OPEN IDENTITY EXCHANGE
White Paper

A Blueprint for National and International Oversight of the Digital Identity Market

Written by Rob Laurence and Ewan Willars
Innovate Identity Ltd

March 2020

PROJECT PARTICIPANTS

Open Identity Exchange (OIX) is a not-for-profit, technology agnostic, collaborative cross sector membership organisation with the purpose of accelerating the adoption of digital identity services based on open standards. OIX's broad membership and independent nature have seen it develop a significant body of digital identity research, and it is a significant influencer working towards the development of a digital identity market.

OIX has established a Peer Review Group comprising regulators and trade associations, across a range of sectors, who have an interest in the development of a digital identity ecosystem and have helped to shape thinking as to how it might be established.

We are grateful for the contributions of the following organisations who contributed to this white paper.

For national oversight:

- Barclays Bank
- Betting and Gaming Council
- Finance and Leasing Association
- Gambling Commission
- Gemserv
- Mobile Ecosystem Forum
- Open Banking Implementation Entity
- OpenID Foundation
- techUK
- The Investment and Savings Alliance

For international oversight:

- Department of Internal Affairs, New Zealand Government
- Digital ID & Authentication Council of Canada
- Digital Transformation Agency, Australia
- DG Connect, European Union

Contents

Executive Summary

In almost every conceivable market, there is an authority or oversight organisation that is responsible for ensuring order and fairness across the market participants. The need is driven by factors such as building confidence and trust in the marketplace, protecting participants and, in many cases, ensuring technical interoperability. The emerging digital identity market in the UK has exactly these needs. An oversight organisation is essential.

In this paper, we explore how an oversight organisation might look. We invited a Peer Review Group, comprising regulators and trade associations, to discuss a series of questions framing the role of such an organisation, its responsibilities, the functions and services that should be provided, as well as its structure, governance, resourcing, costs and funding. The result of this work is a "blueprint" for a national oversight organisation for digital identity.

The Blueprint

1. **The oversight organisation should be formed as a collaboration between the private sector and Government.**
2. **Funding, in the first instance, should come from the private sector members together with a significant contribution from Government, recognising the importance of a national digital identity ecosystem across the private and public sectors.**
3. **The oversight organisation should operate and govern an overarching trust framework that recognises market-specific conditions and requirements.**
4. **The oversight organisation should establish an identity assurance advisory panel, its purpose being to recognise guidance in the areas of identity proofing and verification, identity authentication and attributes. This guidance should extend into the area of equivalencies between different issuers of standards and guidance.**
5. **The oversight organisation should establish a technical standards advisory panel, its purpose being to investigate and recognise open standards for use within the ecosystem, and to influence the development of existing and new standards in areas such as attributes.**
6. **The oversight organisation should establish other advisory panels, as required, to address areas such as fraud and security.**
7. **The oversight organisation should provide the minimum functions and services at the outset, operating as a "thin layer".**
8. **Where possible, the oversight authority should consider outsourcing services to benefit from the experiences and competencies of existing oversight organisations, thereby reducing risk including cost escalation.**
9. **The oversight organisation should minimise costly certification requirements at a national level, with the emphasis on providing guidance, and for schemes to ensure compliance and conformance through audit and contractual arrangements.**

Digital identity ecosystems exist or are being planned in most countries around the world. In many instances, these are being introduced as an extension to national identity cards and databases. However, in countries where no such national identity scheme exists, introducing a digital identity ecosystem has fundamental challenges to overcome: that of acceptability,

scalability and viability. The UK is one such country, as is Australia, Canada, New Zealand, the USA and others. As each country addresses its own challenges, many of which are common, we need to consider these in a wider context – that of portability and interoperability across national borders. The shared vision for digital identity is that it is, just like the Internet, not restricted by borders. A person with a digital identity issued by a scheme in one country should be able to use it with organisations in another country, be that to visit, reside or transact.

In this paper, we also discuss with organisations responsible for digital identity in Australia, Canada, New Zealand and the European Union, the need for a global interoperable model and the type of organisation that would be needed to oversee it.

The result of these discussions is a blueprint for an international oversight model.

The Blueprint

1. **Developments should be driven by governments and private sector in partnership.**
2. **Start with agreeing common principles.**
3. **Undertake bi-lateral and multi-lateral interoperability assessments initially.**
4. **Develop a common framework of outcome-based rules, based on peer-to-peer recognition and recognised standards – retain national flexibility to deliver.**
5. **Act in proportion to the level of systemic importance and risk associated with digital identity.**
6. **Work towards a focused, co-operative organisation to assess and certify cross-border interoperability.**

The primary focus, at least in the short to medium term, must be to establish the UK ecosystem and the market oversight organisation. Much work is required to develop an appropriate model and OIX is playing a leading role in this.

The Peer Review Group also commented that an oversight organisation "needs a market to oversee". Although various initiatives are underway, there is no strategy for digital identity that brings all market sectors and stakeholders together. Government action is needed to drive this forward.

Introduction

The report entitled *An Independent Authority for the UK Digital Identity Ecosystem*, commissioned by the OIX Board and written by Innovate Identity, sets out the rationale for the type of oversight organisation for the UK digital identity market, considering

- Market needs for an overseeing organisation – from state to society
- Type of market regulation – from statutory to self-regulation, or no regulation
- Extent of market regulation
- Role of an oversight organisation

Seven market oversight organisations were reviewed, considering such factors as reasons for formation, legal status and powers, governance, functions and services provided, recognition, ownership, resources and funding.

Market characteristics were identified including

- Extent of regulation and regulatory powers
- Financial risk in market
- Need for technical interoperability and semantic interoperability (naming and addressing standards; eg domain naming conventions)
- Level of functions and support services provided

The broad conclusions drawn were that an oversight organisation for digital identity could have the following characteristics

- Exist in a market that is self-regulated but surrounded by significant regulation in target markets such as financial services, payments and gambling
- Be a not-for-profit, funded by its members and by chargeable services
- Would oversee a market with a high dependency on technical interoperability
- Would need to provide a broad range of functions and support services

To help to better understand, envision and communicate the purpose, role, responsibilities, constraints and funding of an oversight organisation for digital identity, the report recommended the drafting of a "blueprint" for the organisation that covers all aspects of its function and funding.

Recently, the UK Government Digital Service (GDS) has presented an overview of a trust framework for the UK's digital identity ecosystem, with governance of the trust framework falling within the "umbrella" of the UK Government's Digital Identity Unit (DIU). At this stage, it is not clear whether this is intended or not, and what role (if any) the Government envisages for the DIU with respect to being an oversight authority or stakeholder in such an authority.

So, a number of scenarios for the market oversight authority seem possible.

1. The Government could appoint an independent authority to oversee the market.
2. The DIU could take the role of a market authority whilst a market is being established and potentially transition this to the private sector at a future date (such as intended by the Australian Government).
3. The private sector could collaborate at the outset with Government to form an authority based on a public/private sector membership model.

In this paper, we discuss how an oversight organisation might look, considering its role, responsibilities, functions and services, organisation structure, governance model, resource requirements, costs and funding model.

In countries that are developing digital identity ecosystems that are not based on national identity schemes or existing bank-led schemes, notably Australia and Canada, progress is being made to establish trust frameworks at a national level. These are based on a robust approach to the privacy, safety and security of citizens, federated identity models, Open Technical Standards, and a mix of self-certification and independent-certification processes.

Digital identity is an enabler of digital inclusion and digital transformation. It provides the missing identity layer on the Internet, and for open data initiatives such as Open Banking. Digital identities have to be trusted not only at a national level but globally in much the same way as a passport or a www top level domain is today. This leads to a conclusion that there will need to be a global organisation to orchestrate and oversee the governance and interoperability of nationally recognised trust frameworks and digital identity schemes across state borders.

In this paper, we also review the work being undertaken on trust frameworks in jurisdictions including Australia, Canada, New Zealand and EU (through eIDAS), and discuss a high-level model for such a global oversight organisation, taking into consideration other models, organisations and consortiums such as ICANN and W3C, and UN Specialized Agencies such as ICAO (aviation) and ITU (telecoms).

Approach

The 7 UK market oversight organisations reviewed for the report *An Independent Authority for the UK Digital Identity Ecosystem* were as follows:

Current Account Switching Service (CASS/BACS)
Lending Standards Board (LSB)
MRA Service Company (MRASCo)
Nominet
Open Banking Implementation Entity (OBIE)
Pay.UK
Steering Committee on Reciprocity (SCOR)

The characteristics of each marketplace were considered in terms of legislation, type of regulation, financial risk, degree of interoperability and trust, and support required. The characteristics of each oversight organisation were considered including their mandate for existence, history, ownership, governance, functions and services provided, supporting infrastructure and funding.

Findings from the review and subsequent research have led to the drafting of a model for an oversight authority for the UK digital identity market.

The model was presented to the Peer Review Group for discussion and a series of questions were posed to test views and solicit opinions on the scope, role and responsibilities, resources and funding of such an oversight authority. These are presented in the following section.

The investigation into the requirements for global oversight of digital identity was carried out in two parts.

The first involved research and interviews with organisations developing national-level trust frameworks in Australia, Canada, New Zealand and EU (eIDAS). The second considered other models for global oversight.

Findings from these have led to exploration of the various options for global oversight for digital identity.

Blueprint for a National Oversight Authority

In the OIX 7-Layer Digital Identity Ecosystem Model, the role of an oversight authority is seen to encompass layers 1 to 4 – the Governance of the Ecosystem.

Function	Layer	Description
Governance	**Layer 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.
	Layer 2 **Compliance**	Sets out the obligations on market participants to meet the legislative and regulatory requirements.
	Layer 3 **Trust framework** **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.
	Layer 4 **Conformance / compliance**	Sets out the obligations on market participants to meet the standards requirements.
Operation	**Layer 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 trust framework and ensure the integrity of the scheme is upheld.
	Layer 6 **Transaction**	Ensures that each transaction happens as it should and to the benefit of all parties involved.
	Layer 7 **Support**	Ensures that participants including end users have recourse if problems occur.

Trust Frameworks and Schemes

The relationship between an oversight authority and a trust framework needs to be explored. In Australia, the Digital Transformation Agency, appointed by government as the oversight authority, is developing the Trusted Digital Identity Framework. In Canada, the collaborative Digital Identity and Authentication Council of Canada (DIACC) has set out the Pan-Canadian Trust Framework. Both of these examples suggest a national-level trust framework. What is not clear, though, is whether it is envisaged that there will be a single identity scheme or multiple schemes that adhere to the framework.

OIX defines a trust framework as a legally enforceable set of specifications, rules, and agreements that governs an identity system. This rather suggests that the "owner" of the trust framework is, or appoints, some sort of authority that brings the participants in the identity system or identity scheme together or, at the very least, has a measure of oversight over one or more scheme "owners" that comply and are perhaps certified within the trust framework.

Note that there is some disparity in the use of terminology within the identity industry. Developing a common lexicon and creating semantic interoperability would also be an important part of forming a functioning ecosystem.

Question 1

Is the trust framework the overarching governance and legal framework for the UK's national digital identity ecosystem or is it effectively the scheme rules?

If the latter, what are these scheme rules based on and what terminology should be applied?

Peer Review Group

It was agreed that there is confusion arising from the range of definitions applied to what a 'trust framework' is – the 'traditional' holistic definition includes legal, commercial and technical aspects. However, in a world where multiple schemes may operate within a single trust framework, it may be necessary to define and perhaps separate the different meanings.

There was general agreement that in the context of this paper, the trust framework should not be considered to include aspects of a commercial nature.

The trust framework in this sense was agreed to be the higher-level rules and framework needed to enable interoperability between schemes.

It was also agreed that the high-level trust framework should be a thin layer – avoid overpopulating it but provide sufficient information to enable interoperability and cross-scheme trust to be established. For example, recognition of standards (but not their development), to set out common principles, and to set out the requirements of a conformance framework (probably in the form of a certification programme) but not necessarily to operate the certification process itself. This layer may be outcome-focused or principle-based.

It may be that each sector needs to add another level to the framework specific to that sector. For example, this may include information concerning acceptance information (i.e. the level of identity assurance required to access services within that sector).

Technical interoperability driven by common standards (e.g. common data transfer methods) may be an issue best addressed by participants at scheme level, leveraging global standards templates such as OIDC, SAML and W3C Verifiable Credentials as appropriate.

Within an identity scheme, it is envisaged participants will include end users, identity providers, attribute providers, relying parties and scheme owners (possibly identity brokers). The scheme owner or identity broker would be the contracting entity for all but the end users.

Question 2

Is this model and terminology for an identity scheme accepted and are there alternative models that need to be accommodated?

Peer Review Group

Other models do exist that may not easily sit within the definition of a scheme as identified in the discussion document – e.g. proprietary identity services such as that provided by YOTI. Similarly, point-to-point transactional models (IDP-to-RP direct) or self-sovereign solutions also sit outside of that definition.

The definition of scheme and its participant types, as identified in the discussion paper, was agreed to be accurate – comprising of a commercial and legal agreement between participants, involving a scheme owner or 'broker'.

Purpose

The purpose of an oversight authority is to provide leadership and ensure the integrity of the market comprising multiple, interoperable schemes, through appropriate measures. (To be the "go-to" organisation on all subject matters).

Question 3

Is this description of purpose accepted and how should the relationship be conducted with other authorities who have an interest in digital identity? For example, authorities who provide guidance or regulate the Money Laundering Regulations.

Peer Review Group

The purpose was discussed as being:

- To accelerate the market (to create scale)
- To establish trust and confidence in the market and between its participants
- To remove 'blockers' to the development and success of the market

Relationships with other bodies. This was felt to be a challenging concept to establish at this time. Representation by sectoral or industry representative bodies on the national authority in some form was a possible solution.

Question 4

In the 7-Layer model, appropriate measures include principles, policies, procedures and standards, backed up by conformance and compliance obligations. How should these be established and who should be involved?

Peer Review Group

The need for independent audits to be carried out (versus self-asserted compliance, at least for more risky transaction types) was considered a factor that should be set out national framework (authority) level.

Compliance actions and specific audit requirements should lie at scheme level.

A balance will be needed – strong compliance and audit requirements can help to build confidence; however, this can become very costly for participants, and therefore may need to be proportionate to risk.

Liability arrangements should be set at scheme level and schemes should assign liability to each actor in the scheme for the action they undertake, clarifying which actor is responsible for what, and what liability is retained by each.

This will not prevent unforeseen liability issues, but the principle is correct. Schemes should also highlight what 'good actions' look like.

The authority should seek to mitigate liability via the rules of the framework. It may also need to be the arbiter in liability cases (this function could also fall to the scheme rather than the authority) and receive representations concerning compliance in cases where liability is not clear-cut.

Role and Responsibilities

The key high-level role and responsibilities of the oversight authority are considered to be as follows:

1. To provide clarity of vision and strategic direction
2. To set out the policies, rules, guidance and standards to meet the vision
3. To facilitate the engagement of stakeholder groups through representation and consultation
4. To ensure adequate funding and oversee financial performance of the authority
5. To provide all reasonable endeavours to ensure the success of the digital identity ecosystem

Question 5

Do you agree with the responsibilities set out and are there any additions to these?

Peer Review Group

In point 5, avoid the use of 'reasonable endeavours' in the list provided in the discussion document and replace with "To supply appropriate mechanisms and remove blockers to enable a successful market outcome and function."

It was suggested that the bullets be condensed to their core meaning:

- Vision
- Standards
- Engagement
- Competence
- Success
- + Compliance (and liability) – these are not explicitly included in the list at present

It was discussed that an authority's role may include responsibility to ensure conformance with technical standards, and compliance with legal and regulatory requirements and rules by ecosystem participants.

It would be worthwhile considering also the need for rule books to be developed in line with specific (particularly regulated) use cases or by sector.

The Trust Framework

The following table sets out the scope of the trust framework and the areas where rules, guidance and standards will need to be developed or recognised to meet the requirements of an interoperable digital identity ecosystem.

This will drive the functions and services that need to be provided by the authority, and the organisation structure, resource requirements and funding necessary to deliver this.

Table 1. Rules, guidance and standards

Subject	Participant Impact				
	User	Identity Provider	Attribute Provider	Relying Party	Broker
General					
Governance of trust framework	Direct	Direct	Direct	Direct	Direct
Roles and Responsibilities of participants	Indirect	Direct	Direct	Direct	Direct
Risk management	Indirect	Direct	Direct	Direct	Direct
National laws and legal arrangements including liabilities and dispute resolution	Indirect	Direct	Direct	Direct	Direct
Commercial arrangements including fees and compensation	Indirect	Direct	Direct	Direct	Direct
Inclusion and equality – economic, social and ableness	Direct	Direct	Direct	Direct	None
Glossary	Indirect	Indirect	Indirect	Indirect	Indirect
Design					
Identity proofing and verification	Direct	Direct	Indirect	Indirect	None
User authentication and credential management – see note 1	Direct	Direct	Indirect	Indirect	None
Attribute provision and sharing	Indirect	Indirect	Direct	Indirect	None
User consent	Direct	Direct	Direct	Indirect	None
User proxies and Power of Attorney	Direct	Direct	Indirect	Indirect	None
User experience	Direct	Direct	Direct	Direct	None
Service operation	Indirect	Direct	Direct	Direct	Direct

Privacy	Direct	Direct	Direct	Direct	None
Security	Indirect	Direct	Direct	Direct	Direct
Lifecycle					
Joining the trust framework	None	Direct	Direct	Direct	Direct
Testing	None	Direct	Direct	Direct	Direct
Certification – see note 2	None	Direct	Direct	Direct	Direct
Branding and marketing	Indirect	Direct	Direct	Direct	Direct
Operation – see below					
Exiting the trust framework	Indirect	Direct	Direct	Direct	Direct
Operation					
Threat detection and counter fraud	None	Direct	Direct	Direct	Direct
Transaction monitoring and unusual activity	None	Direct	Direct	Direct	Direct
Incident response					
Audit trails and record keeping	None	Direct	Direct	Direct	Direct
Billing and auditing	None	Direct	Direct	Direct	Direct
Recognised Technical Standards and Specifications (see note 3)					
Approval and adoption	None	Direct	Direct	Direct	Direct
Registry	Indirect	Indirect	Indirect	Indirect	Indirect

Notes

1. This needs to include use of biometrics.
2. A separate set of requirements and guidance will need to be developed for auditors' responsibilities within the certification process.
3. Open standards will need to be formally recognised to ensure interoperability across participants. Recommendation from OIX/techUK Interoperability and Standards Working Group is for an Independent Standards Board/Panel to be formed to accept nominations for standards and manage the approval and adoption process.

Question 6

Do you have any views on the subject areas and whether there are areas that are missing and should be included or should be removed?

Peer Review Group

Comments included under response to question 7.

Functions and Services Provided by a National Authority

The table below sets out the principle functions and services that the authority could be expected to deliver.

Table 2. Functions and Services Provided by a National Authority

Area	Comments
Vision and Leadership	
Provide clear vision and strategic direction	In conjunction with Government, regulators and industry.
Industry engagement	Through direct consultation and the facilitation of stakeholder panels.
Funding and resourcing	To consider membership fees, grant funding, and/or revenue for services provided.
Market Design	
Guidance – policies, best practice, principles etc	Yes
Standards, rules and procedures	Yes, including the recognition of open technical standards that have been developed to support the delivery of identity services.
Specifications	Potentially
Certification requirements	Yes
Compliance / conformance tools	Could be third-party but would need recognition
Certification services	Could be third-party but would need recognition
Logos / trustmarks	Yes
Market Operation	
Ongoing monitoring and inspection	Yes, could be via third-parties
Dispute resolution	Potentially
Support / helplines / newsletters / training	Yes
Registry	Yes
External Affairs	
Engagement with UK Government and regulators	Yes
Collaboration and participation with international authorities and organisations	Yes
Promotion and publicity	Yes

Question 7

What are you views on the subject areas and are there areas that are missing and should be included or should be removed?

Peer Review Group

The authority should not be a standards development organisation. This needs to be made clear.

The authority should include within its role the recognition of standards (and possibly collating these, and guiding participants through the range of standards it recognises).

This could include the creation of an independent standards board that guides the authority and what to recognise, although there was some challenge to this model (should the standards recognition body be part of the authority, perhaps via a standing advisory board?)

Participants questioned what type of standards would fall into its remit. For example, security standards? Data transfer (e.g. Open APIs)? Assurance? Performance standards?

Performance standards could be set out at authority level (e.g. minimum performance) with detailed service level agreements being set within the scheme.

Greater clarity is required on how types of standards may differ and how the authority's role and responsibilities would vary in each case.

Model form policies and contracts may be another potential role for the authority to consider, alongside how organisations like OIX might help provide such documents.

Providing proforma documents would help accelerate the market and assist new participants.

Organisation Structure and Resource Requirements

On the assumption that an oversight organisation is **not** set up and regulated by the Government, but is formed jointly between the private sector and Government, it is likely to be

- a private-sector not-for-profit company limited by guarantee
- that has Articles of Association agreed by its founding members
- and is initially funded by its members who wish to be part of the ecosystem

Members could be organisations who shape or benefit from the ecosystem such as

- identity providers
- identity service providers
- identity scheme owners/brokers
- relying parties

In Australia, the Government has empowered the Digital Transformation Agency to be the oversight authority to establish the digital identity market for public and private sector services. In Canada, the Federal and State Governments and private sector are collaborating to create an interoperable digital identity market.

Question 8

Are there alternative collaborative organisation structures that should be considered?

Peer Review Group

In addition to the Limited Company and Government-led potential organisational models, participants also raised two alternatives:

- A looser forum of stakeholder organisations, potentially with some government funding

- An outsourced model, where a proportion of the authority's roles and responsibilities are handled by a third party – the authority itself could be a 'shell' company in such an example.

Question 9

What are your views on a similar approach to that in Australia and what would be the pros and cons of such an approach?

Peer Review Group

The Australian model is for government to establish the authority and its role, and for this to be transitioned across to the private sector at a later date (unlike the Canadian model, for example, where the authority (DIACC) was established at the outset by a collaboration between government and private sector bodies.

It is believed that the Canadian model has funding challenges – the Australian model has avoided this, at least at the outset, via public funding.

In the UK, the Government has previously stated that there is limited appetite to continue to subsidise the funding of digital identity, as has been the case with the Verify scheme.

The overriding view was that the model should be based on a collaboration between government and the private sector. (Funding of this model is addressed in question 12).

Not-for-profit Company Board, Executive and Governance

The Articles of Association would set out the construct of the Board of Directors, executive committees and other representation such as advisory panels representing, for example, consumer groups and relying parties.

The Board could comprise

- elected Directors from member organisations (potentially by category)
- appointed CEO and Executive Directors
- appointed Chair and non-Executive Directors

The Nominet model has 12 directors, 4 from each category. In regulated organisations, there are differing models, from a small to high-number of independent non-Execs and similarly with non-Execs representing the regulated businesses, with generally few Executive Directors.

The Executive Management Team would cover functional areas such as:

- Policy and Legal
- Standards and Compliance
- Services and Operations
- External Affairs

Initially, these might be headed by the Executive Directors but could soon be expected to have "Heads of" in each of these areas and potentially a team below.

For the purposes of good corporate governance (although not a legal requirement) and best practice, Board Committees may be formed to address matters such as

- Audit and Governance
- Nominations
- Remuneration

Question 10

What are your views on a not-for-profit organisation structure, particularly at the outset and during its early years when the key challenge will be to establish the market for digital identity, and who should the organisation be accountable to?

Peer Review Group

Participants agreed that not-for-profit is not the only choice – authorities can be profit making and use their profits to fund ecosystem development or support activities, or even philanthropic activities. For example, Gemserv is profit making, based on an outsourced model.

Another alternative is to separate the organisation into profit making and not-for-profit arms – GSMA have set up such a separation. Many charities also have a similar dual set-up.

Optically it may be preferable (and more realistic) to focus on a not-for-profit status and aim for financial independence at first.

Many oversight organisations, particularly those independent of Government, have one or more advisory panels.

For digital identity, advisory panels (often organised by stakeholder type, thematic subject matter or task-based) could represent stakeholder groups as follows

- Consumers/users
- Service providers (relying parties)
- Identity providers and attribute providers
- Scheme owners
- Standards bodies
- Regulators and organisations providing industry guidance

Question 11

What are your views on advisory panels and representation?

Peer Review Group

A wide representation is important to engage with all stakeholders and interested parties; however, this needs to be balanced with pace and agility. The more parties involved the slower progress is likely to be. This is particularly relevant in the formative period.

Funding

Members could pay

- an annual subscription
- a registration and licence fee (including certification)

The costs of membership could be

- tiered to reflect the size of the organisation
- tiered to reflect the benefits gained
- a flat fee
- subject to an organisation's role in the ecosystem

Additional funding could be generated through providing training or professional accreditation, and organising relevant conferences and events.

Budget and Headcount

From research undertaken, the Lending Standards Board has 14 full-time employees (FTEs) and a budget of £2m. MRASCo between 40 and 50 (outsourced to Gemserv). Nominet has approximately 200, as it has developed its specialisms and services in adjacent fields. CASS has a central budget of £10m.

For the purposes of establishing a budget and headcount for a digital identity overseeing organisation, LSB would appear to be the nearest guide augmented by a degree of technical infrastructure to support a live registry.

Allowing for ramp-up in year 1, this would suggest a headcount of 10 to 15 in year 2, with a budget of between £1.5m and £2.5m. A more detailed business and financial plan could be prepared once requirements are better understood. Certification costs would be in addition to this and borne by those companies entering the market.

Question 12

What are your views on the funding model, budget and headcount?

Peer Review Group

Participants suggested that some form of Government funding, at least in the early stages, should be sought and would be positive (given the potential importance of digital identity to the future UK economy, and the interest in developing the ecosystem in the right way).

Experience from other UK and international authorities suggest that revenue from activities, such as certification, training, accreditation and conferences could form a significant part of the organisation's funding, but this is usually more prevalent for mature, steady-state organisations. This may not be possible at the outset.

Similarly, member fees (usually tiered, by organisation type, size or potential benefit) commonly form a significant revenue stream for the authority, however this is difficult to ensure in the early stages of its development and operation.

To make the case for government funding in the early stages, and to ensure funding requirements are kept to a minimum, it may be worthwhile assessing what the minimum required roles and actions of an authority might be – the minimum viable organisation.

The Blueprint for a National Oversight Organisation for Digital Identity

There is a consensus around the need for an oversight organisation and that this organisation, in common with most organisations in non-government-regulated markets, needs to reflect the envisaged adopters and users of digital identity schemes, this being both the private and public sectors.

This make-up points towards the formation of a member organisation, this typically being a not-for-profit limited company.

The Blueprint

1. **The oversight organisation should be formed as a collaboration between the private sector and Government.**
2. **Funding, in the first instance, should come from the private sector members together with a significant contribution from Government, recognising the importance of a national digital identity ecosystem across the private and public sectors.**
3. **The oversight organisation should operate and govern an overarching trust framework that recognises market-specific conditions and requirements.**
4. **The oversight organisation should establish an identity assurance advisory panel, its purpose being to recognise guidance in the areas of identity proofing and verification, identity authentication and attributes. This guidance should extend into the area of equivalencies between different issuers of standards and guidance.**
5. **The oversight organisation should establish a technical standards advisory panel, its purpose being to investigate and recognise open standards for use within the ecosystem, and to influence the development of existing and new standards in areas such as attributes.**
6. **The oversight organisation should establish other advisory panels, as required, to address areas such as fraud and security.**
7. **The oversight organisation should provide the minimum functions and services at the outset, operating as a "thin layer".**
8. **Where possible, the oversight authority should consider outsourcing services to benefit from the experiences and competencies of existing oversight organisations, thereby reducing risk including cost escalation.**
9. **The oversight organisation should minimise costly certification requirements at a national level, with the emphasis on providing guidance, and for schemes to ensure compliance and conformance through audit and contractual arrangements.**

Blueprint for an International Oversight Organisation

Examining the need for a national authority for digital identity in the UK can also shine a light on the need for a similar function working across national boundaries, specifically to aid interoperability between different national frameworks and schemes.

The ability to access a service offered by an organisation operating within the trust framework in country B, using an identity created by the user and identity provider operating within a trust framework in country A, could be an incredibly valuable proposition in an increasingly mobile and connected global economy.

While the international ecosystem is not the same as those at national level and less well formed, many of the same issues and questions apply. Are schemes and frameworks interoperable? Can participants trust identities created elsewhere? And what type of organisation would be able to underpin interoperability and trust?

The Need for International Interoperability

The report hypothesis is that interoperability *is* needed between national digital identity frameworks and the schemes that operate within them. But is this true? What drives the need for interoperability and therefore some form of international organisation?

The world is more connected and mobile across national borders than ever before. An increasing number of people choose to visit other countries, do business across national boundaries, and live and work in countries that are not their place of birth. In each of these cases, whether to gain access to the country via border control, hire a car, work, access health services or make a cross-border investment, an individual must be able to assert their identity in a way the recipient can trust.

International interoperability could enable digital identity to meet this need. And the demand for this is growing.

Growing International Mobility Driving Demand for Cross-border Identity Services

A UN study a few years ago, identified that 232 million people, which equates to 3.2% of the world's population, live outside their country of origin in 2013[i]. That figure is a significant increase on the 175 million identified in 2000, and 154 million in 1990. The numbers are projected to continue to rise.

To put this international picture in a UK context, an estimated 5.5 million British people live permanently abroad – almost 1 in 10 of the UK population. The countries in which they now reside include Australia (1.3m), Spain (761k), the US (678k), Canada (603k), Ireland (291k), and New Zealand (215k).[ii]

International tourism is another growth sector which could become a major factor which may drive increased demand for international interoperability, and therefore its potential value. In 2018 there were a record 1.4 billion international tourist arrivals worldwide according to the World Tourism Organisation (UNWTO)[iii], which is an increase of 6% over the previous year alone. There were 39 million inbound visits to the UK in 2018, and over 70 million visits by UK citizens abroad.[iv]

Yet, despite an increasing need for cross-border identity services, there remain few options for travellers to prove who they are away from their country of origin in a consistent, trusted, digital manner.

Those that have a digital identity created via a scheme in their own country will struggle to use it in other countries at present, outside of those created and used in the EU.

Is Cross-border Interoperability Being Addressed?

In undertaking research for this report, we looked at a number of national approaches to both home market oversight and sought the views of a number of representatives from national authorities on potential international interoperability solutions, including representatives from the Digital Identity and Authentication Council of Canada (DIACC), the Department of Internal Affairs in New Zealand (DIA), the Digital Transformation Agency in Australia (DTA), and the EU's eGovernment and Trust Unit at DG Connect.

The one significant initiative that has begun to solve the cross-border interoperability challenge for some has been in the Europe Union, and the eIDAS Regulation.

It established a reciprocal and interoperable framework for trust services, including the requirement for member states to recognise eIDAS-notified digital identity schemes wherever they are used to access public services across the EU member states. This is in effect the only true cross-border, multi-national digital identity ecosystem operating across national schemes, but even here cross-border digital identity is far from ubiquitous in practice, particularly in the private sector.

The EU eIDAS framework is a unique case study, existing as it does within the multi-national political, legal and regulatory framework that the European Intergovernmental Treaties provide. A key lesson derived from eIDAS is the need to maintain local determination of the exact processes and standards employed, connected via an outcome-based interoperability framework established by peer review and underpinned by reciprocity between EU member states.

Lessons from the EU

The intergovernmental 27-state treaty that provides the foundation for the EU also provides a unique regulatory framework within which to create interoperability. While international governance of this type may not be replicable elsewhere, a similar approach of enabling national delivery within a multi-national **outcome-focused, peer-to-peer, recognised standards framework** may provide a starting point for wider interoperability.

There are various other examples of international co-operation around digital identity. Could they provide an interoperability solution?

- The UN provides a cross-national legal framework, although in a less extensive and binding form than the EU. A UN-sponsored project under the WTO e-Commerce programme has been established to develop a multi-national approach to trust services, including digital identity.[v] The programme has produced *Draft Provisions on the Cross-Border Recognition of IdM and Trust Services* which takes a largely legalistic approach to developing a common legal framework, and provides some definitions.

While helpful, its progress towards becoming an accepted text and, in particular, achieving the significance of becoming a UN Convention, and the timescale for that, is far from clear.

- Under the OECD's e-Leaders programme, a Thematic Group on Digital Identity has been established comprising New Zealand (the co-ordinator), Australia, Austria, Belgium, Canada, Chile, Denmark, Egypt, Italy, Mexico, Slovenia, Spain and the UK.[vi] This is an informative programme but looks unlikely to establish wide-ranging interoperability.
- A number of bilateral and multi-national MOUs have been signed; for example, as part of their new Digital Economy Partnership Agreement Chile, New Zealand and Singapore have agreed to work towards making their digital identity systems interoperable.[vii]

Co-operation is ultimately the starting point towards developing a common framework, and each of these initiatives showcases the willingness of national governments and other stakeholders to begin to co-operate.

The predominant developments at the moment are loose co-operation agreements between two or more states, usually with some form of existing economic ties underpinning the relationship.

International Organisations' Comments

The need to start small and build up the level of co-operation was a consistent message from a number of international stakeholders interviewed for the report. The need to start by agreeing common principles and objectives, beginning with smaller collections of states with common approaches to digital identity, and initially undertaking interoperability assessment in bilateral or limited multilateral contexts was the message received from most of the respondents.

The outlier was the position of the EU, where greater emphasis was placed on the wide intergovernmental work being undertaken under the UN / WTO programme.

The logical next step is to take a more structured approach to establishing interoperability. The next section of the report examines the type of organisation that might emerge to provide international oversight and interoperability.

Purpose and Role Played by an International Oversight Organisation

An international oversight organisation's primary purpose would be to facilitate the interoperability of digital identities across national borders. To achieve this, there would need to be mutual recognition and trust of each other's scheme (or schemes) underpinned by:

A. A common set of principles and rules to protect all participants
B. Recognised technical standards and open source software to facilitate technical interoperability
C. A way of testing and recognising interoperability between guidance and standards across different countries

A. Establishing common principles

A recurring theme emerging from discussion with stakeholders was the need to develop interoperability firstly by agreeing a set of common principles.

Most national digital identity frameworks establish guiding principles at a relatively early stage in their development. To review these and agree a set of common overarching principles would form a firm foundation for interoperability to be developed. The work already being undertaken by the UN working group [viii], by eIDAS participants and in other bilateral discussions may provide possible starting points.

B. Recognising standards and facilitating technical interoperability

There may be no need for an international organisation to create new technical standards itself. Within the international digital identity ecosystem, a growing range of technical standards are already well-established and widely accepted. Organisations such as the FIDO Alliance and OpenID Foundation provide a range of technical standards; there would be little value in an organisation seeking to replicate their work.

However, formally recognising and cataloguing technical standards that already exist, assessing their interaction, their level of equivalence and interoperability, and helping market participants to understand the choice of technical standards available to them may be a crucial role for the organisation.

C. Testing and recognising interoperability

Assessing, and recognising the equivalency and interoperability of national scheme standards could be the primary role for an international interoperability organisation. This could begin with testing equivalence and the degree of outcome-based interoperability across a number of bi- and multi-lateral international relationships, and over time encompass the international ecosystem in its entirety.

Question 13

Do you agree with the purpose of the organisation and its role (as above), and does the organisation have any other purpose?

International Organisations

There was agreement that the role of an international organisation, should one be necessary, would be to provide the basis for cross-border interoperability, and that the agreement of common principles was essential.

The feedback from stakeholders differed to a degree. Agreeing common principles was recognised by all. However, the question of whether an international oversight organisation should set standards, or define a legal framework, was more varied.

A role proposed for the organisation was to provide interoperability assessments between different national frameworks. Views on whether this could develop to some form of international standard or baseline was more varied. Certification was discussed by a number of respondents as a potential component to provide trust.

Assessing outcomes – assurance levels and levels of trust or risk reduction – was supported. However, the feeling was that national self-determination should be retained, pointing to an interoperability solution based on establishing and recognising common outcomes.

International versus National Determination

Ultimately, trust will also rest on the integrity and implementation of national standards, rules and processes at the local level, typically assured through a national system of conformance and compliance.

It is unlikely that national identity frameworks' governing bodies, typically national authorities or government agencies with a national mandate and autonomy of action, would submit elements of their sovereign role to an international authority. That is, unless it were given formal status by governments, such as via an intergovernmental agreement (such as is the case in the EU), and in areas where there exist International Conventions such as those agreed by the UN and overseen by Specialised Agencies such as ICAO, ICANN and the ITU.

Therefore, considering a compliance role for an international organisation may, at least at this stage, be a step too far. The focus should instead be on more achievable and co-operative aims.

Question 14

Should the organisation have responsibilities for establishing conformance and compliance of member countries' schemes (or ecosystem), or could this be achieved through bilateral agreements between two countries that are recognised by the organisation?

International Organisations

A system of interoperability, based on MoU's and bilateral agreements, is the emerging view, and for an international organisation to simply recognise international agreements that exist was felt to be a positive step. If international common principles and expectations could be set out (for example, through the current UN programme), this was felt to be of additional benefit.

Assessing conformance was thought to be a potential future role for the organisation; for example, by certifying whether recognised standards have been applied, were discussed positively (although whether evidenced by self-attestation, or an audit-based regime was less clear).

A compliance or enforcement role was felt reserved for high risk and systemically important issues – a point likely to be far into the future for digital identity, if at all.

Finding a balance that ensures that the local delivery of national frameworks can continue to reflect local challenges and have freedom of choice in how they deliver the outcomes that their citizens need, while retaining sufficient interoperability and comparability, will be an important success factor.

This suggests an outcome-based process interoperability framework, based on an assessment of comparability, finding common levels of trust and the degree of assurance of identity proofing, validation, verification and authentication.

Functions and Services Provided by an International Organisation

Following a review of international organisations operating in other global sectors, the table below sets out the principle functions and services that an organisation might be expected to deliver.

We have also included functions and services that an organisation might *not* be expected to deliver, to enable comparison with those of a national organisation covered earlier in the report.

Table 3: Possible Functions and Services Provided by an International Organisation

Area	Comments
Vision and Leadership	
Provide clear vision and strategic direction	In conjunction with core members and supported by wider stakeholders.
Industry engagement	Through international and national association members, and more broadly via working groups and expert advisory groups.
Funding and resourcing	Likely to be via member fees and revenue from services provided.
Market Design	
Guidance – policies, best practice, principles etc	Yes
Standards, rules and procedures	Recognition of standards and establishing rules and procedures, and the agreement and maintenance of equivalence matrices.
Specifications	Potentially.
Certification requirements	Maybe or simply acknowledgement of country-level certification processes.
Compliance / conformance tools	Maybe.
Certification services	Yes
Logos / trustmarks	No
Market Operation	
Ongoing monitoring and inspection	No
Dispute resolution	No
Support / helplines / newsletters / training	No
Registry	Possibly.
External Affairs	
Engagement with national Governments and regulators	Yes
Collaboration and participation with international authorities and organisations	Yes
Promotion and publicity	No

Question 15
What are your views on the possible functions of an international organisation?

International Organisations
As with Question 14 above, it was stressed by respondents that, while some functions might be necessary over time, there is likely to be a slow growth of function, rather than an organisation starting with all functions from day one.

Certification was a supported function as part of interoperability assessment. The production of guidance, and the recognition of technical standards were also supported functions.

Potential Operational Models for an International Oversight Organisation

Each of the international or global organisations assessed in the research has developed in its own way and no one model predominated. The organisations are largely focused on the development of new standards (rather than the interoperability between national frameworks, as suggested for digital identity), and in response to a particular set of requirements for their sectors or markets.

Organisations considered in the research were:

- The Internet Corporation for Assigned Names and Numbers (ICANN)
- International Telecommunications Union (ITU)
- International Civil Aviation Organisation (ICAO)
- International Air Transport Association (IATA) OneID Programme
- Fast Identity Online Alliance (FIDO Alliance)
- OpenID Foundation
- World Wide Web Consortium (W3C)

The international authorities and organisations exhibited a range of origins, governance models and structures, stakeholder engagement models, roles and funding requirements.

While the organisations exhibited significant continuity of purpose and roles, there were some outliers:

- The air travel trade association IATA's OneID programme, is a loose programme of shared innovation, with little to show in the way of standard-setting or interoperability framework outputs, despite objectives to do so.
- ICAO being another, as a purely inter-governmental initiative and membership base.
- The third being W3C and its unusually rapid rise to global prominence and systemic importance, following the extremely fast growth in the use and importance of the world wide web in the last few decades, as well as its depoliticised and therefore entirely non-governmental nature.

Despite these outliers, most organisations could broadly be identified as conforming to one of two operational models:

- **Multi-stakeholder organisations** have a very broad base of members and stakeholders formally engaged in a standard-setting operation with a formal, often UN-derived intergovernmental mandate.

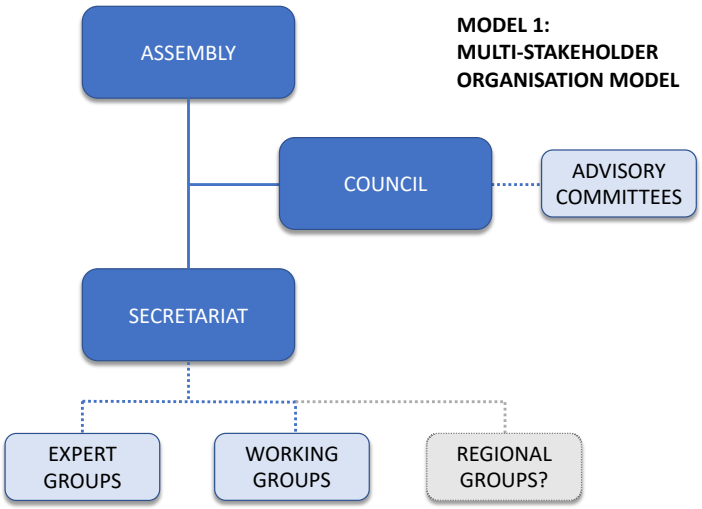
- **Focused organisations** that are smaller-scale not-for-profit membership organisations with a more limited core-membership and narrower, more focused (standard-setting) role and remit.

1) Multi-Stakeholder Organisations

The first archetype that emerged was that of a mature and broad-based global standards organisation, often instigated (and formally recognised) by intergovernmental agreement, and many with UN Specialised Agency status. Those that do have UN designation, and other mature broad-based global standard setters, frequently comply with the WTO's Technical Barriers to Trade (TBT) regulations and standard setting guidelines. This requires a thorough, government-involved, multi-stakeholder decision-making process.

A Multi-Stakeholder Organisation is usually characterised by a very broad membership (although solely Government-member examples exist). They often include academic representation, public and private sector, individual experts, not-for-profit and governmental agencies or national government representatives amongst their members.

Figure 1: Typical Multi-Stakeholder Model Structure



A representative and broad range of member types tend to be involved in an Assembly with ultimate decision-making powers. A Council of members operates as a more streamlined governing body, with expert and stakeholder input via a wide range of technical and task-specific working groups.

As well as tiered membership fees, revenue is often derived from training and certification activities. Significant central and regional secretariats are maintained, able to support well-developed technical/thematic groups and regional engagement.

2) Focused Organisations

These organisations are predominantly (and by comparison to multi-stakeholder organisations) more recent in origin.

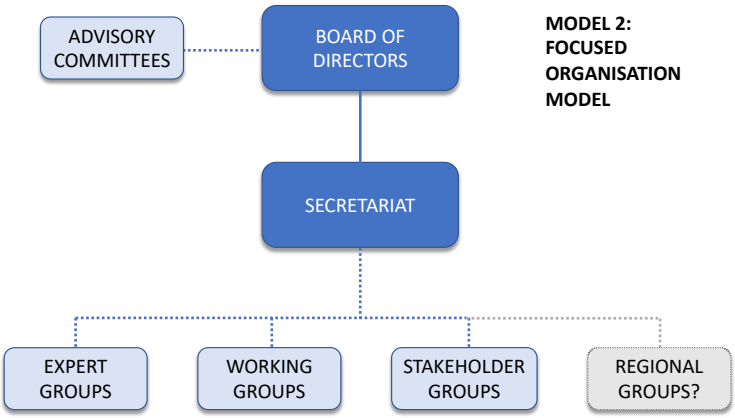
They are frequently instigated by a group of industry or expert stakeholders, seeking to set technical standards to underpin the operation of new markets and emerging technologies. Examples include organisations already focused on the development of digital identity standards, such as the FIDO Alliance, and OpenID Foundation. They are typically not-for-profit

limited companies, operating with a Board of Directors and a relatively small secretariat or management team.

They have a comparatively tight core membership headed by private, or a mixture of public and private, stakeholders. Compared to multi-stakeholder organisations, focused organisations have limited overheads with an annual budget of between £2m and £10m, have an executive board structure, and engage wider stakeholders via expert groups and working groups from within which new or amended standards are discussed and developed.

Their mandate is directly derived from their fee-paying membership. The make-up of their decision-making executive tends to reflect the influence of their primary funding members who make up the Board, and engagement and participation in the wider stakeholder community is managed via working and expert groups, and via the open source nature of the standards development programme.

Figure 2: Typical Focused Organisation Model structure



They often undertake certification programmes, which serves as an additional, and sometimes predominant revenue stream, alongside member subscriptions. Training and accreditation also form potential revenue streams.

Question 16

Are there examples of other organisational models that should be considered?

International Organisations

There were no significant alternative models raised, beyond the emerging pattern of bilateral and multilateral cooperation agreements between two or more states. The bilateral model has no central organisational requirement beyond state-to-state agreements and MoU's, but could facilitate interoperability between nations with significant economic ties and popular mobility, and lead to more formal and structured co-operation over time.

Comparing Organisational Models

Set out in the table below is a comparison between the key features of the two main organisational models.

Table 4: Comparison between Organisational Models

FACTOR	MULTI-STAKEHOLDER MODEL	FOCUSED ORGANISATION MODEL
ROLE	Technical or safety standards setter, usually with a wide scope. Mandatory application or critical to market function.	Technical standard setter (focused scope). Voluntary application, often with significant market penetration
MANDATE	Inter-governmental or UN-mandated organisation.	Industry/expert, member-led mandate.
ORIGINS	Long-standing or having undergone rapid maturity. Often formed by intergovernmental instigation.	Recent (usually <20 year) origination. Industry or stakeholder instigation.
SYSTEMIC IMPORTANCE / RISK	High systemic importance or risk of failure: e.g. Airline safety, telecommunications, internet.	Low to medium systemic importance and risk: e.g. Access management and authentication standards.
DECISION MAKING	'Multi-stakeholder model' – often UN Specialised Agency status - often follow WTO TBT standard setting process - Assembly of wider stakeholders with decision making role - Council decision maker between Assemblies - Often with direct governmental involvement - Broad consensus-driven decision making Regional and specialist groups have a formal role beneath Assembly (chairs voted for by Assembly).	Bespoke, narrower membership and more focused model with expert input – often not-for-profits limited companies. - Executive Board of key members is the governing body - wider stakeholder engagement via working/expert groups and advisory bodies. Proposals are made by WGs for new/amended standards.
GOVERNANCE STRUCTURE	Assembly (Sovereign Body) + Council (Governing Body), supported by a large secretariat.	Executive Board, Board Committees, supported by a small secretariat.
STAKEHOLDER ENGAGEMENT	Decision-making role, embedded in the Sovereign and Governing Bodies (Assembly and Council), decision by broad consensus.	Expert-led, sector-specific, stakeholder-specific or task-specific working groups.
FUNDING SOURCES	Wide range of examples – via government/UN grant, and/or membership fees, some additional revenue streams Government funding is often significant (except W3C, reflecting internet neutrality). Significantly more expensive to run, due to requirements of a broad multi-stakeholder model and	Membership fees plus additional revenue from certification, training or support services. Private sector member contributions are significant. A much smaller budget, a more focused structure, and more reliant on revenue from certification and other services as well as membership fees/grants.

	the costs incurred to support a devolved and very wide engagement and decision-making structure.	
TOTAL FUNDING	£100m+	£2m+
MEMBERSHIP	Governments involved – either Governments only (ICAO) or as part of a wide range of member types. Members often range widely in nature, include individuals, academics, not-for-profit and public/private sector organisations as well as governments.	Potentially no direct Government membership or Board-level representation. Private, or public and private sector membership, but few individual or academic memberships. Individuals, academics and not-for-profits engaged but not always Board-level or fee-paying members.

Question 17

Do you agree with the broad characteristics set out and are there any other factors that should be considered?

International Organisations

The principal variables between the two models were generally agreed to be:

- Market and organisational maturity
- Systemic importance to the international economy
- Level of risk

Assessing the Appropriateness of Different Organisational Models

Digital Identity ecosystems involve a wide range of stakeholders, whether identity providers, digital identity service providers, relying parties across both public and private sectors, regulators, scheme operators, and end users. An organisation seeking to increase interoperability at a global level will certainly need to engage a wide range of stakeholders: in what capacity, and under what organisational model is a key consideration.

The Multi-Stakeholder Model

It is possible that a complex, broad-based organisation could be set up to maximise stakeholder participation, and potentially given an intergovernmental or UN-based mandate of some kind. This may yet prove to be the eventual endpoint for the UN working group discussions currently taking place, although that point remains some way into the future.

In such a circumstance the outcome is likely to be similar in organisation and wide membership to a number of the multi-stakeholder organisations assessed by this study, and in line organisationally with the structure identified in Figure 1 above. A possible membership model is set out in Figure 3 below:

Figure 3: Example Multi-Stakeholder Membership Base

Tiered membership classes could give formal representation to a wide range of organisation types, with diverse membership of a broad-based Assembly, and Governing Council structure.

However, from previous experience such complex organisations tend to emerge and be given formal designation, such as becoming a UN Specialised Agency and applying WTO TBT standard setting rules, once the subject international organisation has already reached a degree of maturity. They are less often created at this level of complexity from scratch. Operating models tend to reflect the significant and systemic importance of the function and standards it is there to create or support – and it is hard to argue that digital identity interoperability across borders meets that criteria at present.

A body organised in this manner would likely incur significant costs to operate, although this may be offset by revenue arising from operating a certification programme and other activities.

Multi-Stakeholder Model Assessment

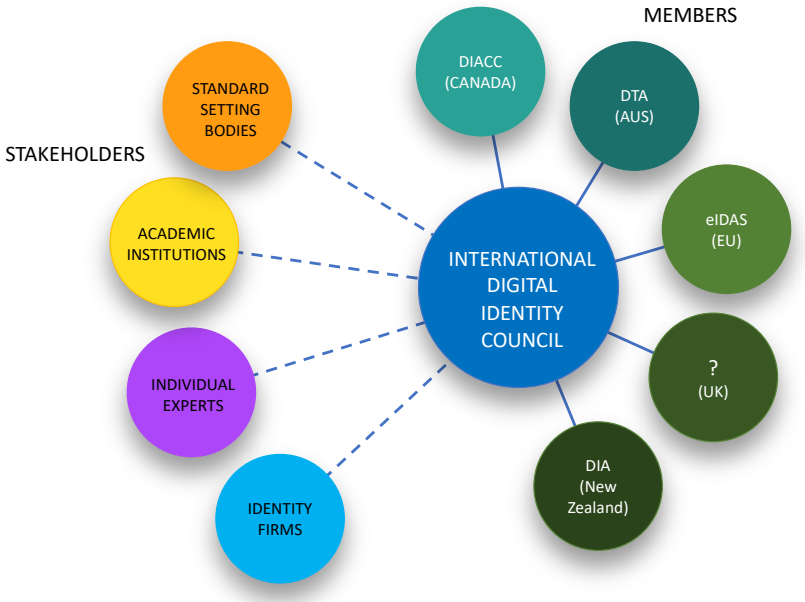
- Wide engagement and decision-making involvement
- Established international standard-setting model
- Potential for intergovernmental recognition
- Regionally active

- Digital identity is not currently of sufficient systemic importance for this to be proportionate
- Usually mature, well-established sectors, rather than early-stage
- Complex and expensive to maintain
- Slow decision making

The Focused Organisation Model

What seems more proportionate to the role we have outlined in this paper, might be a narrower, more focused organisation, more in line with the model adopted by organisations such as OpenID Foundation and the FIDO Alliance.

Figure 4: Example Focused Organisation Membership Base



A more narrowly defined core membership could comprise of the national associations or bodies responsible for maintaining national digital identity frameworks and functioning ecosystems. Engagement would still be possible with a wider group of stakeholders, via expert advisory groups and task-based working groups.

Employing a narrower operational model could streamline decision making processes, reduce operating costs, while being sufficient to maintain the key functions of interoperability assessment and certification. With significantly reduced operating costs, funding could reasonably be expected to be covered by membership fees paid by a limited number of national associations who make up the governing body, alongside potential revenue from the operation (or outsourcing) of a certification programme.

This would not preclude the organisation adding additional layers of membership, role or function in future, for example as digital identity increases in systemic global importance.

Focused Organisation Model Assessment

- Can be established and funded by non-governmental stakeholders, or in collaboration between government and industry
- Early-stage standard-setting or interoperability model
- Agile, centralised, relatively lower-cost solution
- Wider engagement possible via stakeholder groups

- A small membership base may not be financially sustainable.
- As the systemic importance and number of nations with a digital identity framework increases, a focused organisation may not remain a representative or proportionate solution.
- May lack governmental recognition if purely industry-led

Question 18

Do you agree with the appropriateness of the Focused Organisation Model in this context? Are there other factors that should be brought into consideration that might make a stronger case for a Multi-Stakeholder Model or another alternative structure?

International Organisations

Other than the response from DG Connect, which emphasised the potential for the UN workstream to create an international framework in time, the focused organisation gained a great deal of support in principle.

However, as for other questions, an iterative, proportionate route was recommended, starting with bilateral and limited multilateral assessment of interoperability, and agreeing common principles, with an organisation perhaps coming later in the process, as a logical next step as digital identity solutions are rolled out more widely, and both cross-border demand and the systemic importance of digital identity to the international economy grows.

The Blueprint for an International Oversight Organisation for Digital Identity

There is wide agreement around the underlying need for and value of cross-border interoperability for Digital Identity.

From the research undertaken on existing international oversight organisations, there are a couple of typologies that emerged. Whether it is possible to develop an oversight organisation focused on interoperability (whatever its organisational shape and scale) from scratch before a longer period of building bilateral and multilateral cooperation was a more challenging issue for respondents.

The Way Forward: Reflections on Interviews with National Authorities

Following informal interviews held with representatives of a number of national authorities, and government departments responsible for overseeing national identity frameworks[ix], there were some common messages that could help to inform the next steps towards creating an organisation and solving cross-border interoperability challenges.

There was a degree of wariness communicated concerning the impact an international authority may have over the sovereign nature of national identity frameworks – national autonomy and flexibility of delivery should be retained, or agreement will be hard to broker.

The starting point was clearly felt to be in agreeing common principles between different states, and then building co-operation and bilateral or multilateral interoperability assessment on the basis of a common set of guiding principles.

The need to retain proportionality between the solution and the level of risk and systemic importance was felt, in most cases, to be an important factor. Increased systemic importance will be driven by

- Wider adoption of digital identity frameworks by states
- Increased global mobility
- Increased value and risk associated with cross-border digital identity use and transactions underpinned by digital identity

The Blueprint

1. **Developments should be driven by governments and private sector in partnership.**
2. **Start with agreeing common principles.**
3. **Undertake bi-lateral and multi-lateral interoperability assessments initially.**
4. **Develop a common framework of outcome-based rules, based on peer-to-peer recognition and recognised standards – retain national flexibility to deliver.**
5. **Act in proportion to the level of systemic importance and risk associated with digital identity.**
6. **Work towards a focused, co-operative organisation to assess and certify cross-border interoperability.**

Conclusions

National

There is clear recognition that a national oversight organisation is needed to orchestrate and govern a digital identity ecosystem in the UK, and that this organisation needs to be representative of all stakeholders across the UK. Representation could come in a number of forms, from membership of the organisation, to advisory panels and user groups. The recommendation is that, through collaboration between the public and private sectors, an independent authority should be established, accountable for oversight of a Government-developed or approved trust framework.

Work is required to provide further detail in a number of areas, culminating in a costed business plan. These areas include

- Purpose, scope and terms of reference
- Membership structure, options and fees
- Organisation structure, roles and resource requirements
- Design of overarching trust framework
- Governance model
- Functions and services
- Advisory panels and user groups

The Peer Review Group also commented that an oversight organisation "needs a market to oversee". In the UK, although various initiatives are underway, there is no strategy for digital identity that brings all market sectors and stakeholders together. OIX is gearing up to meet this challenge but Government support and action is also needed to drive this forward.

International

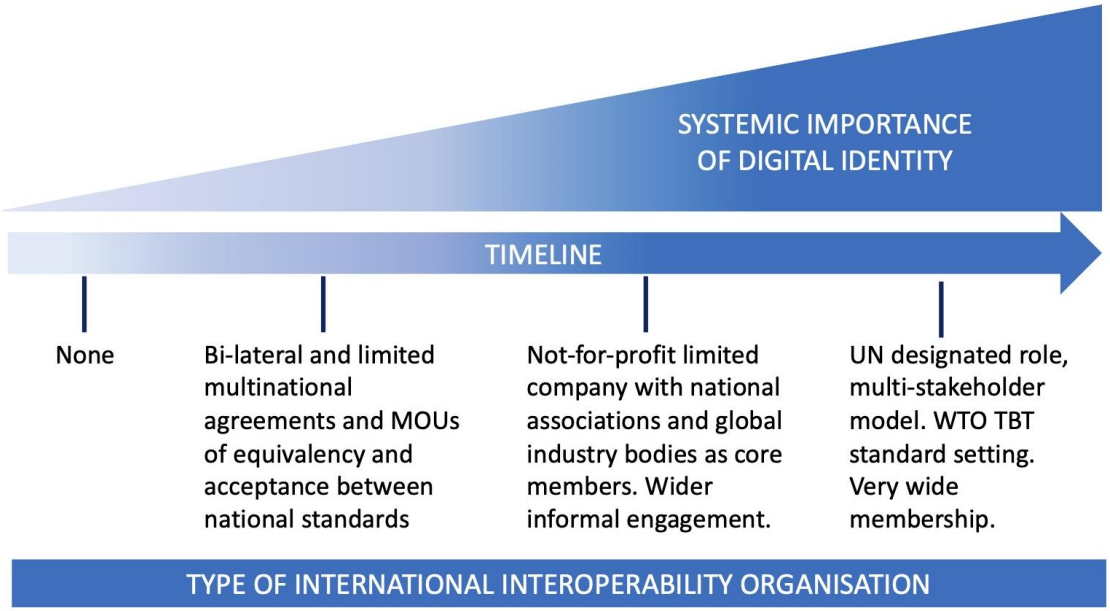
There is clear willingness amongst international stakeholders to explore interoperability in greater detail, starting with finding common principles and interoperability assessment across smaller sub-sets of states who have digital identity frameworks already in place.

it was clear that there was little demand at this stage for an international standard-setting organisation, instead the organisation's role is better focused on assessing, and potentially certifying interoperability between national frameworks, and recognising the technical standards that already exist.

Proportionality was another key message – and this begins to suggest there may be a continuum, leading from the absence of interoperability, through initial stages of bilateral and multilateral assessment and development of common principles, to an early-stage international oversight organisation based on the focused model explored in this report.

At a later stage, when the systemic importance of digital identity to the global economy warrants it, to expand the organisation to reflect the multi-stakeholder model. See Figure 5 below.

Figure 5: Increasing Systemic Importance vs Organisational Model



The acceptance of the growing importance of finding a way to ensure interoperability and develop the international framework for digital identity was common to all respondents and provides a very positive platform for future developments.

It may be possible to begin more detailed interoperability assessments, and to establish common principles in the near term.

The question then is more to do with the extent of the role required at each stage of the development of the international identity ecosystem, and how quickly the need for a formal organisation will become evident.

REFERENCES

[i] *https://www.dw.com/en/more-people-living-abroad-than-ever-says-un-study/a-17083834*
[ii] *http://news.bbc.co.uk/1/shared/spl/hi/in_depth/brits_abroad/html/default.stm*
[iii] https://www.theguardian.com/news/2019/jul/01/global-tourism-hits-record-highs-but-who-goes-where-on-holiday
[iv] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwj56ved2b_nAhWgTxUIHdTmDk4QFjABegQIChAF&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FSN06022%2FSN06022.pdf&usg=AOvVaw3_HalaIZfoVXgw_xirxB13
https://migrationobservatory.ox.ac.uk/resources/briefings/migrants-in-the-uk-an-overview/
https://www.statista.com/statistics/578815/most-visited-countries-united-kingdom-uk-residents/
https://www.ons.gov.uk/peoplepopulationandcommunity/leisureandtourism/articles/traveltrends/2018
https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/articles/whodoestheuktradewith/2017-02-21
[v] https://uncitral.un.org/en/working_groups/4/electronic_commerce
[vi] https://static1.squarespace.com/static/5ae1d5ea5cfd798b6b4ac148/t/5bc069bd71c10bb81a0afec7/1539336645293/16_A_OECD+%2820180927%29+eID+Conference+-+Lisbon.pdf
[vii] https://www.gsma.com/identity/news-flash-push-for-international-id-interoperability / https://www.mfat.govt.nz/assets/FTAs-agreed-not-signed/DEPA/DEPA-Chile-New-Zealand-Singapore-21-Jan-2020-for-release.pdf
[viii] https://uncitral.un.org/en/working_groups/4/electronic_commerce
[ix] DIACC, DTA Australia, DIA New Zealand, EU eGovernment and Trust Unit DG Connect