Open Identity Exchange

'Next steps for DCMS Digital Identity policy development' questionnaire – OIX Response

12th October 2020

Version 1.0

Author: Nick Mothershaw, Chief Executive
Email: nick.mothershaw@openidentityexchange.org
Mobile: 07885 618523

1 Introduction

This document records OIXs response to the 'Next steps for DCMS Digital Identity policy development' questionnaire.

Key points made in the response can be summarised as:

- OIX advocates for a public-private approach to the definition of the UK Trust Framework for Digital Identity and the accompanying Competent Authority.
- As well as Identity Providers, The Trust Framework must recognise and accredit suppliers of components of trust, and relying parties undertaking their own ID verification.
- The Competent Authority should be a public-private partnership.
- OIX could be considered as start point from which to define the Competent Authority, which could also leverage the OIX brand and the OIX Directory.
- Inclusion is already being partly addressed by the OIX / TechUK Inclusion Steering Group.
- A fine balance between privacy and transparency must be struck
- Any fees for government data sources must be of a level that will allow relying parties to achieve cost efficiencies over and above using existing ID verification approaches.

2 OIX Response

OIX Response to Next steps for DCMS Digital Identity policy development questionnaire.

1. **What is your Name?**

   Nick Mothershaw

2. **What Organisation do you work for?**

   The Open Identity Exchange

3. **What is your email address?**

   nick.mothershaw@openidentityexchange.org

Trust Framework Development

In response to the Call for Evidence, the general consensus was that government should take the lead in setting the rules and building public trust. Other countries and markets have developed a trust framework to address these challenges.
A trust framework is a set of rules and standards governing the use of digital identity. All organisations that are part of the trust framework will create products and services, check identities and share attributes in a consistent way, enabling interoperability and increasing public confidence.

4. What thematic areas should be considered in the development of a trust framework and why?

Focus on creating a user centric national trust framework for interoperability, inclusivity, privacy and security that is strong enough to ensure these principles are but that allows flexibility, extension and innovation by Trust Schemes that are created to meet the needs of specific sectors and use cases.

Work with the private sector to collaboratively define the framework and ensure it meets the needs of both public and private sectors, thus achieving private sector support and buy in and ultimately interoperability.

The areas that should be covered by the national trust framework to ensure interoperability would be:

- Trustmark: A signal to all parties that the framework is in operation.
- User Services: privacy/consent rules, right to close accounts and have information returned / removed from relying parties, identity recovery, fraud information and repair, support services and redress.
- Relying Party Services: fraud information and repair, support services and redress.
- Trust Rules: ID Proofing, Authentication, ID Assurance, trusted access to eligibility information.
- General Rules: Record Keeping, minimal Fraud Controls to ensure the overall ecosystem is protected.
- Security Rules: minimum security standards to be met.
- Trust Registry: authorisation of parties into the accredited ecosystem.

Please see the OIX Guide to Trust Frameworks for more detail on what should be considered in each of these areas.

The framework should recognise that the achievement of trust in the identity may be achieved by different parties:

- Directly by a **Relying Party**
- By an **Identity Provider**
- In part by **Evidence Verifiers** or **ID Technology Providers** who might provide (perhaps via a Self-Sovereign ID, or perhaps directly) component parts of the solution that are used by a Relying Party or ID provider. An example might be an authenticator provider who could be accredited to part of GPG44, or an evidence verifier who be accredited to part of GPG45.

The trust framework and its accreditation process should therefore support each of these different parties.

Consideration should be given to framework level management of:

- Fraud attacks and fraud information sharing.
- User redress and ultimate ombudsman

Many use-cases demand, or benefit from, transparency between parties:

- The user should be able to see a record of who they have shared their data with.
- The relying party may need to receive the detail of the evidence behind a user's trusted identity or verified trusted evidence.

The framework should allow this transparency where required. The framework should not try to introduce "blinding" of parties to enforce privacy – this should be a Trust Scheme level rule if required.

5. Which existing standards or guidance do you think should be referenced?

GPG45 and GPG44.

OIX would like to see a more granular approach to ID adopted within GPG45. More "settings on the dial" are required to:

- Allow very simple verified IDs to be established for purposes such as age verification and address verification.
- Align with existing long-standing approaches to ID validation and verification for AML KYC checks in finance.

GPG43. This is currently written to be a public sector document, primarily aimed at public sector relying parties. It should be updated, or an equivalent document created that is aligned to the framework.

6. Thinking about UK legislation, international legislation and/or technological developments, what dependencies do you think should be considered in the development of the trust framework?

Alignment with eIDAS.

The framework should allow for the provision of trusted information via Self Sovereign style Digital IDs.

The framework should steer clear of setting or enforcing particular technical standards. However, the framework might endorse technical standards as being acceptable (e.g. OIDC, W3C Verifiable Credentials).

Legislation

Legislation for digital identity is needed to provide a basis of national and international confidence in digital identities. This legislation will be the subject of a formal public consultation, as mentioned in the Call for Evidence response published on 1 September. Detailed proposals are being developed and may cover the rules and standards that will be part of the Trust Framework, an oversight function for this enabling framework, and the removal of legal barriers to the use of digital identity.

7. What legislative changes and data do you need to enable the use of digital identity tools within your business?

Government should create the national trust framework, in collaboration with private sector, and then work to enable its acceptance through changes to sector or use-case based legislation.

OIX will continue to work with government to identify legislation that needs to be changed to allow Digital ID to be accepted for different use-cases.

OIX will also support government in the identification and prioritisation of data that will improve inclusion within Digital ID, through the Inclusion Steering Group.

8. Where should we prioritise our efforts, and what benefits can we expect to see for people and the economy?

It's difficult to subjectively prioritise which market or use-cases should be focussed upon. A detailed market analysis should be undertaken to enable a more empirical prioritisation.

Key markets or use-cases that are exploring the adoption of trusted identities are:

- Age Verification (online and face to face)
- Finance - KYC
- Finance - Pensions
- Employment Vetting / Eligibility
- Air Travel (cross boarder travel)
- Health – presentation of health status
- House conveyancing
- Property Rental
- Gambling

OIX is working to drive adoption of interoperable trusted Digital ID across these different areas.

Governance and oversight

A governance and oversight function will be helpful to enable the safe creation and use of digital identities across the economy, and provide guidance if something goes wrong.

9. What should be the tools available to an oversight body to ensure adherence to the Trust Framework?

Accreditation supported by legislation and regulation.

Accreditation should include obligations on the accredited party around user support and redress.

Different methods of accreditation should be considered: from self-assessment to full certification.

The framework should enable Trust Schemes to enforce and administer accreditation to the framework and the scheme.

The Trust Framework governance body needs to be, or needs to appoint, an ultimate arbiter, or ombudsman, to ensure the right of users and relying parties are represented.

The OIX Directory can be used to communicate accreditations to the market.

10. What should be the consequences for infringements of the agreed Trust Framework?

Withdrawal of accreditation

Legal consequences of breach of contract.

11. How should redress be handled for organisations that consume digital identity, and for people if something goes wrong?

For organisations liability cover for costs incurred could be implemented. The framework could allow 'fault-based liability' to be implemented: if the accredited party can show they have followed the rules of the framework, then they would not be at fault and would not take any liability.

For users, monetary compensation or re-dress packages, such as ID theft monitoring, could be offered.

A collective fund for compensation users, along the lines of the travel or finance industry, could be established. Accredited parties could have to pay a levy into this fund.

However, the goal of for Digital Identity in the UK (and elsewhere) should be that it's use is more cost effective for relying parties than using traditional electronic and manual

approaches to identity verification and management. Any consideration around compensation mechanisms should take this goal into account. If the inclusion of compensation makes the cost of digital identity prohibitive then digital identity will fail and relying parties will carry on using the proven solution for ID verification and management that they have in place today.

12. What existing bodies or groups may be well placed to provide oversight?

OIX is uniquely positioned in the UK market as a representative of identity services suppliers who are those most likely to be accredited to the framework.

OIX also has a wealth of knowledge around trust frameworks and identity interoperability.

However, OIX is not today a governance or oversight body for standards.

OIX produced a paper in March 2020 exploring the need for an oversight authority for identity: A Blueprint for National and International Oversight of the Digital Identity Market This examined similar technically complex markets, such as finance and the internet, and concluded that governance bodies are typically independent non for profit organisations. The OIX paper made a number of recommendations that apply in the context of creating a governance body for digital identity in the UK:

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

OIX proposes to work with the UK government to define the scope and operational requirements for an oversight and governance body for the UK trust framework.

OIX would then wish to be considered as a start point for the formation of a governance body in the UK. An adjunct or subsidiary of OIX could be formed to create and operate the required governance body, ensuring legal and financial separation from our role as a global members organisation driving the definition and adoption of identity trust. This new sister organisation would leverage:

- The OIX brand, already established as a trusted identity knowledge-authority.
- OIXs extensive knowledge base built up through papers and projects over the past 10 years (many of which were funded by UK government).
- The OIX member community to create and then promote adoption of the trust framework in the private and public sectors.
- The OIX peer review community to gain sector-based input into and support for the trust framework
- The OIX Directory to communicate accreditation to the framework.

This approach would be faster and more cost effective

OIX could also be the steward of the Trustmark for the UK Trust Framework

13. It is envisaged that an advisory group will be created to provide viewpoints from industry and privacy groups - how could this be best enabled?

OIX would recommend that a public-private steering group is set up to design the trust framework and create the oversight authority. This steering group might then evolve into the governance board for the authority as it is then formed. Members of this steering group should include:

- Government identity policy stakeholders: DCMS, GDS
- Government identity relying parties: representatives from the government Digital Identity Steering Committee.
- Private sector relying parties, or trade body representatives, for key sectors: Finance, Travel, Health, Gambling, Age and so on.
- OIX as the representative of the identity supplier community.
- Representatives advocating on behalf of the consumer.

The OIX paper on oversight for Digital Identity recommends that there are a number of advisory groups established as part of the formation and operation of an oversight authority. These would include:

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

It might also be appropriate to set up advisory boards around key principles: Inclusion, Privacy, Security. The OIX Inclusion Steering Group is already addressing his key principle.

Attribute checking of government data

Respondents felt strongly that the government should unlock additional data sets. Government data was seen as essential for meeting digital identity needs and could be woven with other data sets if the individual chose.

14. What attribute datasets would be useful for your organisation (beyond passports and driving licences)?

The OIX Inclusion Working Group identified the following top 10 data sources that will allow more users to more easily attain identity trust, whether via a Digital Identity provider for when used directly as an authoritative source of Identity Evidence via a relying party:

- HMPO - Passport
- DVLA - Driving licence
- Student loan accounts
- Birth register
- DWP & HMRC records
- Learning Records Service
- NHS central patient registry
- Council tax bills
- Occupational pensions
- Travel concessions

The OIX Inclusion Steering Group is commissioning a segmentation exercise to quantify how many users of different types (e.g. young, old, new to country, financially disadvantaged) will be assisted in attaining identity trust through access to these, and other, key datasets.

15. How likely is it that your organisation will invest to enable checks against government identity data when it is available?

N/A

16. What is the commercially viable price point for your organisation to make a single check against an attribute dataset?

OIX does not consume identity information itself. However typical pricing for a single dataset check for ID purpose on datasets that are available today, for example credit reference data and telco data, are priced at pence, often a few pence, not pounds. The price varies dependent in the risk profile of the consuming relying party and what other data is already available in the market. There is a vibrant competitive market for ID data validation and verification services in the UK, which shows that good margins can be made at relatively low “per click” pricing. Government needs to be careful not to price itself out of the market, or worse generate inclusion issues, through setting too high a price for government data. Government would be better focussing on the economic

value generated for UK Plc as a result of these data sets being available. OIX's offer to UK government of producing an analysis of the economic value of releasing key data sets to key market sectors is still an area we could work collaboratively on.

Another consideration is that the government own Open Data approach could imply that individual users should be able to assert their data to a third party for no cost.

However, the goal of for Digital Identity in the UK (and elsewhere) should be that it's use is more cost effective for relying parties than using traditional electronic and manual approaches to identity verification and management. Any consideration around fees for data should take this goal into account. If the inclusion of fees for data makes the cost of digital identity prohibitive then digital identity will fail and relying parties will carry on using the proven solution for ID verification and management that they have in place today.

17. **Which type of digital identity checks would be most useful to your service model? E.g. are 'yes/no' validity checks relating to data inputted by your customer sufficient? Are photo or fuzzy matching essential components?**

Relying parties ideally want more information about the evidence being verified: how verified, date created / issued, date last used, lost / stolen, date last updated, previous names and addresses. All this helps the relying party mitigate against fraud risk (e.g. recent updates) and provide a better service.

If the source data contains a photo of the user, then matching this against a photo would be highly desirable.

When a matching process is undertaken by the evidence issuer this makes them an evidence verifier. In this role they should also be subject to the rules of the trust framework (matching rules, record keeping, fraud controls etc.)

Fuzzy matching, such as name synonyms (Mohammed / Muhammad) and address formats are desirable.

International Interoperability

The Call for Evidence restated the importance of the UK taking an international approach to digital identity. Respondents see the UK as having the experience to lead the development of international best practice.

18. How important to you is international interoperability? (Scale 1-5, 5 High)

5

19. With which markets is it particularly important for the UK to achieve interoperability?

OIX is about to release a methodology for trust framework interoperability assessment.

This will allow the UK Trust Framework to be assessed again other published trust frameworks such as eIDAS, NIST or DIACC.

OIX proposes that this methodology is applied between a draft version UK trust framework and at least one other key framework to assess how it will align with and interoperate with other key trust frameworks prior to its finalisation. This could be achieved through an OIX project.

Privacy and inclusion

Respondents have highlighted privacy, inclusivity, and proportionality as three of the key principles underpinning the development of digital identity for the economy.

20. What are your concerns about consumer protection and privacy in developing a new digital identity trust framework?

We are confident a user centric trust framework can be created that supports consumer protection and privacy by default.

It is important though not to sacrifice other principles, such as transparency, to achieve perceived privacy requirements. For example, the approach to "double blind" hubs implemented previously for government in the UK is not required, or indeed permissible, for many private sector implementations.

21. Do you already have practices implemented into your service that focus on diversity, inclusion and safeguarding (e.g. in policies or embedded into technology)? If yes, please provide examples. If not, have you encountered any barriers in trying to do so?

Not applicable in this context - OIX does not run a consumer facing service.

22. What could government do to help ensure digital identity is as inclusive as possible?

OIX is already running an Inclusion Steering Group, in collaboration with TechUK. This group has identified the following three priorities:

- A segmentation exercise should be undertaken to quantify how many users of different types (e.g. young, old, new to country, financially disadvantaged) will be assisted in attaining identity trust through access to key datasets.
- Vouching should be included in ID proofing standards i.e. GPG45.
- Identify and drive for access to be enabled to the top 3 data sources to aid inclusion.

The original OIX / TechUK Inclusion Working Group identified the following top 10 data sources that will allow more users to more easily attain identity trust, whether via a Digital Identity provider for when used directly as an authoritative source of Identity Evidence via a relying party. The segmentation exercise will also allow these to be prioritised to maximise inclusion benefits of their use:

- HMPO - Passport
- DVLA - Driving licence
- Student loan accounts
- Birth register
- DWP & HMRC records
- Learning Records Service

- NHS central patient registry
- Council tax bills
- Occupational pensions
- Travel concessions

23. What are your key accessibility concerns in the area of digital identity?

OIX believes accessibility must be built into the framework from the ground up. Whilst mobile devices offer many accessibility advantages, they are not a panacea to address accessibility issues, so the framework needs to support a broad range of form factors and access techniques.

Listening Sessions

We anticipate that the listening sessions will commence from 21st October. Please indicate below the topics that are of most interest to you. Please tick all that apply.

24. What topics are you most interested in exploring during the listening sessions? (TICK ALL THAT APPLY)

Trust Framework development - YES
Legislation - YES
Governance and oversight - YES
Attribute checking of government data - YES
International interoperability - YES
Privacy and inclusion - YES

OIX would want to be involved in all of these listening sessions.