scheme, and relying parties may wish to accept digital identities from more than one IDP and, indeed, more than one scheme. This will reflect their individual risk appetites, and the range of intended uses.

This leads to the conclusion that a model will need to be developed to allow schemes to interoperate and to ensure an orderly, transparent market emerges. This can, in turn, help stimulate investment in the market and maximise the value of digital identity to all parties in the digital identity ecosystem. In the absence of such a model, the ability to scale and deliver cost-effective schemes becomes questionable, regulatory clarity may still be lacking for relying parties, and, for the end user, it would deliver only marginal benefit over the status quo today.

If a multi-scheme, interoperable digital identity market is to emerge then trust, underpinned by appropriate contractual arrangements, is an imperative.

Trust itself is a concept that is often over-simplified; in reality it is a multi-faceted and somewhat complex concept, closely intertwined with interoperability. Trust comprises a number of factors, all of which must be satisfied: they include reliability (will the service work, and what happens if something goes wrong?), the credibility and integrity of the organisations, the clarity of the service being offered, and whether the user can expect their security and privacy to be upheld.

However, when broken down into the mechanisms that exist to both develop and then communicate trust, ***how*** they might be applied to the digital identity market – and ***by what type of organisation*** – become much more practical and grounded discussions.

So, what are the mechanisms able to bring about trust, and what type of market structure and organisations or authority might be needed to ensure the integrity of the market?

TRUST MECHANISMS

The market mechanisms able to develop, maintain and communicate trust within an ecosystem are well developed, but have seldom been collectively explored in detail regarding their potential use for digital identity. The research identified a wide number of specific mechanisms and how they might be applied; chief amongst them were:

TRUST FACTOR	MECHANISMS
STANDARDS	• Standardisation of process or product • Outcome-based standards • Principle-based standards
COMPLIANCE	• Self-reporting • Occasional spot checks / issue-based investigation • Data monitoring • Regular audits
CONFORMANCE	• Attestation • Certification • Accreditation

PERFORMANCE	• Legally binding service level agreements • Key performance indicators • Fraud prevention measures • Participant guidelines and customer charters
RECOGNISING AND PROMOTING TRUST	• Trustmarks • Online registers and databases • Digital seals and signatures
SUPPORT	• Customer charters • Security and privacy assurance • Dispute resolution mechanisms • Ombudsman

SEEKING THE RIGHT MIX OF TRUST MECHANISMS

The research uncovered the differing role that the mechanisms can play, whether employed to build trust between organisations in a business to business (B2B) identity transaction, such as between an IDP and a relying party, or between a business and a consumer (B2C) such as between an end user and their IDP.

Legislation and regulation, the agreement of standards, the application of conformance and compliance mechanisms, the development of the ecosystem rules, policies and principles are governance mechanisms that enable trust to be developed at a market level. The scheme rules, platforms and services, the identity transaction itself and the support provided to users and organisations in the event that something goes wrong are much more operational matters.

This approach led to the development of the 7-Layer Model, built around a layered approach to understanding the construction of a trusted digital identity ecosystem, and which helps to identify trust functions that are (at present) missing in the UK market.

LAYER	TRUST AND INTEROPERABILITY FUNCTIONS
1 STATE (INCLUDING LEGISLATION AND REGULATION)	• Provides legal and regulatory clarity. • Sets out the overarching legal environment that the ecosystem will operate within.
2 COMPLIANCE	• Provides legal and regulatory assurance. • Reduces regulatory risk.
3 ECOSYSTEM (INCLUDING STANDARDS, POLICIES AND GUIDANCE)	• Provides a basis for trust. • Provides interoperability and operational clarity.
4 CONFORMANCE (INCLUDING SOME COMPLIANCE FUNCTIONS)	• Provides assurance to participants. • Provides interoperability and operational assurance.
5 SCHEME (INCLUDING SERVICES)	• Accreditation/certification, registration, trustmarks (B2B). • Common platform and service definition.
6 TRANSACTION	• Trustmark (B2C) - assures performance and level of experience with the user. • Ensures an efficient transaction.
7 SUPPORT	• Manages risk and provides reassurance. • Ensures clarity concerning liability in the case of a compliance, conformance or transactional error. • Dispute resolution, recourse and recompense.

CREATING A CROSS-SCHEME TRUST FRAMEWORK

In the UK, where a market of multiple digital identity schemes and services is envisaged, a new form of multi-scheme trust framework will be needed to ensure interoperability and trust, not only within schemes, but across schemes and their participants.

The conclusion from this, considering the range of different use cases and identity transactions we may see, is that some form of collaborative, overarching organisation will be needed to provide a space for all stakeholders to define common, interoperable standards, and to agree the trust mechanisms and common rules needed for the ecosystem to operate successfully.

This is perhaps unconventional in the digital identity world, as it splits the trust framework into rules and mechanisms that are best agreed and operated across schemes, via an overarching organisation, and those that are better delivered at a scheme level. This is quite different from many markets, where the trust framework is synonymous with a single dominant scheme; splitting these two separate but complementary layers of trust seems to be a far more elegant and practical solution for the UK.

KEY FINDINGS

The research condensed a wide range of insights into a number of key findings that can inform the future development of the digital identity market:

1. **Interoperability and trust are closely and symbiotically linked – they need to be considered in tandem when developing an ecosystem.**
2. **Enabling an interoperable, trusted ecosystem will require some form of overarching organisation, particularly if it may be a multi-scheme environment.**
3. **Common digital identity standards will be required to underpin interoperability and trust across the ecosystem.**
4. **There are a clearly defined range of mechanisms able to build and maintain trust, but no single mix or model is appropriate for all markets; an appropriate mix needs to be found based on a stringent assessment of the ecosystem requirements.**
5. **Higher risk transactions (such as those involving personal data) require more stringent and enforceable trust mechanisms to be developed.**
6. **However, already highly regulated activities require less stringent compliance and oversight and instead, a greater focus on conformance by the overarching authority, given the strength of existing oversight and compliance mechanisms.**
7. **The user's interests must be a central consideration when seeking the means to establish and communicate trust and interoperability within an ecosystem – user trust is as vital as the need for trust between organisations.**
8. **The design and application of mechanisms to communicate trust needs to be considered with the type of transaction and recipient (and their capability) in mind – in digital identity, trustmarks could feasibly be used both for B2B and B2C transactions.**

One conclusion is certain, and that is without trust the market cannot be successful; trust must be placed alongside interoperability as a vitally important issue to be addressed. For government, industry and users alike, to see stakeholders acting collectively on the following recommendations would be a significant step towards unlocking a genuinely trusted digital identity ecosystem.

RECOMMENDATIONS

1. Industry to establish a collaborative organisation for digital identity

A collaborative organisation, the shape and form of which still needs to be agreed, would provide a space for open discussion to take place between industry participants across the public and private sectors. Stakeholders then to agree the mechanisms required to provide a trusted, interoperable cross-sector digital identity ecosystem, including:

- A set of common principles (including user outcomes and user support) to guide the participating organisations' digital identity operations and their interactions with other participating organisations and users.
- The certification, trustmark and/or registry functions that will be needed, and who or how to operate them.

For this to be successful a missing ingredient is the funding such an organisation would require. If a collaborative organisation's responsibilities are limited in number and scope the funding required will be small in comparison to some existing market authorities, but will nevertheless need to be agreed, most likely by participating organisations.

2. Industry and Government to collaborate in the development of digital identity standards

At present UK standards are not sufficiently developed to meet all of the needs of both public and private sectors. However, the existing Good Practice Guides 44 and 45, along with a range of international standards such as ISOs and the work of the Open ID Foundation and others could provide a firm foundation for the further development of digital identity standards. GPG45 in particular provides a method of identifying specific 'Identity Profiles' needed for particular digital identity use cases, with the level of assurance balanced to the level of risk.

The collaborative organisation could, as part of its role, develop standards that meet the needs of a range of use cases across sectors, take a wide view of forthcoming regulation, and ensure interoperability across different standards or approaches.

A collaborative programme facilitated by the organisation involving a range of government and industry stakeholders should further refine and publish the suite of open standards needed to underpin a trusted interoperable ecosystem able to serve a number of sectors and use cases.

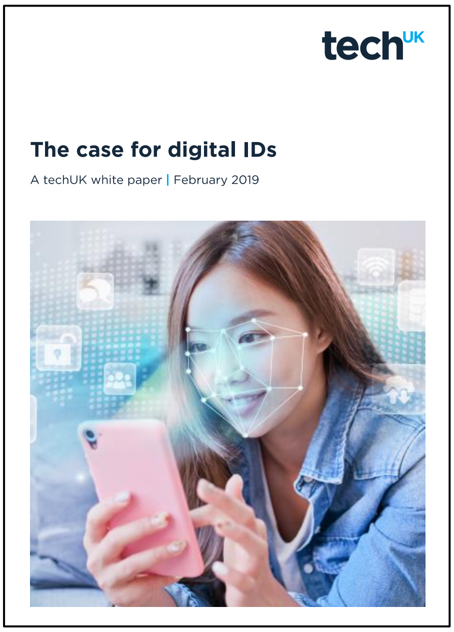
3. Competent National Authorities to formally recognise reusable digital identity

It would be a significant development if Competent National Authorities were to formally recognise the use of reusable digital identities for their areas of authority. This would provide additional regulatory clarity, reduce risk for relying parties and users, and thereby generate market demand.

Furthermore, once digital identity standards have been refined and established, and the level of assurance and outcome deemed suitable for specific use cases, it is recommended that the Competent National Authority for each sector or use case formally recognise the standards or identity profiles specific to their area.

CHAPTER 1: INTRODUCTION

The objectives of this project are to provide a lead on how trust can be established between all parties in an emerging interoperable digital identity ecosystem within the UK.



techUK

The case for digital IDs

A techUK white paper | February 2019

The project follows the publication in February 2019 of a techUK white paper, *The Case for Digital IDs*.[i] The paper argued that "a coherent strategy is urgently required, with leadership and governance which can link up the public and private sectors to enable strong, secure and trustworthy methods of digital identity to be widely available to citizens and businesses".

> **techUK Recommendation #8: "Nominate a competent independent authority for digital identity."**

In the UK, where there appears to be little appetite for a national digital identity scheme, it is envisaged that several schemes will emerge servicing sector and cross-sector opportunities as requirements and regulations vary.

A market where a user can have more than one digital identity, with more than one identity provider (IDP) exists today. In future, each IDP may belong to more than one scheme and relying parties may wish to accept digital identities from more than one IDP and, indeed, more than one scheme, reflecting their individual risk appetites, and range of uses.

DEVELOPING AN INTEROPERABLE MARKET

This has led OIX to the conclusion that a model will need to be developed to allow schemes to interoperate and to ensure an orderly, transparent market emerges. This can, in turn, help stimulate investment in the market and maximise the value of digital identity to all parties in the digital identity ecosystem. In the absence of such a model, the ability to scale and deliver cost-effective schemes becomes questionable and, for the user, a fragmented market delivers only marginal benefit over the status quo we see today.

An interoperable market model may come about in one of three ways:

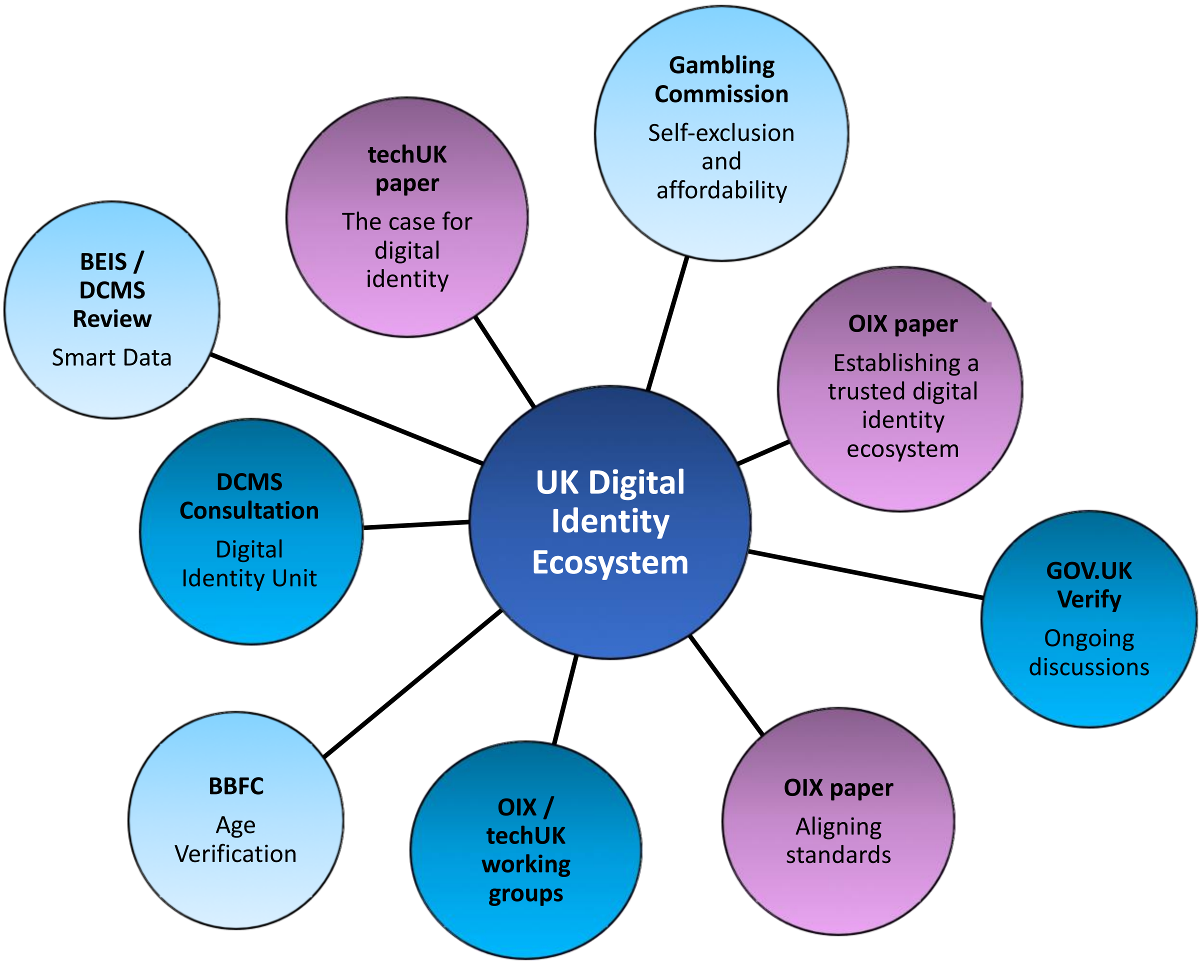
1. Government policy backed by action
2. An industry or industries-led approach
3. Through the collaboration and collective efforts of all parties in a digital identity ecosystem.

As far as the UK is concerned, the Government has indicated on numerous occasions that it sees the private sector taking the lead, supported by Government.[ii] At an industry level, there is no compelling reason or imminent forcing action (such as legislation or regulation) to push competing providers to collaborate in this way. This leaves the third way as the most realistic approach to developing the model.

IDENTITY INITIATIVES

As the UK digital identity ecosystem continues to develop, there are a wide range of consultations, research and publications, and each provides an opportunity to shape the emerging market. However, while the various initiatives each help to sculpt the market and the collective vision, care needs to be taken to co-ordinate diverse actions; interoperability requires alignment, and clarity.

FIGURE 1


UK Digital Identity Ecosystem
Gambling Commission Self-exclusion and affordability
techUK paper The case for digital identity
BEIS / DCMS Review Smart Data
OIX paper Establishing a trusted digital identity ecosystem
DCMS Consultation Digital Identity Unit
GOV.UK Verify Ongoing discussions
BBFC Age Verification
OIX / techUK working groups
OIX paper Aligning standards

THE IMPORTANCE OF TRUST

Even a highly interoperable model can only be successful if confidence and trust can be established across the ecosystem, thereby encouraging participation.

This project has brought together input from a range of parties who might themselves form part of a future digital identity ecosystem, to explore what is needed to generate trust, and to consider how the means to establish and promote trust to users and businesses might respond to underlying market needs. This report examines the various trust mechanisms that are commonly used in other industries, the principles that lie behind the choice of trust mechanisms to employ, and the choice of organisation or industry layer to operate them.

In so doing it hopes to inform the further development of the digital identity market in the UK as it continues to form, by provide recommendations to government and regulators, and to industry, for the development of a trusted digital identity ecosystem in the UK.

PROJECT HYPOTHESES

The hypotheses below have informed the development of this project.

1. In an emerging market of interoperable digital identity schemes trust will be an important element:
    a. IDPs and relying parties will need simple but effective assurances that the other party meets the required standards, technical requirements and complies with scheme rules as well as relevant legislation and regulation.
    b. Users will need assurances that any identity scheme or identity transaction conforms to a known level of trust, that it will work effectively, and that they have the required degree of protection.

2. That level of trust can only be assured through appropriate certification, encapsulating such matters as legal and regulatory compliance, consumer protection, dispute resolution, recompense, approved standards, and certification processes, and appropriate signals able to communicate a firm or scheme's conformance.

3. The act of assuring and communicating trust is best governed by an independent authority (or authorities) of some type.

PROJECT OBJECTIVES

- **To establish a model for an ecosystem that can underpin risk mitigation and build trust; e.g. legislation, regulation, governance, ethics and social justice, standards.**
- **To determine the key elements of the ecosystem and where these principles need to be applied.**
- **To review the mechanisms available to establish and assure trust.**
- **To consider and make recommendations on how trustmarks and other mechanisms to communicate trust could be implemented in the UK.**

TERMS AND DEFINITIONS

It was agreed at the outset of the project to set out a range of key terms and definitions for the purposes of this report.

FIGURE 2

TERM	DEFINITION
Attribute	A quality or characteristic ascribed to an individual.
Attribute Provider	A source of verified attribute information concerning an individual.
Authentication	The process by which a system confirms the user is known to that system, usually through the use of one or more Credentials.[iii]
Digital identity	A collection of data belonging to a claimed identity, usually which has been verified by trusted parties, which can be used as a digital representation of an individual.
Identity Provider	An organisation that provides services to an individual to manage their Digital Identity. Through the Identity Provider (IDP) users can authenticate to relying parties to access services.
Identity Transaction	The exchange of identity data to fulfil a transaction. For example, identity transactions can be between the individual and their IDP, or between the IDP and a Relying Party (RP) as well as other variations.
Independent Authority	An industry organisation with an independent remit, with authority granted by a national administration, regulator or otherwise competent authority, that carries out a number of governance and trust functions to help ensure the functional operation of a market.
Industry Authority	An industry organisation with an independent remit, with authority granted voluntarily by its industry members, that carry out a number of governance and trust functions to help ensure the functional operation of a market.
Interoperability	The ability of two or more components or systems to exchange information, and to trust and use the information that has been exchanged.
Relying Party	An organisation relying on an IDP to determine the identity or attributes of an individual, usually in order that the individual can access a service.
Scheme *	A common, contractually binding conformance agreement amongst multiple parties; IDPs and RPs can join the scheme, making it easier for users to exchange verified digital identity information.
Standards	Standards provide rules and guidelines established by consensus, or by a competent authority (govt, regulator, industry body), that apply across a defined ecosystem or market.
Technical Standards	The exact, detailed specifications to be met by a system, or process, in order for it to meet essential requirements and achieve interoperability.
Trust	The degree of confidence between participants in a transaction or delivery of a service that the other parties will honour their side of the agreement.
Trust Framework *	A trust framework provides a trusted environment that can include a range of participating organisations, or schemes, where participants desire to engage in a common type of transaction with other participants, and to do so consistently and predictably. Trust frameworks are typically based on a set of common standards, principles, and agreements.
Trust Mechanisms	A variety of processes such as certification, oversight and the use of registries and trustmarks to develop, assure, communicate and promote trust in a service or service provider.
Trustmarks	Visual or written representations of trust and user or business protection, and to assert that a service provider is accredited, certified or otherwise assessed.
User	For the purpose of this report, a user is an individual who is seeking to assert their identity to access a service.

* The definition of what constitutes a 'scheme' and a 'trust framework' are often conflated in literature. In practice they can be combined, or be separate, and each may carry out a different layer of trust functions; this report has consequently defined them as two separate concepts.

CHAPTER 2: KEY CONCEPTS – TRUST & INTEROPERABILITY

Before reviewing the mechanisms and options available to create trust in an interoperable market, and issues such as trustmarks or certification processes, it is important to establish clarity regarding the two key concepts: interoperability and trust.

Interoperability and trust have an interlinked relationship in a functioning market. An interoperable digital identity market might be described as functioning efficiently, effectively, and consistently across a number of market participants. A high level of interoperability will enable a number of trust factors to be satisfied:

- That the experience will be efficient.
- That the transaction will be effective in the task it is expected to satisfy.
- That the data exchanged will be correct.
- That the organisations exchanging data will use it in a trustworthy manner.
- That the expectation of failure is low, and that liability and redress are agreed when it does.

Interoperability will ensure a workable market; trust is a significant factor affecting the willingness of users to participate in the market and the value they place on it. Both are needed for a functional market to flourish.

INTEROPERABILITY

The concept of interoperability was originally derived from the world of technology and software, and is defined in that context as "the ability of two or more components or systems to exchange information and to use the information that has been exchanged."

We can break this concept down further, by looking at the sub-concepts of technical, semantic and organisational interoperability[iv], as well as the concept introduced here of 'user interoperability', and identify some of the mechanisms available to achieve these aims (the mechanisms themselves are explored in detail in the next chapter).

FIGURE 3

INTEROPERABILITY CONCEPT	DESCRIPTION
Technical Interoperability	The ability of two or more participants in a market to accept data from each other and perform a given task in an appropriate and satisfactory manner.
Semantic Interoperability	Ensuring that the various participants within a market are able to share information with an unambiguous, shared meaning and value.
Organisational Interoperability	Ensuring that objectives and processes are aligned, and relationships clearly defined across multiple organisations participating in a market.
User Interoperability	Ensuring users can trust the market actors and easily access their preferred service, through whichever participating organisation they interact with.

The first three interoperability concepts in figure 3 above are well-established, used in recent literature such as the European Interoperability Framework.[v] They are usually used to describe peer -to-peer organisational relationships; the direct relevance to the user is often only inferred.

It is important to note that semantic interoperability will remain a challenge in digital identity while there is no established lexicon or common list of defined terms and definitions. To establish a common language of identity would be a major step forward.

An interoperable digital identity ecosystem will require strong user buy-in and participation, and users clearly lie at the centre of a functioning, interoperable market. Interoperability for users is expressed as their experience of a good, consistent service available across a range of service providers, and the assurance that if something goes wrong that there are mechanisms in place to protect the user. For the purpose of this paper, this explicitly user-centric interoperability concept is described as User Interoperability.

The table below sets out some mechanisms typically used to facilitate or ensure market interoperability, and illustrative examples from the digital identity and personal data ecosystem.

FIGURE 4

INTEROPERABILITY CONCEPT	INTEROPERABILITY MECHANISMS	EXAMPLES (not exhaustive)
Technical Interoperability	• **Standards or standardisation** (to describe common ways of doing things, and the specifics of how this is to be undertaken or what the result needs to be). Technical Interoperability can also be achieved via **legislation or regulation**. • **Attestation, certification or accreditation**, alongside some form of **assurance of compliance** (to ensure that standards or rules are adhered to).	• GPG45 • eIDAS Regulation • Strong Customer Authentication Regulatory Technical Standard
Semantic Interoperability	• Establishment of **common syntax, terms and definitions, shared ontology,** agreed via **guidance**, **schemes**, and **legal agreements** (to ensure common understanding of data types and values).	• Good Practice Guides • JMLSG Guidance Notes
Organisational Interoperability	• **Industry agreements** and the operations of **industry associations, schemes** and **trust frameworks, SLAs** and **change management protocols** (to ensure common objectives are agreed, to provide market oversight and fair play, and alignment between participants).	• GOV.UK Verify Scheme Rules • TISA Identity Scheme Trust Framework (in development)
User Interoperability	• **Communications tools** such as **trustmarks and trust registries** (to communicate the assurance of quality and compliance). • **Certification, accreditation or attestation** (to assure consistency of user experience and that the service or product 'will work'), and performance metrics established via KPIs and SLAs. • **Consumer protections** such as **guarantees or dispute resolution services** (to provide confidence that the user will be treated fairly and ethically, their data will be protected, and that there are liability and dispute resolution agreements, and repair and recovery protocols in place if something goes wrong).	• GOV.UK Verify Government-backed trustmark • ICO Data Sharing Code of Practice

TRUST

Interoperability underpins but also relies upon trust and trust mechanisms. Without trust, market participation by either organisations or users is limited. Without interoperability, trust is compromised.

Trust is often described as encapsulating several different aspects:

- Confidence in a product or service's legal standing.
- Expectations of a satisfactory degree of efficiency and effectiveness.
- That there is a safety net, or means to settle a dispute if something goes wrong.
- That your personal information will be handled appropriately, and your privacy and security will not be compromised.

Trust can be expressed as a series of concepts and questions, mapped to market functions: [vi] [vii]

FIGURE 5

TRUST CONCEPT	QUESTION	TRUST AND INTEROPERABILITY FUNCTIONS
Reliability	Is it consistent? Will it do what they say it will do?	• Standards • Legal contracts and SLAs • Certification and accreditation
Integrity	Is there a set of values or behaviours, will the other party stick to them, and do the right thing even if costs them	• Legal contracts • Dispute resolution • Codes of conduct • Trustmarks and registers • Account recovery and repair
Credibility	Does the other party have the necessary ability, competence, technical knowledge?	• Licensing, certification and accreditation • Trustmarks • Oversight and enforcement
Clarity	Is what is being provided and what is expected of both parties clear and transparent?	• Education and awareness raising • Trustmarks and registers
Security	Is there protection to ensure the security of any information being shared?	• Standards • Oversight and enforcement
Privacy	Is there a suitable level of protection to ensure that privacy will not be compromised?	• Legal • Codes of conduct • Oversight and enforcement

In this chapter a number of concepts central to understanding trust and interoperability and their relationship have been introduced. In turn, this helps the reader to understand some of the roles and outcomes required for interoperability and trust to be established, and provides a framework for understanding what can be surprisingly slippery ideas.

The concepts above have a practical expression in the structure of a market ecosystem and the roles of participating organisations. Without these elements of trust, users and organisations will be unable to exchange data and provide and receive services. In the next chapter we examine the practical trust mechanisms in more detail, and how they can be utilised within an ecosystem.

CHAPTER 3: ESTABLISHING AND COMMUNICATING TRUST

Answering the trust questions positively and ensuring all users and participating organisations are able to trust their interactions with others is critical. This is true whether they are an individual or a business; each transaction has to be trusted for an interoperable market to function effectively. There are a range of trust mechanisms that can be applied, explored below.

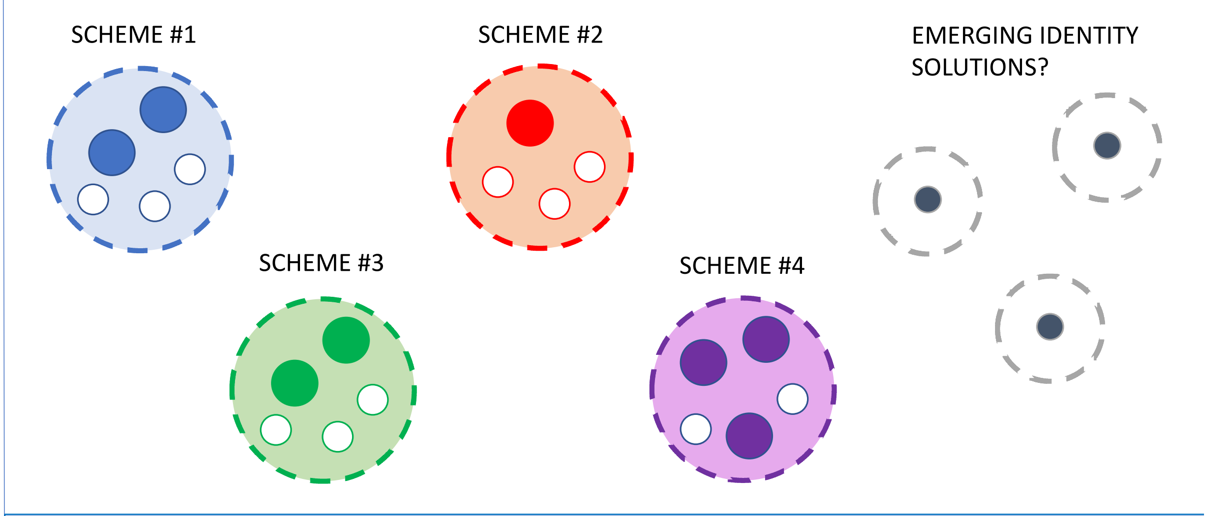
A) Standards

Standards describe common ways of doing things and may either include the specifics of how this is to be undertaken, or simply what the result needs to be, and usually how the result is to be interpreted or used. Standards can take the form of one of a number of approaches:

- **Standardisation** prescribes process and technical specification in detail, and often with little option to deviate, usually for risk or safety reasons.
- **Outcome-based standards** may not specify every element of a process but ensure a consistent and comparable outcome.
- **Principle-based standards** ensure that underlying conduct expectations are met, as well as consistent outcomes for the user or market participant, if not the exact features.
- Standards with **formal recognition** are either developed by government or regulators, or the standards are recognised and have legal status of some sort. They are often mandatory.
- Standards with **informal recognition** are typically developed by trade associations, or self-regulatory industry organisations, and are voluntary in nature and often have no legal status, although they may be contractually binding.

FIGURE 6

MULTI-SCHEME STANDARDS-BASED INTEROPERABILITY



MULTI-SCHEME INTEROPERABILITY WILL BE FOUNDED ON STANDARDS

- A common standards framework + technical standards, for intended regulated uses with some form of government or regulatory recognition, are able to provide semantic and high-level technical interoperability both **within** and **between** schemes (and could potentially encompass emerging identity solutions, such as self-sovereign identity or other alternative architectures).
- Scheme rules (including technical specification) provide operational interoperability amongst participants.
- Contractual arrangements and customer charters can then provide consumer interoperability, building on the functional interoperability founded on standards and scheme rules.

In figure 6 above, users and relying parties could potentially choose from a variety of IDPs (provided the user has a digital identity with the IDP) from across a variety of schemes, safe in the knowledge that they conform to the same overarching standards that are commonly recognised. It can provide the basis for both choice and competition within a wider trust framework underpinned by standards.

Formally recognised standards are needed to underpin interoperability in a multi-scheme digital identity ecosystem.

B) Compliance Mechanisms

Some form of formal checking by an appropriate authority or third party under a contractual, legal or regulatory mandate is usually required to ensure that compliance is achieved; appropriate oversight and control systems are therefore required.

Monitoring and being able to audit and investigate non-compliance, and to levy penalties for non-compliance are also critical elements for ensuring clarity on liability when something goes wrong and the form of redress, which is required for participating organisations and individuals alike.

A number of the mechanisms below may be used, sometimes in tandem, depending on the circumstance. Compliance options include:

- **Self-reporting** where transparency is used to encourage compliance and communicate it to other market participants or authorities.
- **Occasional spot checks / issue-based investigation** by an independent third party, whether scheme operator, industry authority or independent authority, can be used as an efficient way to investigate potential breaches.
- **Data monitoring** where publicly available information (or occasionally private data) is monitored by a third party to demonstrate compliance.
- **Regular audits**, usually forming part of a formal inspection / compliance assessment regime are more assured methods of ensuring compliance.

The evidence suggests that the frameworks that govern higher risk transactions involving sensitive personal or financial information or transactions of significant value more typically feature regulated or otherwise mandated reporting processes, and formal audit-focused compliance regimes.

Compliance and oversight regimes could be calibrated to the level of risk involved in a transaction (perhaps based on the Level of Identity required – see GPG45). For example, the compliance and oversight regime for an age verification solution would have very different requirements if calibrated to the level of risk, compared to a use case involving access to a financial product that includes some form of credit facility.

C) Conformance Mechanisms

Organisations agreeing to adhere to standards, establishing that participants in an ecosystem or scheme must have an appropriate level of competence, and (for example) that the right security and privacy controls are followed can be assured by a variety of conformance mechanisms. The options broadly include the following three methods:

- **Attestation** – an individual or organisation's own declaration that a standard has been adhered to, usually a formal, written statement by senior managers or a form of annual self-reporting – this may also have formal regulatory or legal status.
- **Certification** – formal communication that a process, product or organisation has been checked by a competent third party or authority, and conforms to a level of quality, or has achieved a required level of attainment.

- **Accreditation** – formal recognition that an organisation is competent to perform specific processes, activities, or tasks (accreditation) and has some form of permission to operate (licencing).

The level of formality and relative strength of the mechanism of choice is linked to:

a) the real (or perceived) degree of risk involved in the transaction (the likelihood and severity of the negative impact on either party if 'something goes wrong' with the transaction), and therefore to

b) the willingness of participants to take part in a given transaction without the necessary assurances.

D) Performance Mechanisms

Ensuring efficient, effective performance within an ecosystem is vital to ensure trust is able to be developed amongst users and organisations alike. Consistent, predictable levels of performance – how long processes take, the latency of systems in-use, failure rates and the frequency or duration of outages or downtime, for example – are set out in contract, or by regulation. They help to ensure commercial models are sustainable, that end users and firm participants can expect a consistent and effective experience, and that the basis for liability and redress in the case of performance failure is clearly defined. The mechanisms include:

- **Legally binding Service Level Agreements (SLAs)** with agreed redress processes and compensation for participants if the agreed levels of attainment are not reached by another party – this forms the basis for a liability framework.
- **Key Performance Indicators (KPIs)** may not be contractually binding, but are a method of targeting, tracking and assessing levels of performance within a multi-party system.
- **Fraud prevention measures** including monitoring, reporting and the sharing of signals run alongside performance monitoring regimes, able to identify process weaknesses, identify adverse behaviour, and protect users and participating organisations.
- **Participant guidelines** and **customer charters** are other (usually not legally-enforceable) methods of agreeing and setting out performance level expectations for various types of participants.

The evidence from other schemes and trust frameworks suggests that a mix of these measures are usually deployed. Due to the regulatory risk among systems that support transactions of a high-risk nature, or concerning financial or personal data being exchanged, service and performance levels are commonly set out in contract or are otherwise binding and have clear penalties in place for significant performance failure.

E) Mechanisms to Recognise and Promote Trust

The trust factors above are explicitly or implicitly communicated to users via a variety of means, often operating in tandem, and applied differently depending on whether the transaction in question is 'business-to-business' (B2B) such as between a relying party and an identity provider, or 'business-to-consumer' (B2C) such as between a user and their identity provider. The differences between effective B2B and B2C approaches are explored in greater depth later in the report. The main mechanisms are:

- **Trustmarks** – 'trustmark' is a term that in form can range from protected terms or labels signifying technical certification (e.g. ISO signification) to logos signifying membership of a trust framework or scheme of some sort and compliance with its obligations. Trustmarks are most often experienced in a B2C environment, although B2B examples also exist.

- **Online registers and databases** – a searchable or widely accessible registry of certified, accredited or licensed organisations is often used in conjunction with a trustmark of some sort, although they are sometimes used alone. Registries or databases are more usually used for B2B transactions, and may be used to check the veracity of a trustmark with an authoritative source.
- **Digital seals and signatures** – Electronic or digital seals or electronic signatures are means to digitally signify that a document or data conforms to a standardised degree of protection in term of assuring its authenticity and integrity. In the EU these functions were included in the eIDAS Regulation.

The provision of searchable registries of certified or accredited scheme participants seems to be relatively ubiquitous, although the degree to which they are accessed by users is less clear. Seals and signatures on the other hand are largely confined to a few specific regimes, and mainly operate under the interoperability framework provided by the eIDAS Regulation.

Trustmarks are frequently used – in fact there may be an argument that users are faced with too many. They can be utilised for both B2B and B2C, although in slightly different ways.

F) Support Mechanisms

As identified previously, a vital component for trust to be established is to ensure that the participants in a transaction believe that there is a low likelihood that things will go wrong, and if they do that there is a course of redress, and that a dispute would be dealt with fairly, and efficiently, and without loss or detriment.

- **Ethical behaviour and customer charters** - there is often an element of ethics involved in establishing trust – will an organisation act in the interest of the digital identity user, and will reasonable levels of behaviour and conduct be upheld by all parties?
- **Security and privacy assurance** - at a more technical level, is there an assurance that security and privacy is being upheld for the participant? This is often considered in term of protection for the individual user; however, protection measures are also a key element in B2B trust relationships.
- **Dispute resolution mechanisms** - clear, established and shared ways to resolve problems when they occur are frequently used in trusted systems to support participants.
- **Communicating trust and guarantees** – a variety of channels to communicate user support such as via B2C trustmarks or registries are common.
- **Ombudsman** - in some markets, an Ombudsman has been installed as an additional layer of user recourse.

Having a means to assure and communicate that an organisation will ensure users are protected appears to be a key trust component in all systems. Many support and protection measures are already set out in relevant consumer or corporate law, while many schemes develop additional support and consumer protection measures in addition to the legal minima.

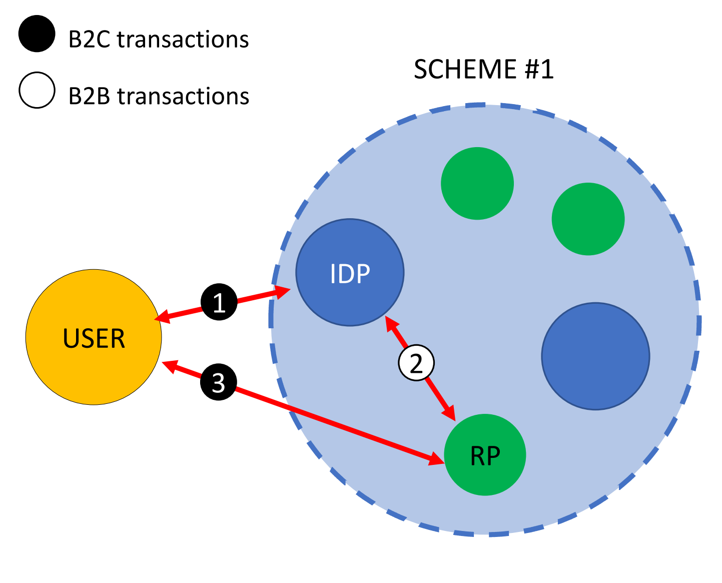
CHAPTER 4: TRUSTED TRANSACTIONS

Another determinant of the type of trust mechanism that may be considered most appropriate to a given relationship will depend on whether the relationship in question is B2C, involving an individual user at one end of the transaction, or B2B, where both ends of the transactions involve scheme participants.

Trust is required at a transactional level; the Transactional Analysis below examines a range of discrete transactions that may occur within a digital identity scheme, or between multiple schemes in an interoperable environment. This is simply being used in the report to help to illustrate the different approaches that may be taken to create and communicate trust in an ecosystem enabling reusable digital identity.

FIGURE 7

TRANSACTIONAL TRUST ANALYSIS: SCHEME-BASED TRANSACTIONS



Within a single scheme, there are a range of transactions, and each one must be founded on trust.

1 The initial transaction between a user and their IDP to establish their digital identity and provide consent to share.

2 The transfer of trustworthy attributes and transition of a trustworthy session with the user.

3 The transaction between user and relying party to access a service or product, as part of a scheme.

The transactional analysis presented in figure 7 showcases the divide between the transactions involving a user, and those which are strictly business-to-business in nature. Mapping the transactions types in more detail helps to demonstrate the complexity of relationships, even in a single-scheme ecosystem.

It may be that some relying parties may lie outside of the formal scheme and engage with IDPs on a transaction-by-transaction basis, or may more usually be contractually bound within the scheme. A scheme is defined in this report as a multi-party, contractual agreement (see Terms and Definitions).

While relying parties may have a position outside of the multi-party contractual arrangements of the scheme itself, they must still operate with the clear consent of the user, and in the knowledge that the IDP they are transacting with recognises the standards and levels of performance needed for the use case, including the required outcomes and performance levels, customer protection measures and liability arrangements.

The standards that underpin the transaction, and many of the mechanisms that set the basis for a trusted, interoperable ecosystem are likely to be provided by the framework layer across the ecosystem, rather than by a single scheme alone.

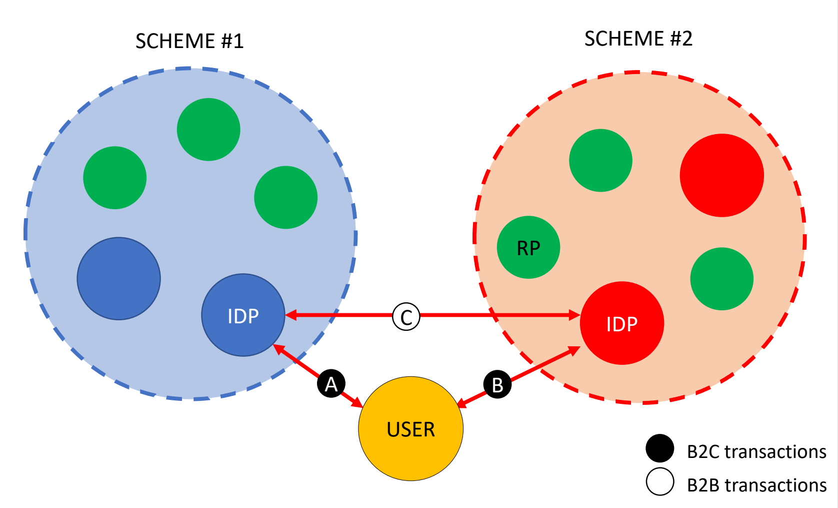
TRANSACTIONS IN A MULTI-SCHEME FRAMEWORK

The interoperability model in a multi-scheme environment could be provided by a shared trust framework that operates across schemes. A common set of standards, operating principles, and trust mechanisms could operate at a layer that exists above schemes to provide a trusted, interoperable and inclusive ecosystem.

In such a multi-scheme ecosystem, the range of transactions may become more varied still, and a couple of potential examples are demonstrated in figures 8 and 9 below.

FIGURE 8

TRANSACTIONAL TRUST ANALYSIS: MULTI-SCHEME TRUST (1)



A The initial transaction between a user and their IDP to establish their digital identity and consent to share it.

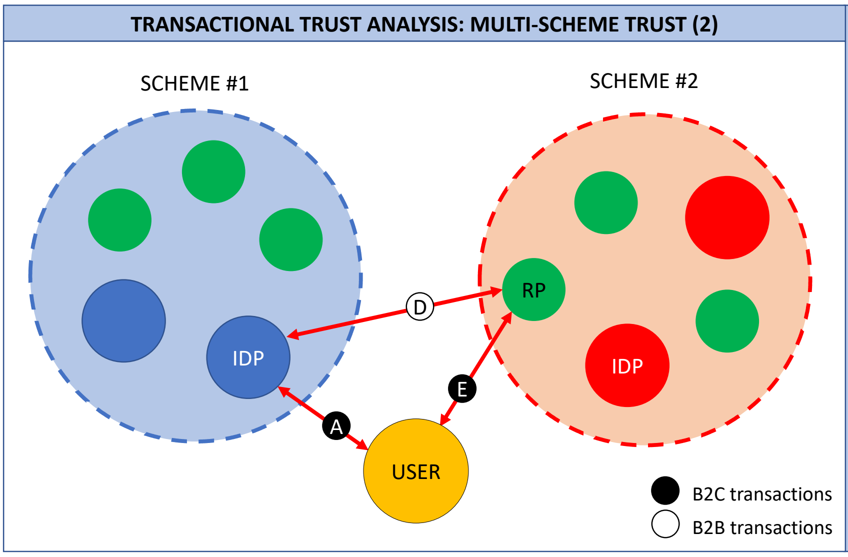
B A user may wish to transact with an IDP operating in a second scheme, to access additional services via setting up a second digital identity.

C This may involve a transfer of the user's data in a transaction between two IDPs, each operating in different schemes, within the interoperable market.

It may be that in practice few users would want data to be transferred between one IDP and another in order to set up an alternative IDP, but it is potentially possible within a wider trusted framework that operates to common standards, for example if one IDP fails. In such an example the transfer of trust would form a vital component.

FIGURE 9

TRANSACTIONAL TRUST ANALYSIS: MULTI-SCHEME TRUST (2)



A The initial transaction between a User and their IDP to establish their digital identity and consent to share.

D A User may wish to access a service from a Relying Party in one scheme, using their digital identity created with an IDP in a second scheme, requiring a transaction between the IDP and RP. It may also be possible for that RP to Step-Up the User's identity.

E The RP may then transact with the User.

The second illustration (figure 9) demonstrates that trusted transactions may also include relationships between an IDP and RPs that lies outside of the scheme in question but within the trusted ecosystem.

ARE TRUSTMARKS RELEVANT TO B2B AND B2C?

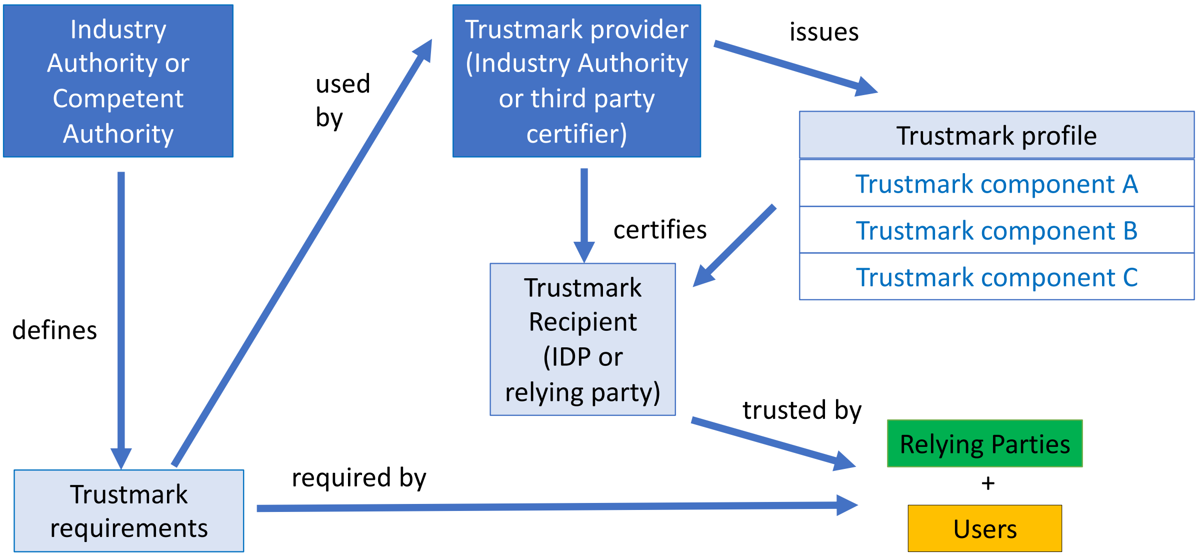
As we explored earlier in the report, some trust mechanisms are more suited or commonly used for B2B transactions, and some more readily for B2C transactions involving a user.

Most literature focuses on the role that trustmarks play in conveying trust to the user, i.e. for B2C use cases. In such cases the trustmark is often used to *implicitly* communicate the presence of standards, conformance, compliance and performance mechanisms covered earlier in the report, as well as communicating the level of user protection, and the level of support and redress if something goes wrong.

In a B2B context, a trustmark system is more frequently used to *explicitly* verify adherence to technical elements of a standard, with a conformance regime between different participating firms, or compliance with legal or regulatory obligations.

Figure 10 below demonstrates how such a trustmark might operate in practice:

FIGURE 10



Note that the three trustmark components included in figure 10 above are merely an illustration of how different sub-certification or sub-standards focused on specific elements could be used to certify the trustmark recipient – e.g. technical processes as well as security and privacy standards. The certification itself is more likely to be carried out by an independent organisation, whether that be an independent industry authority, or a trusted third party under contract.

B2B vs B2C TRUST: CONCLUSIONS

From the analysis we are able to draw broad conclusions regarding the appropriateness of various trust mechanisms, whether applied to B2B or B2C transactions:

FIGURE 11 a - f

TRUST FACTOR	B2B	B2C
Standards	Common, recognised Standards	

Notes: Common, recognised standards are vital to underpin B2B trusted transactions as well as to deliver interoperability. Standards must be open and inclusive, and able to evolve to meet changing needs. Users may not be aware of the existence or the detail of standards, but the trust mechanisms users rely on are founded upon the interoperable platform provided by standards.

TRUST FACTOR	B2B	B2C
Compliance	Reporting Monitoring Audits	

Notes: The sensitive, high-risk nature of some identity transactions requires formal reporting and oversight regimes – although some of these may in part be provided by existing legislative / regulatory regimes (examples may include anti-money laundering legislation, or data protection regulation such as GDPR). An overarching trust framework would ensure consistency of approach across the ecosystem, even where compliance requirements differ according to the use case.

TRUST FACTOR	B2B	B2C
Conformance	Attestation Accreditation Certification	

Notes: As with standards, conformance mechanisms do not directly include users, but they benefit from a high-conformance ecosystem.

TRUST FACTOR	B2B	B2C
Performance	SLAs KPIs Participant Guidelines	Customer Charters Contractual performance User experience

TRUST FACTOR	B2B	B2C
Communicating trust	Register of certified / accredited participants B2B trustmarks	Register of certified / accredited participants B2C trustmarks

Notes: Some literature has cast doubt on the efficacy of trustmarks in a B2B context.[viii] However, as explored in figure 10 on the previous page, B2B trustmarks can play an important role as an explicit signifier of certification or compliance.

TRUST FACTOR	B2B	B2C
Support	Participant Guidelines Liability framework Scheme rules Contracts and commercial law	Customer charters Dispute resolution services Financial or other guarantees Contracts and consumer law

CHAPTER 5: THE NEED FOR A COLLABORATIVE ORGANISATION FOR DIGITAL IDENTITY

Unless the lack of appetite for a single collaborative scheme in the UK changes it seems likely, at least in the short to medium term, that the digital identity market in the UK will feature more than a single scheme – there may be a number of schemes with a variety of technical architectures, needing to conform to common outcomes.

In mono-schemed ecosystems or those dominated by a single scheme for regulated uses, trust mechanisms are commonly developed and operated at scheme level – in a mono-scheme environment the mechanisms are therefore able to be applied right across the (national) identity ecosystem via a single scheme-based authority.

In a multi-scheme ecosystem this would not be possible – trust and interoperability would need, to some degree, to exist across and between schemes and their participants. For that to happen, a cross-scheme trust ecosystem would necessitate some form of independent co-ordinating organisation, to agree common standards, the trust mechanisms required and how they should be operated, and common elements such as common principles or user charters.

For the Government to deliver on its statement that it wishes to 'build a flourishing ecosystem',[ix] in order to develop a trusted interoperable digital identity ecosystem that encompasses multiple schemes, some form of cross-industry independent collaborative body will be required.

THE 7-LAYER MARKET MODEL

A market's structure is often described as consisting of a number of layers, each corresponding to certain types of roles and functions; for example, for software and data systems, layered models have been developed to describe the operating and governance structure of a network or specific environment.

To help establish a common understanding of the ecosystem, a 7-Layer hierarchical model has been developed.

Learning from existing models such as the Open Systems Implementation (OSI) Model,[x] the 7-Layer Market Model (see also figure 13) explores the market layer at which specific mechanisms are usually developed and implemented, identifying the component parts that need to be developed within the emerging digital identity ecosystem to generate trust, and interoperability.

FIGURE 12

7-LAYER MARKET MODEL
1 STATE
2 COMPLIANCE
3 ECOSYSTEM
4 CONFORMANCE
5 SCHEME
6 TRANSACTION
7 SUPPORT

What does this look like in detail? What are the trust and interoperability functions of each layer, and what examples can we see in the wider market?

FIGURE 13 a

	LAYER	TRUST AND INTEROPERABILITY FUNCTIONS	DESCRIPTION	EXAMPLES
GOVERNANCE	**1 STATE** (INCLUDING LEGISLATION AND REGULATION)	Provides legal and regulatory clarity. Sets out the overarching legal environment that the ecosystem will operate within.	a) Sets out the specific policy, order or mandate for a regulated, independently supervised or non-regulated, non-supervised market. (Note that this may not exist).	• eIDAS
			b) Provides legal clarity around aspects of the market operation.	• GDPR (Data Protection Act) • Equality Act • Competition Act
			c) Legislation and regulation (including industry guidance) - this may need to be reviewed and amended to explicitly recognise the acceptability of federated digital identity.	• UK Money Laundering Regulations • JMLSG Guidance • FATF
	2 COMPLIANCE	Provides legal and regulatory assurance. Reduces regulatory risk.	Assurance to establish that market participants have met their obligations to meet legislative and regulatory requirements.	• FCA Compliance Reporting
	3 ECOSYSTEM (INCLUDING STANDARDS, PRINCIPLES, POLICIES AND GUIDANCE)	Provides a basis for trust. Provides interoperability and operational clarity.	a) Sets out the principles, policies, procedures and standards (including guidance and best practice) required to ensure interoperability, privacy, security and performance levels across the participants in the market.	• GPG44 • GPG45 • OIDC • SAML • ISO27001
			b) Sets out the business and legal procedures, standard terms and conditions (minimum requirements) covering such elements as account recovery and identity repair, liability, dispute resolution and recompense.	• Obligations common to all schemes.

Continued from the previous page:

FIGURE 13 b

GOVERNANCE	**4 CONFORMANCE** (INCLUDING SOME COMPLIANCE FUNCTIONS)	Provides assurance to participants. Provides interoperability and operational assurance.	Sets out the obligations on market participants to meet the standards requirements, contractual and (potentially) regulatory obligations. As well as conformance, some compliance assurance.	• tScheme / Lloyds certification manual.
OPERATIONS	**5 SCHEME** (INCLUDING SERVICES)	Accreditation / certification and registration (B2B), and trustmark (B2B). Assures rules of operation have been followed.	The business, legal and technical rules of operation that form a multi-party contractual arrangement, to meet the terms and conditions of relying parties, for one or a number of use cases, and to ensure the integrity of the scheme. Includes any required platforms or services.	• GOV.UK Verify Operations Manual. • Work in other jurisdictions, e.g. DTA in Australia.
	6 TRANSACTION	Trustmark (B2C) - assures performance and level of experience with the user. Ensures an efficient transaction.	Trust framework procedures and technical rules. Ensures that each transaction happens as it should and to the benefit of all parties involved.	• GOV.UK Verify Operations Manual. • GOV.UK Verify / Govt trustmark
	7 SUPPORT	Manages risk and provides reassurance. Ensures clarity concerning liability in the case of a compliance, conformance or transactional error.	Ensures that participants including end users have recourse if problems occur. Including the means to raise grievances, dispute resolution mechanisms, and a means to secure recompense or restitution for a user or organisation.	• GOV.UK Verify Operations Manual.

In the 7-Layer Model, a trust framework forms the basis for the business, legal and technical arrangements contracted at scheme level. Given the emerging shape of the UK market and the aim to establish an interoperable market, the digital identity ecosystem will require overarching rules, at a business, legal and technical level, to govern interoperability.

These need to be set out in arrangements that schemes conform with. This leads to the concept of a multi-scheme interoperable trust framework (as distinct from a scheme trust framework).

i **A number of the trust mechanisms will need to be defined and possibly certified at a cross-scheme level, by an independent overarching organisation of some kind.**

MAPPING ROLES AND RESPONSIBILITIES

FIGURE 14

	LAYER	GOVERNMENT (HMT/DIU/FCA)	OVERARCHING AUTHORITY	SCHEME	IDENTITY PROVIDER
GOVERNANCE	STATE	Implement 5MLD (HMT) and give digital identity standards formal recognition (FCA)	Provide high level guidance – interprets standards.		
	COMPLIANCE		Define and implement cross-scheme compliance register / certification	Define and implement compliance requirements within scheme.	Implement and comply
	ECOSYSTEM	Define digital identity standards for public and private sector. (Digital Identity Unit - DIU)	Define sectoral standards. Ensure interoperability across standards	Implement	Implement
	CONFORMANCE		Provides principles and outcome-focused conformance, some compliance elements	Defines and operates scheme-based conformance assurance – certification and monitoring	Deliver and demonstrate conformance and compliance where required.
OPERATIONS	SCHEME		Define B2B trustmark Educates and raises business awareness	Operate scheme-level B2B trustmark	
	TRANSACTION			Ensures scheme performance Operate B2C trustmark Educates and raises user awareness	Ensures performance Educates and raises user awareness
	SUPPORT		Defines policies and processes.	Provides	Provides

In figure 15 below, the process of verifying the age of a customer by a remote gambling firm is used to illustrate the interaction between the layers, the function of the seven layers in practice, and who is involved at each stage. It is interesting to note that the end user is only directly involved in the final three layers, and the Transaction and Support layers in particular.

FIGURE 15

LAYER	USE CASE EXAMPLE: AGE VERIFICATION	WHO IS INVOLVED?
LAYER 1 **STATE**	Money Laundering Regulations require identification of customers. The Digital Economy Act 2017 appoints BBFC as age verification regulator.	• Government • Regulators
LAYER 2 **COMPLIANCE**	BBFC role to set and enforce standards.[xi] Gambling Commission publish the Licence Conditions and Code of Practice (LCCP) and operate an enforcement regime.[xii]	• Regulators / Supervisors • Gambling Firms
LAYER 3 **ECOSYSTEM**	JMLSG Guidance sets out money laundering controls. The LCCP sets out the conditions that must be followed by gambling companies. The BBFC will decide the age verification processes that will be allowed.	• Regulators / Supervisors • Gambling firms
LAYER 4 **CONFORMANCE**	The LCCP also provides (mainly outcome-based) codes of practice, including sector-specific detail. Some elements of the Code are are mandatory, some of which are voluntary but have a legal standing.	• Regulators / Supervisors • Gambling firms
LAYER 5 **SCHEME**	Using a digital identity to identify a customer and verify their age would require service or scheme/s to be developed, with further rules, policies and trust mechanisms utilised between the user, the relying party and IDP.	• Users • Identity Providers • Relying Parties • Scheme Operators
LAYER 6 **TRANSACTION**	Standardised processes ensure information is exchanged effectively, the transaction between the RP and IDP is trusted, and the transaction takes place to agreed levels of performance and user experience.	• User • Identity Provider • Relying Party
LAYER 7 **SUPPORT**	If something goes wrong with the transactions, or the identity is compromised, there are agreed customer dispute mechanisms, liability agreements and the means of obtaining recourse for the user.	• User • Identity Provider • Relying Party

CHAPTER 6: CONCLUSIONS

To capture the concepts and practical findings uncovered in this research project, a number of key findings have been distilled that apply to the development of a trusted digital identity market.

KEY FINDINGS

1. **Interoperability and trust are closely and symbiotically linked – they need to be considered in tandem when developing an ecosystem.**

2. **Enabling an interoperable, trusted ecosystem will require some form of overarching organisation, particularly if it may be a multi-scheme environment.**

3. **Common digital identity standards will be required to underpin interoperability and trust across the ecosystem.**

4. **There are a clearly defined range of mechanisms able to build and maintain trust, but no single mix or model is appropriate for all markets; an appropriate mix needs to be found based on a stringent assessment of the ecosystem requirements.**

5. **Higher risk transactions (such as those involving personal data) require more stringent and enforceable trust mechanisms to be developed.**

6. **However, already highly regulated activities require less stringent compliance and oversight and instead, a greater focus on conformance by the overarching authority, given the strength of existing oversight and compliance mechanisms.**

7. **The user's interests must be a central consideration when seeking the means to establish and communicate trust and interoperability within an ecosystem – user trust is as vital as the need for trust between organisations.**

8. **The design and application of mechanisms to communicate trust needs to be considered with the type of transaction and recipient (and their capability) in mind – in digital identity, trustmarks could feasibly be used both for B2B and B2C transactions.**

CONCLUSIONS

Most clear amongst the conclusions drawn from the research are a) that a cross-sector collaborative organisation will be needed, and b) that common standards will need to be in place in order for interoperability and trust to be established. It may be too early to define the exact shape or form that the collaborative organisation will take, however the key role of providing a single collaborative space for government and industry stakeholders to discuss and develop standards, common principles, and agree the trust mechanisms required and how they will operate is clear.

In considering the mix of trust mechanisms that may be needed to establish a trusted, interoperable ecosystem, given the high degree of regulation and existing compliance controls established for the sharing and use of personal data (such as GDPR), and concerning the onboarding and identification of customers by relying parties (in the Money Laundering Directives and JMLSG Guidance), it could be argued that the digital identity ecosystem will not need highly intrusive compliance and oversight mechanisms.

On the other hand, the high-risk nature of digital identity transactions, and perceptions of high levels of risk by users and relying parties will mean that some form of conformance and compliance regime will be needed – by way of establishing and then communicating trust within the ecosystem. Conformance and compliance frameworks build economic value by opening up participation in the trusted market to new users and organisations, and by developing the option for solutions or standards to be recognised by regulators. This role could be played by Competent National Authorities recognising specific digital identity standards developed through cross-industry and government collaboration.

Considering these two factors together suggests that some form of formal certification or registry of trusted participants will be needed, but perhaps assured by attestation rather than an intrusive compliance regime at authority level. However, the assurance provided needs to be sufficiently robust to provide the foundation for the re-use of the identity across multiple relying parties. Finding an appropriate balance and aligning this across different use cases will be vital.

If the trusted environment covers multiple schemes, potentially with multiple technical processes and architectures, conformance and compliance may favour principle-based or outcome-based rules.

This approach:

- Provides a common environment across multiple schemes, and alternative architectures.
- Gives the flexibility needed to accommodate innovation.
- Enables differentiation, providing competition and choice for users and relying parties.
- Ensures a common minimum level of performance and consumer protection.
- Provides the potential for a trustmark to be developed at a cross-scheme as well as scheme level.

Regarding the likely catalyst for the collaborative organisation to emerge, there is no immediate legislative or regulatory stimulus on the horizon for digital identity, nor does Government seem minded to act to create a formal authority by regulation or legislation. Given the potentially significant economic benefits of digital identity, and established government policy to bring about a functioning market, a number of conditions are satisfied that suggest that some form of 'bottom-up' industry-led organisation would be the most likely option available to the market.

RECOMMENDATIONS

1. Industry to establish a collaborative organisation for digital identity

A collaborative organisation, the shape and form of which still needs to be agreed, would provide a space for open discussion to take place between industry participants across the public and private sectors. Stakeholders then to agree the mechanisms required to provide a trusted, interoperable cross-sector digital identity ecosystem, including:

- A set of common principles (including user outcomes and user support) to guide the participating organisations' digital identity operations and their interactions with other participating organisations and users.
- The certification, trustmark and/or registry functions that will be needed, and who or how to operate them.

For this to be successful a missing ingredient is the funding such an organisation would require. If a collaborative organisation's responsibilities are limited in number and scope the funding required will be small in comparison to some existing market authorities, but will nevertheless need to be agreed, most likely by participating organisations.

2. Industry and Government to collaborate in the development of digital identity standards

At present UK standards are not sufficiently developed to meet all of the needs of both public and private sectors. However, the existing Good Practice Guides 44 and 45, along with a range of international standards such as ISOs and the work of the Open ID Foundation and others could provide a firm foundation for the further development of digital identity standards. GPG45 in particular provides a method of identifying specific 'Identity Profiles' needed for particular digital identity use cases, with the level of assurance balanced to the level of risk.

The collaborative organisation could, as part of its role, develop standards that meet the needs of a range of use cases across sectors, take a wide view of forthcoming regulation, and ensure interoperability across different standards or approaches.

A collaborative programme facilitated by the organisation involving a range of government and industry stakeholders should further refine and publish the suite of open standards needed to underpin a trusted interoperable ecosystem able to serve a number of sectors and use cases.

3. Competent National Authorities to formally recognise reusable digital identity

It would be a significant development if Competent National Authorities were to formally recognise the use of reusable digital identities for their areas of authority. This would provide additional regulatory clarity, reduce risk for relying parties and users, and thereby generate market demand.

Furthermore, once digital identity standards have been refined and established, and the level of assurance and outcome deemed suitable for specific use cases, it is recommended that the Competent National Authority for each sector or use case formally recognise the standards or identity profiles specific to their area.

REFERENCES

[i] THE CASE FOR DIGITAL IDs
https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf
TechUK (2019)

[ii] DCMS/GDS STATEMENT
https://www.gov.uk/government/news/minister-confirms-government-ambition-on-digital-identity
Cabinet Office Press Release (11 June 2019)

[iii] GOOD PRACTICE GUIDE 44 *Authentication Credentials in Support of HMG Online Services*
https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services
GDS (2014)

[iv] THREE DIMENSIONS OF ORGANIZATIONAL INTEROPERABILITY *Insights from recent studies for improving interoperability frame-works*
https://pdfs.semanticscholar.org/e577/473a84b71fda605b04aa64a65d95d96fd596.pdf
H Kubicek, European Journal of E-Practice (2009)

[v] EUROPEAN INTEROPERABILITY FRAMEWORK
https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf
European Commission (2017)

[vi] TRUSTMARKS REPORT 2013: Can I Trust the Trustmark?
https://ec.europa.eu/info/sites/info/files/trust_mark_report_2013_en.pdf
European Consumer Centres Network (2013)

[vii] TRUST AND CREDIBILITY IN WEB-BASED HEALTH INFORMATION: A Review and Agenda for Future Research
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5495972/
L Sbaffi & J Rowley, Journal of Medical Internet Research (2017)

[viii] TRUSTMARKS IN THE IDENTITY ECOSYSTEM *Definitions, Use, and Governance*
https://www.openidentityexchange.org/wp-content/uploads/2016/11/Trustmarks-paper-FINAL-v2.pdf
G Rosner, Open Identity Exchange (2016)

[ix] DCMS/GDS STATEMENT (June 2019, reference as (ii) above)

[x] OSI 7 LAYER MODEL
https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

[xi] BBFC STATEMENT
https://bbfc.co.uk/about-bbfc/age-verification
(2017)

[xii] LICENCE CONDITIONS AND CODES OF PRACTICE
https://www.gamblingcommission.gov.uk/PDF/LCCP/Licence-conditions-and-codes-of-practice.pdf
Gambling Commission (May 2019)