# Accelerating the UK Digital Identity Services Market

## *Proposal for a Registry of UK Standards and Services*

**The Open Identity Exchange | Hindle Consulting Limited**

*Andrew Hindle*
*07 August 2015*

# Executive Summary

Demand for high quality, secure and convenient access to online services across both public and private sectors continues to grow. These services are accessed not only through browsers and smartphone platforms, but increasingly via other networked devices and by other software platforms on behalf of individuals and public and private sector entities. Underpinning these services, and critical to their success, are dynamic supply chains of trusted and interconnected digital identity services.

These supply chains span the public and private sectors, and broadly support the European Digital Single Market initiative, which has an estimated eventual contribution to the European economy of €340 billion

(Dunne, 2014). The supply chains include central government services such as GOV.UK Verify; regional services; and identity infrastructure and platform vendors such as Microsoft, Ping Identity, Verizon, Digidentity and others. It is an emerging open market, but it is not accelerating at a pace that will support the anticipated growth of UK services over the next 5 years. Inhibitors to the market include the lack of open standards and processes governing the permissible reuse of identity services across the public and private sectors. This impacts the interoperability of systems, and the trust and transparency between services and their users.

This white paper explores one significant factor that is acting as a brake on the delivery of services: the lack of an independent, reliable and agile repository of digital identity standards and services. As a mechanism to accelerate the provision of this infrastructure of services, an incremental extension of the current OIX ruleset and processes is proposed which would provide a public, trusted registry of services and a self-certification process. This enhancement would help to reduce the risks associated with innovation, enabling open, interoperable standards and solutions to be developed more rapidly and deployed more widely. Organisations may use this process to ensure that their digital identity solutions are aligned and interoperable with emerging best practice in the digital identity market.

Together with existing standards, deployments and well-established market principles, the extended ruleset and processes will reduce splintering of the market into siloed proprietary systems and services - a common outcome in early markets, which inhibits adoption by users - and will help to accelerate growth for the open digital identity services market in the UK.

## Introduction: Problem Statement and Rationale for an OIX Test Infrastructure

Digital identity services form a nascent critical infrastructure in a rapidly evolving market in which a wide range of private and public sector players operate. Traditional 'back office' data services for checking identity at new customer registration are now complemented by 'front office' federated systems in which a user asserts an identity from another domain.

In the UK, GOV.UK Verify will continue to iterate and evolve as part of this network of interconnected and federated digital identity services. GOV.UK Verify is grounded in the notion of a federated model which relies on an open market of standards-based supply chain services that may be used at different times and in different ways by a wide range of service providers.

This market and approach are new and, as such, are unavoidably characterised by a substantial number of unknowns. OIX UK and the UK Government Cabinet Office have developed an open and collaborative process for investigating these unknowns. Projects operated under this process are becoming more numerous as the market matures and as more parties leverage the benefits of interoperability that come from open identity standards.

In the current market, however, there are few standardised and certified methods by which organisations can test and demonstrate how federated and other identity services can be deployed in their service context. Whilst technical certification testing processes and registries certainly exist, these are not normally specific to a given regulatory context. The lack of clarity as to whether services are aligned to a particular set of business, technical or regulatory standards, and how that alignment has been determined, has three significant and deleterious effects on the development of the broader identity ecosystem:

**Barriers to Market Entry**

Each new proposed project must develop in-house, custom test components from scratch: the costs and time required can be significant. Further, custom components have little value or recognition across market sectors - so although they may support initial technical testing, they do not validate any new product or service as interoperable or 'fit-for-purpose'.

**Service On-ramp Delays**

Even those projects that are successful at the Alpha stage[1] can take significant time to move to production: integration testing work undertaken during an Alpha is often redundant for the purposes of validating a production solution, due to the lack of robust testing and component reuse mechanisms.

**Innovation Stifling**

Organisations wishing to propose innovative or alternative solutions that might benefit the entire ecosystem (including the Government Digital Service ('GDS') and other UK central government departments, as well as the wider public and private sector) are deterred, since there are few cost-effective ways to objectively or independently demonstrate new services without significant up-front investment or disruption of existing services.

In the open digital identity services market in which GOV.UK Verify will make a significant early impact, services and solutions are emerging which potentially benefit from an established test infrastructure capability. The TISA Savings and Investments Policy Project ("TSIP"), for example, calls for a "Digital Passport" (TSIP 2015) to simplify individuals' engagement with financial services providers; and it has been proposed that any such solution would benefit from alignment with GOV.UK Verify (Out-law.com 2015). The lack of robust and accepted testing and self-certification capability in the market can only delay the provision of innovative solutions such as TSIP.

Solution vendors and service providers across the public and private sectors will need to understand how they interoperate with digital identity services in a multitude of contexts. However, collaboration between organisations to understand and test interoperability is impeded by a number of legitimate concerns:

[1] In the OIX UK project process, an Alpha is a prototype, testing and learning phase: http://oixuk.org/?page_id=6

- How is intellectual property managed?
- On what financial basis are projects progressed?
- How are components certified as aligned to GOV. UK Verify standards and good practice guidance; to the Privacy and Consumer Advocacy Group Identity Assurance Principles (PCAG 2014); and/or to other project-relevant principles or standards (such as SAFE-BioPharma or UMA)?
- How are project findings communicated?
- How do components move from the OIX test process into commercial deployment?

OIX UK and the Cabinet Office have developed a process and ruleset to address such concerns in a consistent and transparent manner so that multiple collaborative projects can take place with interested stakeholders. However, the growing number of projects and the maturing of the digital identity services market mean that the process and ruleset might be incrementally extended to support growth in use-cases, standards, suppliers and users. This paper explores how that incremental extension should occur.

## Identity Supply Chain Participants

We have identified a broad range of participants in the existing identity supply chain who could benefit from the extension of the OIX UK process and ruleset to enable an increased volume of collaborative projects. The list of participants and benefits, given in Table 1, is neither intended to be prescriptive, nor assumed to be complete. Indeed, the very nature of this fast-moving market means that it is highly likely that other participants with other needs will emerge. A key design goal of the system must be to allow sufficient agility to incorporate new participants and requirements that cannot be anticipated at the time of initial service provision.

| Group | Example Benefits |
|---|---|
| Identity Providers (IdPs) | ● Facilitate the adoption of federated and other identity services by enabling customer insight research with their user groups in different transaction contexts.<br>● Enable new protocols such as OpenID Connect to be tested with different infrastructure providers.<br>● Enable new customer data sources to be tested |

| | |
|---|---|
| | in identity registration. |
| New Infrastructure Services (including for local/regional government; NHS; matching services (Lindley 2014); Attribute Exchanges (Wilson 2013); and others) | ● Demonstrate compliance with privacy principles to stakeholders.<br>● Demonstrate alignment with GOV.UK Verify.<br>● Test new protocols with Identity Providers, Attribute Providers and Relying Parties.<br>● Enable pilot work without exclusion from downstream procurements. |
| Relying Parties | ● Facilitate the understanding of how identity services should be deployed in the context of new and redesigned digital services.<br>● Allow related innovations, such as Attribute Exchange, to be tested alongside identity services.<br>● Avoid the need to choose suppliers before fully understanding the user needs. |

*Table 1 - Identity Supply Chain*

Collaboration between competitors is uncommon, particularly in early markets. However, all parties benefit from the adoption of an open, standards-based market where service providers compete on the service quality and not on their ability to 'lock-in' users through proprietary standards that are inoperable outside their domain.

## The Role of OIX

Standards for interoperability can, by definition, only be developed collaboratively. OIX provides a widely accepted set of rules to enable all competitor organisations to trust one another during collaborations. Of greatest sensitivity is the management of Intellectual Property Rights. In simple terms, no intellectual property is brought into OIX projects and none taken out.

Transparency is another key enabler of trust; and it is particularly important for the involvement of the public sector. To comply with European procurement laws, projects in which the public sector is involved must not provide an advantage to the project participants that would lead to unfair competition in the later market. For this reason, OIX projects are facilitated by a neutral Project Co-ordinator, and a White Paper of the project findings is produced. Presentation of projects at free-to-enter OIX meetings means that interested parties are not disadvantaged by being unable to participate.

These rules enable projects to take place with a limited number of participants and allow them to progress more rapidly as a result. No party is obliged to work with any other; projects are formed by volunteers with a common interest in working together to address a specific challenge. OIX is not a standards setting body and there is no process for adoption of a project's recommendations: the project's findings are presented to industry peers and their implementation in practice will be based on their perceived merit. Working in this way, no committee is required to sanction the creation of an OIX project.

Market participants also need to communicate their requirements and alignments to standards so that others can develop products and services that interoperate with them. OIX has developed OIXnet in order to provide Trust Framework Providers (TFPs) and Communities of Interest (COIs) a platform to develop trust through transparency and enable increased adoption through exposure. The OIXnet registry offers identity system participants the opportunity to share trust-related information about their respective systems and deployments to encourage global interoperability (Warren, 2015). OIXnet already hosts a registry of self-certified OpenID Connect implementations.

## Requirements for Test Services

One of the most pressing requirements articulated by the industry is for the availability of test services to help accelerate development and delivery of projects. As with eventual production solutions, any such test services must support the open and competitive market of solution providers - IdPs; relying parties; software, solution and infrastructure vendors; and others. In particular:

1. The overall design of any solution should support the provision of test services by multiple providers; whilst ensuring that such services conform to an agreed set of standards or specifications,.
2. Provision of a test service by a provider must not preclude that provider from participating in other procurement processes.

For example, given the presence of GOV.UK Verify, any solution should state whether they are aligned with the published standards of GOV.UK and GOV.UK Verify.

As illustrated in Figure 1, we assume an eventual business network environment in which suppliers will choose whether or not to provide test services; and suppliers that are competitive in certain environments may elect to collaborate for testing purposes in other cases.

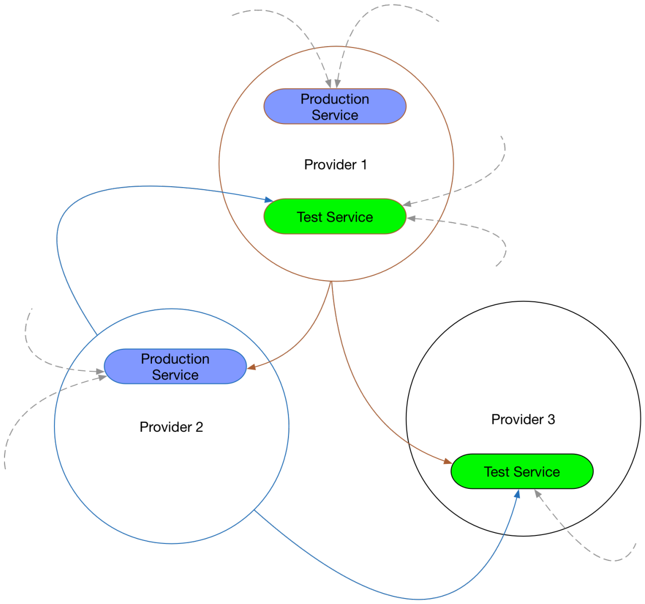

*Figure 1 - Test Infrastructure Network*

It is outside of the scope of this paper to discuss in detail how an eventual inter-hub network should be constructed. The creation of a register of services and standards would, however, accelerate other OIX projects to consider the range of questions that inter-hub networks will raise, including (but not limited to):

- The economic model, including IdPs and, potentially, hub operators;
- Privacy and security considerations;
- Technical design, implementation and maintenance; including user experience and information flow.

### Supply Chain Interactions and Constraints

The digital identity supply chain crosses the public and private sectors, and includes technical standards bodies as well as open-source projects. Over time, supply chain participants compete and co-operate in varying ways, and to varying degrees, depending on the specifics of any given project or deployment.

It is clear that not all private sector initiatives will need direct interaction with GOV.UK Verify, or other public services. However, companies providing solutions to the private sector need to ensure that policy constraints do not preclude them from subsequently providing solutions to the public sector, and vice-versa. At the same time, appropriate consideration must be given to the proper protection of intellectual property; and to the need not to compromise the potential for profitable business operations.

Any service must therefore operate within the following key constraints (illustrated in *Figure 2*):

1. The need to satisfy public procurement rules, and in particular The Public Contracts Regulation 2015, section 41.
2. The need to properly protect IPR, whilst supporting an environment conducive to joint innovation and development.
3. The need to protect personal data, and the implication of Privacy regulations and principles.
4. The proper management of any costs associated with the operation of a test infrastructure.

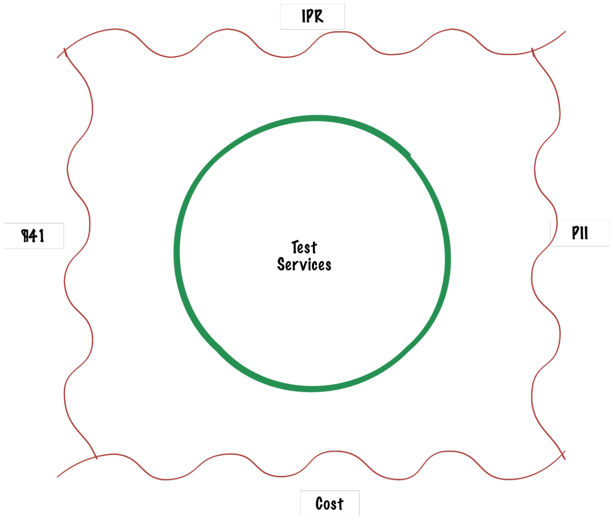

*Figure 2 - Test Service Viability Constraints*

The private sector benefits from at least a tacit imprimatur of acceptance from the Cabinet Office. In the context of GOV.UK Verify, the OIX Stage Gate process (Figure 3), which includes the involvement of the Cabinet Office, is well established as a mechanism which provides, direction as to whether a project is in alignment with GOV.UK Verify.

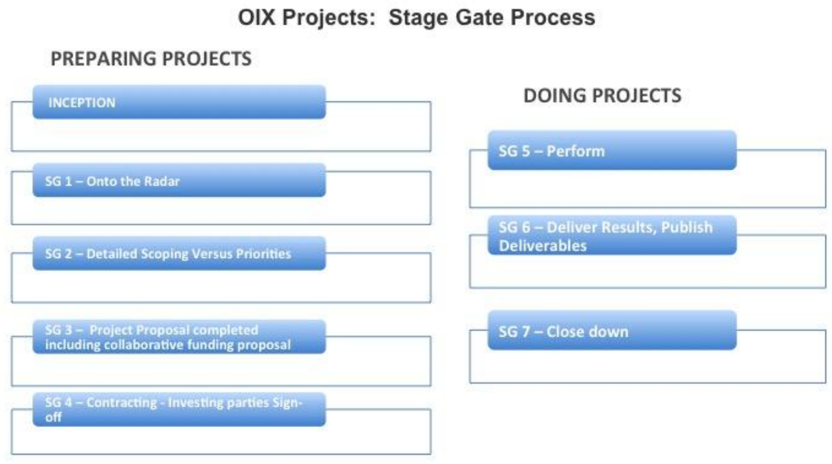
OIX Projects: Stage Gate Process
PREPARING PROJECTS
INCEPTION
SG 1 – Onto the Radar
SG 2 – Detailed Scoping Versus Priorities
SG 3 – Project Proposal completed including collaborative funding proposal
SG 4 – Contracting - Investing parties Sign-off
DOING PROJECTS
SG 5 – Perform
SG 6 – Deliver Results, Publish Deliverables
SG 7 – Close down

*Figure 3 - OIX Stage Gate process*

## Example Use-Cases

To provide better context and understanding of where a register of standards and services might help accelerate market development and adoption of services, we present overviews of two active projects. OIX proposes these projects as examples of where benefits can be achieved from the suggested extension to the OIX ruleset as they are set in highly interconnected and inter-reliant environments where multiple public and private sector stakeholders need to understand how they will align in the deployment of best practice digital identity services.

### Example 1: Identity Services for Digital Health Services

Many customers wish to be able to transact digitally with health service providers. A number of digital transactions can be done today, such as the 'Choose and Book' system that allows users to book appointments with their GP. But there are many other types of transaction that could be delivered more conveniently and efficiently through digital channels.

The National Health Service is not a single entity. It is made up of over 30,000 separate organisations that provide primary and secondary care: hospital trusts, General Practitioners, specialist service providers, and others. Each organisation is responsible for the management of sensitive personal data about its customers and has systems and processes for doing so.

Both users and health service providers worry about the privacy of personal data, yet treatment very commonly requires personal data to flow across organisational boundaries. Users increasingly expect to be able to interact with health services digitally, so the NHS must develop cross-organisational standards for identity assurance and the management of access to personal data. Systems must also be developed with a view to future standards, such as OAuth 2.0, UMA and OpenID Connect, which may have applicability in providing efficient and secure access to personal health data. (HEART, 2015)

The NHS' Health and Social Care Information Centre (HSCIC) wishes to investigate how they might leverage identity services developed to enable users to access public services provided by central government. These investigations will cover all aspects of identity assurance provision including, though not necessarily limited to:

- the customer journey;
- the technical design;
- the standards for registration of the identity;
- the 'edge' scenarios: where things go wrong - and how they are managed when they do.

The HSCIC need to start testing identity services to see how they support the many complex usages to which they might be put in a health context. The learnings from these tests need to be fed back to the new market so that it can evolve to accommodate the health sector's specific needs.

HSCIC is already collaborating directly with GOV.UK Verify in developing a private beta, where users can use GOV.UK Verify to access aspects of their health record. This project will help NHS understand how to use identity assurance to provide digital services, and the results of this beta will help inform how it might be used in wider health context.

The provision of a registry of identity standards and services - production services as well as testing tools or evaluation versions of products and services - will help HSCIC to understand more about what they need to do to align with the growing ecosystem of services in the UK; will provide easier reuse of components and services during development of the project; and will help the project more quickly demonstrate its alignment with the relevant standards and regulatory frameworks.

**Example 2: Application for a Blue Badge**

A Blue Badge enables people with severe mobility problems to park without charge or time limit in otherwise restricted on-street parking environments, and allows them to park on yellow lines for up to three hours, unless a loading ban is in place. However, the application process for a Blue Badge is complex with many personal details requested. It can take as long as 10 weeks before the successful applicant receives a Blue Badge.

An OIX project (Litton, 2014) conducted by Warwickshire County Council, Verizon, Mydex, GDS and the Department for Work and Pensions ('DWP') has developed an architectural design for an online transaction that reduces the application process to 10 minutes for the 40% of applicants who are recipients of specific benefits from the DWP. The design is based on the user's digital identity from GOV.UK Verify. It allows DWP to respond with a 'yes' or 'no' to a question asked by the local authority: "is this applicant eligible for a Blue Badge?". The DWP do not need to expose more than this minimal amount of data to the enquiring local authority.

The design of this 'attribute exchange' architecture has been developed and tested through the alpha project. However, before it can be implemented consideration needs to be given to the 60% of eligible applicants who do not receive the DWP benefits. For these people proof of eligibility needs to be provided from other authoritative sources: for example, an assessment from a mobility expert. The project now wishes to explore how these assertions of eligibility could be provided.

The technical infrastructure for the first alpha project has been developed to an open design by the private sector organisations participating in the project under the Open Identity Exchange Contributors Agreement. These arrangements safeguard all parties and enable collaborative projects to take place with costs shared across all parties.

For the next project it is intended that the components built for the first alpha project should be reused. Additional components from health service suppliers can be designed and incorporated into the test infrastructure as needed. The provision of a registry of compliant standards and services - production services as well as testing tools or evaluation versions of products and services - will make it easier to adopt such components during the project; will accelerate the design and development of the project; and will allow the project more quickly to demonstrate its own alignment with the relevant standards and regulatory frameworks.

### A Registry of Standards and Services

In the open digital identity solutions market, test and production services will be provided by many suppliers - a single, central supplier will be unable to support the breadth of technical requirements eventually envisaged; and central provision would be cost-prohibitive. Where appropriate, services must be able to demonstrate their alignment with the rest of the marketplace and the principles by which it and its ecosystem operate. In order to contribute to collaborative innovation and development across the supply chain, service providers need reassurance that their IP is properly protected and that test service provision will support - not inhibit - commercial endeavour.

An open and trusted registry of standards and services, supported by a lightweight and agile self-certification scheme for providers, would provide a mechanism for service providers to advertise availability of the service in a way which is trusted by their customers.

In order to meet burgeoning demand from the community in a resonable timeframe it would be sensible to leverage an existing registry and set of trust and collaboration principles that are already widely understood and accepted within the ecosystem, and by GOV.UK Verify.

Providing the registry and the self-certification process in conjunction with the well-established OIX stage gate framework will result in greater transparency to the alignment of any particular service with existing standards and frameworks, and the principles by which the particular ecosystem already operates.

A logical outcome, therefore, is to consider the provision of a public registry of self-certified services via OIXnet, and the integration of the registration process with the existing OIX stage gate framework - illustrated in Figure 4. OIX UK will establish the initial categories and criteria for self-certification; it is envisaged that, as the community introduces new service capabilities, this learning will be fed back into the system to allow for additional categories and criteria for registration and self-certification.

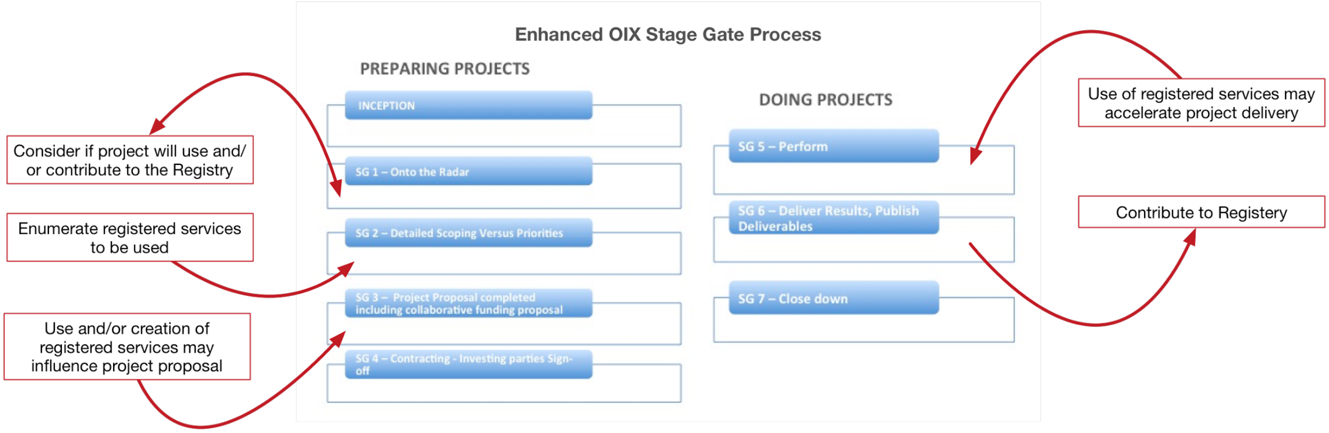
Enhanced OIX Stage Gate Process
PREPARING PROJECTS
INCEPTION
SG 1 – Onto the Radar
SG 2 – Detailed Scoping Versus Priorities
SG 3 – Project Proposal completed including collaborative funding proposal
SG 4 – Contracting - Investing parties Sign-off
DOING PROJECTS
SG 5 – Perform
SG 6 – Deliver Results, Publish Deliverables
SG 7 – Close down
Consider if project will use and/ or contribute to the Registry
Enumerate registered services to be used
Use and/or creation of registered services may influence project proposal
Use of registered services may accelerate project delivery
Contribute to Registery

*Figure 4 - Enhanced OIX Stage Gate process*

In order to enable initial provision of the registry and the supporting self-certification process to the community in a reasonable timeframe, we propose a phased introduction of capability certification, with on-going and iterative certification releases.

## Phasing and Timelines

To help set expectations with the community, an initial progress timeline is proposed in Table 2. This timeline supports a prompt initial release for the proposed registry in response to the demand we have already heard from the community; meeting the milestones described requires appropriate constraints on the initial capabilities that are to be certified.

| When | Who | What |
|---|---|---|
| Autumn 2015 | OIX UK | Establish registry<br>Finalise phase 1 certification criteria |
| Autumn 2015 | Phase 1 providers | Submit standards and service descriptions |
| Winter 2015 | **Phase 1 Registry Available** | Providers self-certify<br>Phase 1 services available for use |
| Winter 2015 | OIX UK | Develop means for establishing more formal certification, for example reaching out to UKAS |
| Early 2016 | **Phase 2 Registry Available** | Providers self-certify<br>Phase 2 services available for use |
| 2016 onwards | Ongoing development of new certification criteria; on-boarding of new test service providers | |

*Table 2 - Proposed Phasing & Timelines*

**Phasing: Just Enough**

The initial phase of certification should support a minimal set of capabilities which are sufficient for the highest priority initial testing solutions that the community requires, and postpones more complex and/or contentious areas which - whilst clearly important to the community - will require more time to properly develop. Appendix 1 lays out a series of capabilities that have been explicitly requested by the community and/or are suggested by the use-cases; and proposes appropriate release phasing based on rough assessments of the complexity of providing such capabilities in a secure and scalable way.

## Conclusion

Feedback from the identity supply chain strongly supports the establishing of a registry of standards and services to help accelerate market growth. Accelerating market growth is in the interest of all participants in the ecosystem. Creating a process that follows well-established open market principles is the quickest and most sustainable way to provide the facilities required. OIX UK, via OIXnet, can provide a service registry and self-certification programme with well-understood rules of operation, which allow for proper commercial engagement and encourage ongoing innovation through cross-industry collaboration. The model proposed herein allows for an initial programme to be available - and for the first self-certified services to be operational - by the end of 2015.

The design requirements we have established suggest a set of guidelines for the operation of OIX projects:

1. **OIX Mandate**: OIX collaborative projects are conducted to progress the adoption of open identity services to catalyse the local markets that interoperate with global ecosystems.
2. **Voluntary Participation**: no organisation is obliged to work together with any other organisation in an OIX project and may withdraw its support and name at any time.
3. **Objective**: the intention of the incubation of services through OIX projects is to give them the opportunity for commercial adoption.
4. I**ntellectual Property**: all project participants must sign the Open Identity Exchange Contributor Agreement.
5. **Transparency**: Project participants should openly declare what they contribute and what they desire to achieve from a collaboration. Every project will have an independent coordinator, a white paper published on the OIX Website, and its findings presented and discussed at OIX Workshops.
6. **Procurement**: participation in an OIX project should not impact on the ability to participate in future procurements from the public or the private sector.
7. **Process**: Projects will follow the OIX Stage Gate process for projects to ensure that OIX rules are followed and that all stakeholders - including Cabinet Office, supply chain participants and eventual customers - are appropriately involved at the relevant stage.
8. **Safety First:** Projects will not use live data.
9. **Practicality**: Projects should be: short term; focused and limited in scope; self-funding.
10. **Privacy**: All projects should be reviewed against the principles set out by the Privacy & Consumer Advisory Group.

Such guidelines serve to nurture trust by providing a clear set of boundaries within which the registry and process is understood by all participants to operate. Just as the market itself is evolving, so the guidelines for operation will need regular review and evolution in order that the process can continue to be relevant and useful.

In keeping with the OIX process, the next step should be to test the recommendations of this paper in the context of a pilot project. Doing so will allow the self-certification criteria, the guidelines and the process to be developed and refined to optimally meet requirements across both public and private sector participants.

The design principles for the proposed registry support the general requirements of the UK market. They are sufficiently flexible to allow the registry to be extended to support related EU requirements. The design may serve market needs in other geographies; eventually providing a global platform for the incubation of integration and interoperability services.

Demand for services that improve convenience, user experience **and** security is at an all-time high, and will continue to grow - in the UK and beyond - as citizens and organisations become ever-more connected and digitally savvy. It is in the industry's interest to respond appropriately and rapidly to this demand; and the proposed test infrastructure process will do much to support this response.

## Appendix I : Initial Requirements and Proposed Phasing

This appendix describes capabilities and services that have been explicitly requested by the community and/or are suggested by the use-cases. These are described in Table 3, along with a proposal for release phasing based on rough assessments of the complexity of providing such capabilities in a secure and scalable way.

It is expected that the details of this phasing will change as the registry evolves. In particular, providers might have a specific commercial or technical interest in accelerating availability of certain test capabilities, which is certainly encouraged, and supported by the model proposed. For instance, test services might certify against a minimum core set of functionality, but could also offer documented extensions to the core functionality; these extensions may then be considered for formal inclusion in the certification criteria or options in later phases of the registry.

| Capability | Suggested Release | Notes |
|---|---|---|
| Basic emulation of GOV.UK Verify connection by Relying Parties; with limited cryptography requirements[2] | Phase 1 | As described in the on-boarding documents (GOV.UK Verify 2015) |
| Enhanced cryptography for basic emulation | Phase 2 | If required |
| Basic test identity data | Phase 1 | It is not recommended that test services handle real identity data[3] |
| Enhanced test identity data | Phase 2+ | Consider providing a well-defined set of test identities that could also encapsulate specific areas of technical challenge (thick file, thin file, no file etc.) in Phase 2, if viable |
| IdP Connection | Phase 2+ | Initial services should not attempt to connect through to the IdPs. This functionality might be considered for Phase 2 or later |
| Matching Data Service | Phase 2 | This is an area that is known to be a significant challenge to parties connecting to hubs. It is not yet clear how a test service could help with this, but it might be possible (for example) to host a working, sample matching data service and/or adapter, with published code, as a reference example that RPs and infrastructure vendors could use |

[2] Limiting cryptography requirements will accelerate deployment and simplify use; this must be balanced against the need to properly align with GOV.UK Verify and with the IDAP SAML profile.

[3] Attention must be given to the core privacy requirements established by GOV.UK Verify (Hughes 2015), and to the PCAG Identity Assurance Principles.

| | | |
|---|---|---|
| User Experience Testing | Phase 2 | See later section on Customer Insight Research |
| New Protocol Support | Phase 2+ | Support for ‘overlay’ protocols such as OpenID Connect, UMA etc. |
| Attribute Exchange | Phase 2 | Support for attribute exchange testing |

*Table 3 - Proposed Phasing*

**On Customer Insight Research**

Customer Insight Research is a critical part of almost every OIX project, and a key differentiator in ensuring that projects are likely to be successful once rolled out to real-world deployments.

It is clear that the availability of test infrastructure capabilities would be of major help to developing Customer Insight and UX/UI testing facilities. This must, however, be balanced against the additional complexity that such research implies for the test services. It is therefore proposed that support for a UI/UX testing certification should be prioritised for Phase 2 deployment; but that work may begin on planning for this during Phase 1 to allow sufficient time to fully develop the requirements. We expect that customer insight research will continue as normal pending availability of the certification process.

## Works Cited

**Dunne, Joseph.** "Mapping the Cost of Non-Europe, 2014-2019" European Added Value Unit – European Parliament PE 563.350 2nd Edition, July 2014. Web. 16 July 2015

**Litton, Ian and Rob Laurence.** "Can Attribute Provision, Together with Identity Assurance, Transform Local Government Services." OIX UK, Aug. 2014. Web. 26 June 2015.

**Lindley, Emma.** "Data Matching in the Identity Ecosystem." OIX UK, 2014. Web. 26 June 2015.

**"GOV.UK Verify Onboarding Guide."** *GOV.UK Verify Onboarding Guide — GOV.UK Verify Documentation.* Web. 26 June 2015.

**"HEART WG."** OpenID Foundation. Web. 26 June 2015.

**Hughes, Janet.** "GOV.UK Verify Hub - Privacy Aspects." *Identity Assurance and GOV.UK Verify*. GOV.UK, 22 June 2015. Web. 26 June 2015.

**Out-law.com.** "'Digital Passport' in Financial Services and Government's 'Verify' Regime Should 'run along the Same Track', Says Expert." *Out-law.com*. Pinsent Masons, 30 Mar. 2015. Web. 26 June 2015.

**PCAG.** "Identity Assurance Principles." 30 Sept. 2014. Web. 26 June 2015.

**TSIP.** "Saving Our Financial Future." *THE SAVINGS AND INVESTMENTS POLICY PROJECT* (n.d.). Web. 26 June 2015.

**Warren, Hal.** "The Value of OIXnet." Feb. 2015. Web. 26 June 2015.

**Wilson, Steve.** "Attribute Exchange Networks: New Infrastructure for Digital Business." OIX UK, Oct. 2013. Web. 26 June 2015