OIX White Paper

Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK:

Is there a need for certification, trustmarks and an independent authority?

Presented by

Rob Laurence and Ewan Willars

(Innovate Identity Ltd)

Friday 20th September 2019

Project Team - Participating Organisations

GDS

TISA

Barclays

Digidentity

Experian

GB Group

HSBC

Idemia

LexisNexis

Post Office

Yoti

OIX

Innovate Identity

Peer Review Group - Participating Organisations

HM Treasury

DCMS

FCA

JMLSG

ABI

BSA

FLA

OBIE

FDP (Onfido)

Gambling Commission

RGA

Sky Betting and Gaming

IAG (BA)

Timpson

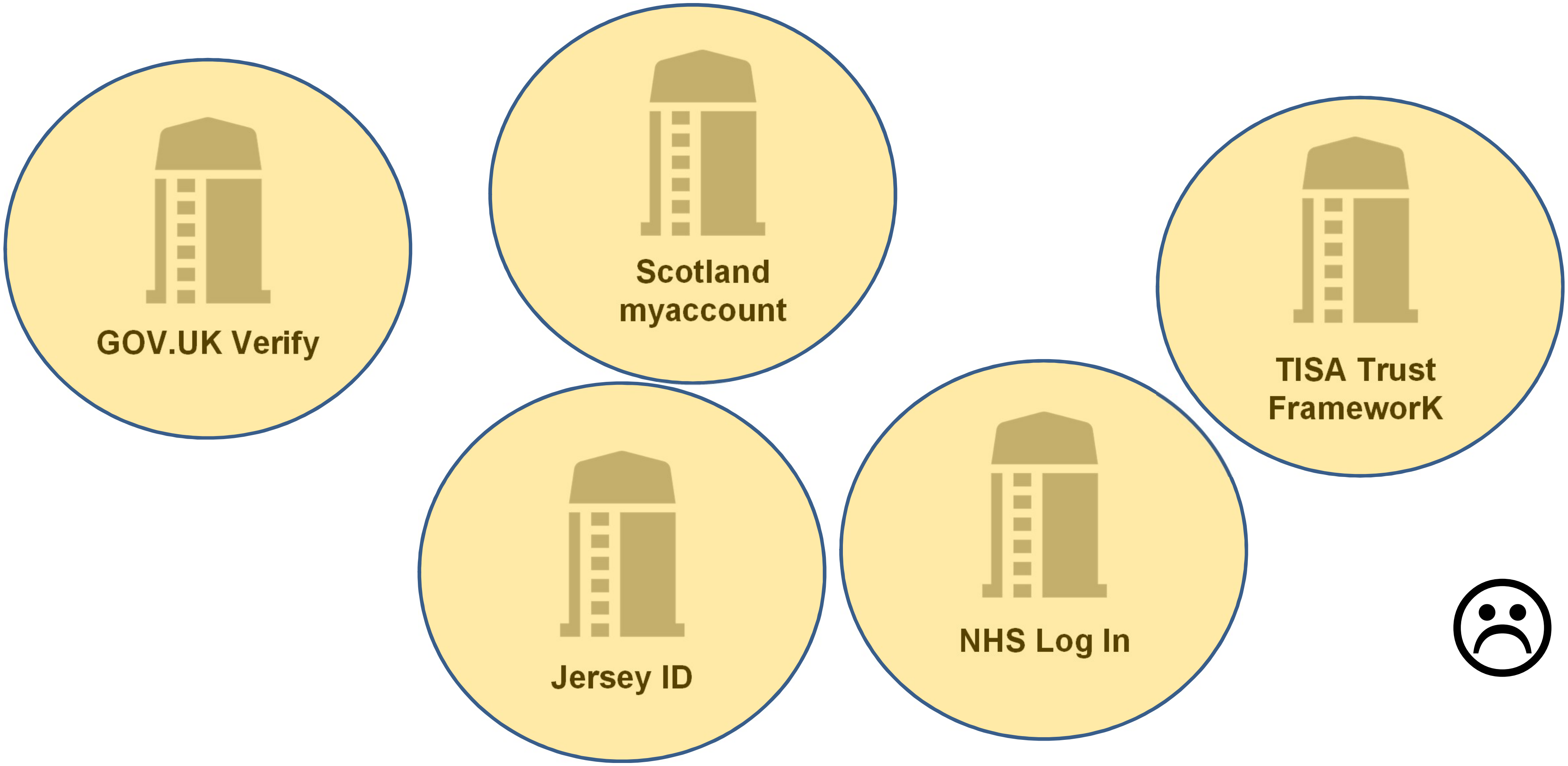
tScheme

OIX

Innovate Identity

ICO (review only)

Digital Identity Schemes – Silo Model



GOV.UK Verify

Scotland myaccount

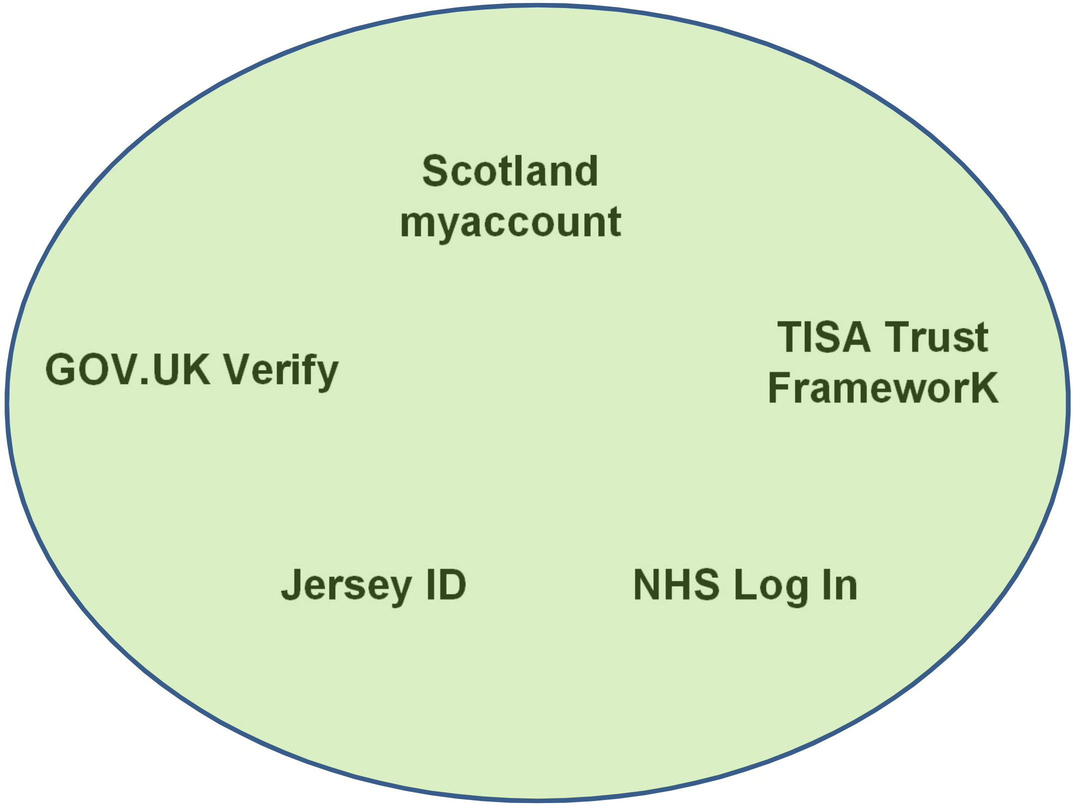
TISA Trust FrameworK

Jersey ID

NHS Log In

☹

Digital Identity Schemes – Trusted Interoperable Ecosystem



Scotland myaccount

GOV.UK Verify

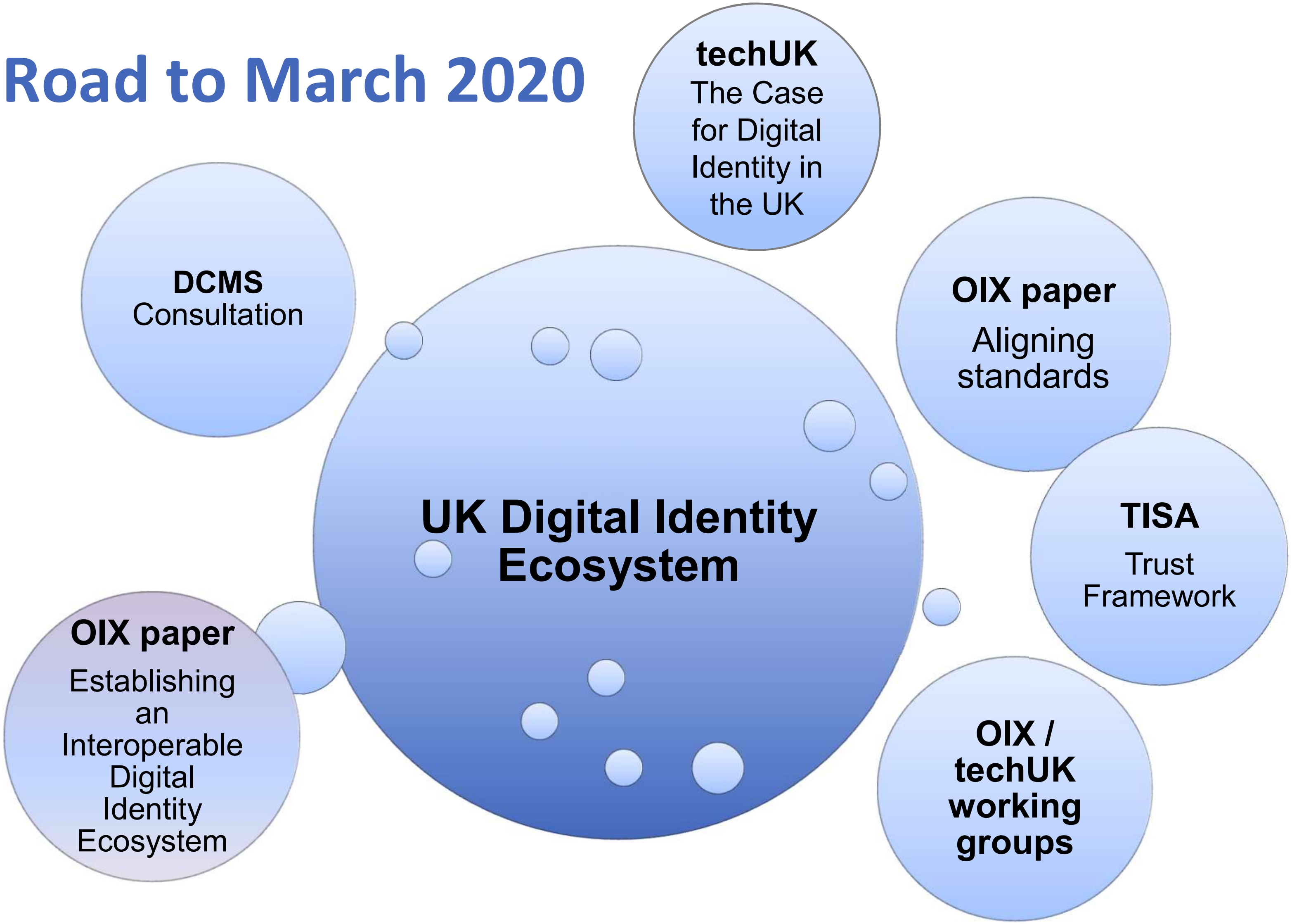
TISA Trust FrameworK

Jersey ID

NHS Log In

☺

The Road to March 2020



UK Digital Identity Ecosystem

techUK
The Case for Digital Identity in the UK

DCMS
Consultation

OIX paper
Aligning standards

TISA
Trust Framework

OIX / techUK working groups

OIX paper
Establishing an Interoperable Digital Identity Ecosystem

Report hypotheses

1. In an emerging market of interoperable digital identity schemes trust will be an important element.

2. That level of trust can only be assured through appropriate certification.

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

Report objectives

1. 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.

2. To determine the key elements of the ecosystem and where these principles need to be applied.

3. To review the mechanisms available to establish and assure trust.

4. To consider and make recommendations on how trustmarks and other mechanisms to communicate trust could be implemented in the UK.

The 7-Layer Digital Identity Ecosystem Model

1	STATE
2	COMPLIANCE
3	ECOSYSTEM
4	CONFORMANCE
5	SCHEME
6	TRANSACTION
7	SUPPORT

The 7-Layer Digital Identity Ecosystem Model

Function	Layer	Description
Governance	1) State Legislation and regulation	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). Provides legal clarity around aspects of the market operation. Legislation and regulation (including industry guidance) that may need to be reviewed and amended to explicitly recognise the acceptability of federated digital identity.
	2) Compliance	Sets out the obligations on market participants to meet the legislative and regulatory requirements.
	3) Ecosystem Principles, policies, procedures and standards	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. 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.
	4) Conformance Incl some compliance	Sets out the obligations on market participants to meet the standards requirements.

The 7-Layer Digital Identity Ecosystem Model

Function	Layer	Description
Operation	5) Scheme / service	The business, legal and technical rules of operation that form a multi-party contractual arrangement, to meet the terms and conditions of the ecosystem and ensure the integrity of the scheme is upheld in line with the governance framework.
	6) Transaction	Ensures that each transaction happens as it should and to the benefit of all parties involved.
	7) Support	Ensures that participants including end users have recourse if problems occur.

Approach Taken

Interoperability and Trust as Concepts

Trust and Interoperability Mechanisms:

- Standards
- Conformance Mechanisms
- Compliance Mechanisms
- Performance Mechanisms
- Mechanisms to Promote and Communicate Trust
- User Support Mechanisms

Trusted Transactions in a Existing Multi-Scheme Ecosystems

- B2B vs B2C Trusted Transactions
- Scheme to scheme?

The need for an Overarching Organisation for the Digital Identity Market

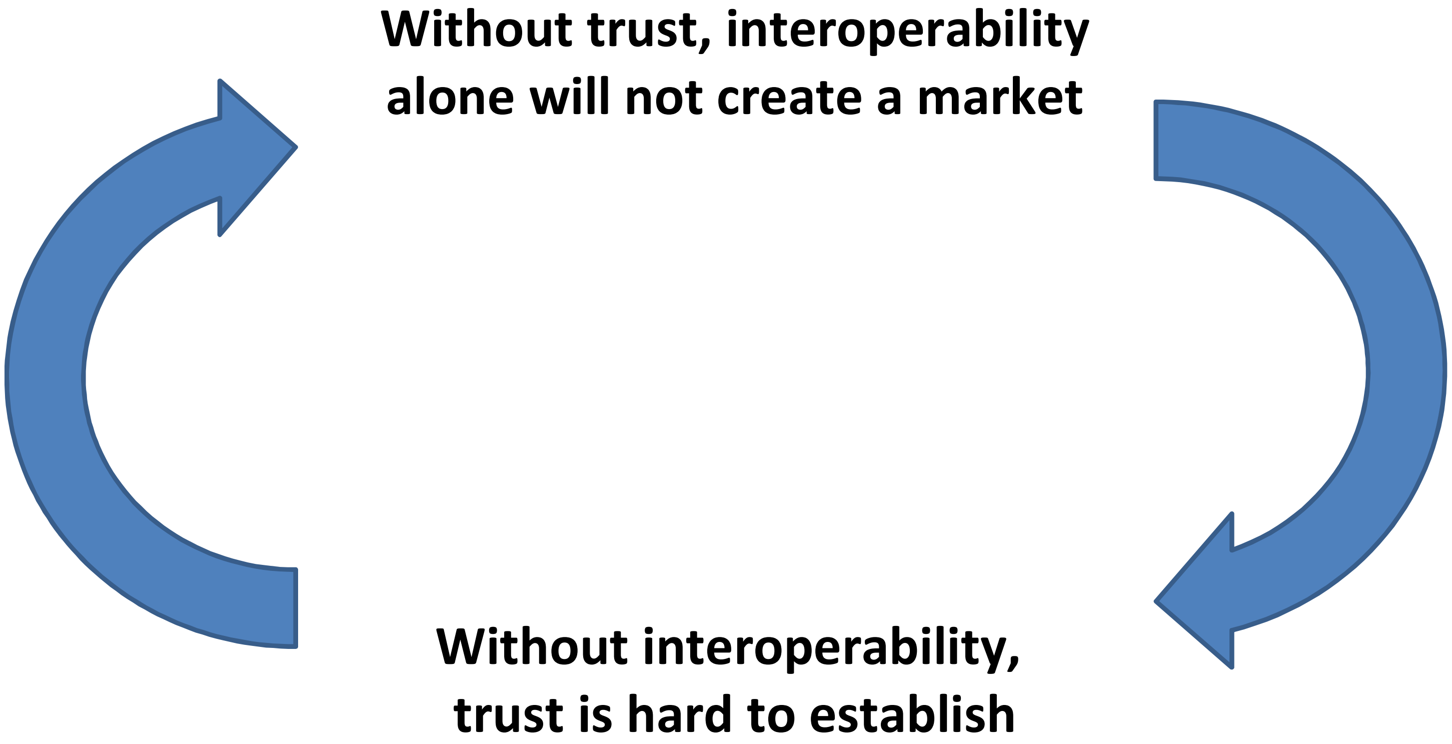
Key concepts - Trust

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 agreed between participating firms • Licensing, 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 services • Codes of Conduct • Trustmarks and registers
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

Key concepts - Interoperability

CONCEPT	DESCRIPTION	MARKET MECHANISMS
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.	• Standards or standardisation • Attestation, certification or accreditation • Assurance of compliance
Semantic Interoperability	Ensuring that the various participants within a market are able to share information with an unambiguous, shared meaning and value.	• Communication protocols • Shared ontology • Schemes • Legal agreements
Organisational Interoperability	Ensuring that objectives and processes are aligned, and relationships clearly defined across multiple organisations participating in a market.	• Industry agreements • Industry associations • Schemes and trust frameworks • SLAs • Change management protocols
User Interoperability	Ensuring that consumers are empowered to participate in the market, have trust in the market actors, and able to achieve at least a minimum level of experience and satisfaction, whichever participating organisation they interact with.	• Signals such as trustmarks and trust registries • Certification, accreditation or assurance • Consumer protection such as guarantees or dispute resolution

Trust and interoperability interact



Without trust, interoperability alone will not create a market

Without interoperability, trust is hard to establish

Trust mechanisms

There are a range of potential mechanisms used to establish, ensure and communicate trust.

TRUST COMPONENT	OPTIONS
Establishing and Recognising Standards	• Standardisation (specification) • Outcome-based standards • Principle-based standards + • Formal recognition (legislative, regulatory) • Informal recognition (industry, scheme)
Compliance	• Self-reporting (voluntary or regulatory) • Data Monitoring (potentially in real time) • Occasional spot checks / issue-based investigation • Regular audits / assessments • Contractual arrangements and legal frameworks
Conformance	• Attestation • Certification • Accreditation • Licencing

Trust mechanisms

TRUST COMPONENT	OPTIONS
Signals: to Recognise and Promote Trust	• B2B and/or B2C • Trustmarks • Registers / Databases • Digital seals and signatures
User Protection	• Charters • Performance – SLAs, targets, penalties • Dispute resolution ○ Complaints handling ○ Arbitration / mediation ○ Compensation ○ Ombudsman • Liability • Legal agreements

How will trust be developed and by who?

MARKET ACTORS AND POTENTIAL ROLES

LAYER	LIKELY FUNCTIONS
Government • DCMS • GDS • NHS	• Legislative framework • National policy • National standards
Regulator • FCA • PSR	• Regulatory guidance • Performance requirements • Orderly market
Industry Organisation • Lending Standards Board • Pay.UK • OBIE	• Governance • Technical or Sectoral standards • Trustmarks / Signals • Principles and Customer Outcomes
Scheme • Gov.UK Verify • NHS Digital • TISA? • YOTI?	• Contractual framework • Commercial framework • Liability • Technical or Operational standards • Trust / Signals
Organisation • IDPs • RPs	• Consumer contracts • Service provision • Value exchange

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 (Findings 5 and 6 are relevant here).

Key findings (cont)

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 a greater focus on conformance by the overarching authority, given the strength of existing oversight and compliance mechanisms that were established with the regulation and are operated elsewhere.

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 B2B trust.

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.

Report recommendations

1. Industry to establish a collaborative organisation for digital identity

A collaborative organisation, which shape and form still needs to be agreed, would provide a space for collaboration and discussion to take place between industry participants across the public and private sectors. Stakeholders 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.

Report recommendations

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

An open, collaborative overarching 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.

Report recommendations

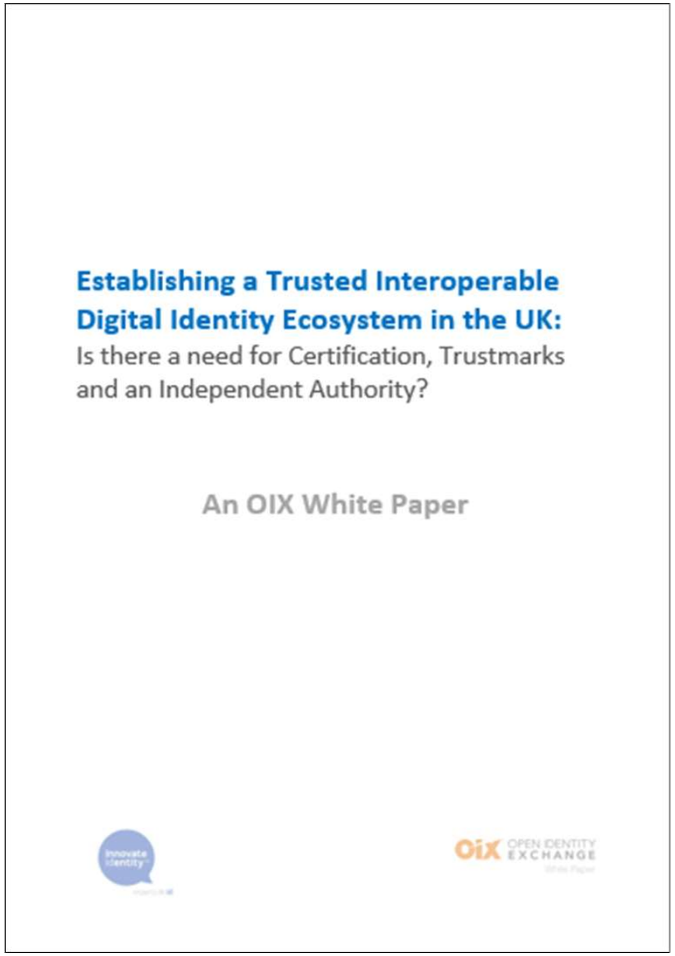
3. Competent National Authorities to formally recognise digital identity standards

Once digital identity standards have been established, and the level of assurance and outcome deemed suitable for specific use cases and calibrated to the level of risk associated with each one, it is recommended that the Competent National Authority for each sector or use case formally recognises the standards specific to their area. This would provide regulatory clarity, reduce risk for relying parties and users, and thereby generate market demand.

innovate identity™
experts in id

OIX United Kingdom

Available from
27th September



Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK:
Is there a need for Certification, Trustmarks and an Independent Authority?

An OIX White Paper

Thank you