# Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK:

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

## 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<br>• Outcome-based standards<br>• Principle-based standards |
| **COMPLIANCE** | • Self-reporting<br>• Occasional spot checks / issue-based investigation<br>• Data monitoring<br>• Regular audits |
| **CONFORMANCE** | • Attestation<br>• Certification<br>• *Accreditation* |
| **PERFORMANCE** | • Legally binding service level agreements<br>• Key performance indicators<br>• Fraud prevention measures<br>• Participant guidelines and customer charters |
| **RECOGNISING AND PROMOTING TRUST** | • Trustmarks<br>• Online registers and databases<br>• Digital seals and signatures |
| **SUPPORT** | • Customer charters<br>• Security and privacy assurance<br>• Dispute resolution mechanisms<br>• 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.<br>• Sets out the overarching legal environment that the ecosystem will operate within. |
| **2 COMPLIANCE** | • Provides legal and regulatory assurance.<br>• Reduces regulatory risk. |
| **3 ECOSYSTEM** (INCLUDING STANDARDS, POLICIES AND GUIDANCE) | • Provides a basis for trust.<br>• Provides interoperability and operational clarity. |
| **4 CONFORMANCE** (INCLUDING SOME COMPLIANCE FUNCTIONS) | • Provides assurance to participants.<br>• Provides interoperability and operational assurance. |
| **5 SCHEME** (INCLUDING SERVICES) | • Accreditation/certification, registration, trustmarks (B2B).<br>• Common platform and service definition. |
| **6 TRANSACTION** | • Trustmark (B2C) - assures performance and level of experience with the user.<br>• Ensures an efficient transaction. |
| **7 SUPPORT** | • Manages risk and provides reassurance.<br>• Ensures clarity concerning liability in the case of a compliance, conformance or transactional error.<br>• 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.