DISCOVERING THE NEEDS FOR UK IDENTITY ASSURANCE

THE OPEN IDENTITY EXCHANGE | INNOVATE IDENTITY

Emma Lindley

September 2015

Executive Summary

The UK currently has a wide variety of online identity requirements, sector specific standards and point solutions. In order to understand the overall UK market needs better, the Open Identity Exchange (OIX) has been asked by its members to run a discovery exercise during 2015 to understand what the private sector needs are for digital identity services, how these relate to central government needs, and what questions would arise when considering the potential development of sector-based and cross-sector approaches to identity assurance.

This approach will help inform thinking in both the public and private sectors about the future development of this market.

As part of this work, OIX would like to understand the extent to which the capabilities government and certified companies have developed for UK digital identity, could usefully be applied to meet needs in the private sector, and what the questions and issues would be in that scenario.

As the initial phase to this work in May 2015, led by the OIX and facilitated by KPMG, a workshop took place with senior representatives of some of the UK's biggest organisations from a wide cross section of industries. Major banks, telecoms providers, retailers, local authorities, online gambling providers, identity providers, central government, representatives from the sharing economy, industry associations and subject matter experts all joined together to answer questions relating to the UK digital identity ecosystem growth.

The results of this workshop found there was an agreement that the UK market currently has a wide range of identity needs, and that there is currently a fragmented approach to satisfy those needs across industry sectors. The participants in the workshop identified that their organisations would like to explore a cross sector approach to identity needs in the UK. Potential benefits to a cross sector model were identified; these included increased customer acquisition and revenue, improved customer experience, reduced cost of compliance and reduced fraud.

This white paper provides an overview of the initial workshop including the process and participants. It also sets out a scope and structure for how this work will be expanded beyond those organisations that were represented in May 2015, to understand the wider identity needs across the UK. Industry participation in this project is encouraged, and details of how to engage in this process can be found in the conclusions section of this document.

Table of Contents

1. Background to the UK Market

UK Internet users are up 2.4 million from 2013[1] and online retail sales are predicted to reach £52.25bn this year. Over 50% of adults now bank online, growing from 30% in 2007[3], and those online banking customers now make over 5 million of those transactions through mobile apps[4]. With the number of UK citizens who have never used the Internet down 1.2 million since 2013,[5] it has become abundantly clear that the shift online is not showing signs of slowing down.

Users are attracted to the online experience because it is quicker, and more convenient. For organisations, the online shift creates ways to attract new customers, increase revenue and cut the cost of manual paper-based processes.

For the UK, the digital shift is a platform for growth and has fast become a vital part of our economy. It enables the UK to compete with other countries in a way we have never done before, and projects us forward to become one of the leading digital economies worldwide.

However, with this move online and more businesses and consumers transacting in this way, fraud is also booming. Cifas reported this year that overall fraud is still on the rise, with 41% of all fraud being identity fraud and the numbers are still increasing.[6]

Hackers are stealing personal data at an increasing rate[7] in the knowledge that this personal data has value in enabling access to consumer and business services where money or goods can be stolen.

Additionally, in the race to create value through marketing, global corporations are increasingly accused of requesting too much of, exploiting, and in some cases selling, individual's personal data without knowledge or consent. Governments throughout the EU

are raising concerns about this and in some cases raising legal action to protect citizens.[8]

UK and EU research reveals that concerns about privacy and the protection of personal data are increasingly of importance to the public. This perceived lack of control over their data, along with high profile losses of personal data by organisations, add to the feelings of concern. [9]

Research by Symantec showed 57% of users are worried that their personal data was not being kept safe by organisations, and 88% felt that keeping data safe and secure was a factor of importance when choosing an organisation to shop with or use.[10]

Increasing and new regulations such as the 4th Money Laundering Directive[11] and PSD2[12] mean more organisations than ever before have to have higher assurance of their customers' identity.

This increased fraud, compromise of personal information[13] and a lack of trust is damaging for not only consumers and businesses, but for the entire UK economy. It threatens to slow digital growth and to affect the UK's position in the global market place.

Being able to know whom we are dealing with online, in a safe secure way whilst protecting privacy, is important to ensuring users and organisations can continue to trust and transact online. How the UK deals with this issue will be paramount to its digital growth.

The current marketplace is fragmented, any standards or regulation that do exist differ from sector to sector meaning there is no consistent approach to addressing the problem of online identity.

In relation to solving the issue, there are many point solutions in the emerging marketplace of identity verification and authentication services, but generally they are not user centric. Users may have limited or no control over their personal data, and this existing marketplace means consumers have to have their identity verified many multiples of times. In summary the current UK identity ecosystem is sub-optimal.

New models such as identity federation, aim to address the challenges set out above. There are a number of sectors, such as the biopharmaceutical industry and European Markets e.g. Denmark amongst others, which have adopted variations of a federated approach to identity and reported cost savings and fraud reduction.

There are a number of different ways in which a federated approach could be adopted. However, the core principle is that trust frameworks are in place that allow the user to reuse identity services across

different transactional contexts. In simple terms: verify once, use many times.

In the UK, the first federated model exists through GOV.UK Verify. This model assumes a market of open standards which can be used by the different service providers. It also supports the principles that the Information Commissioner's Office (ICO) has laid out for consumer protection and privacy.

However, the GOV.UK Verify model exists for public services delivered by central government. Would a federated identity model work for the private sector too? If so, how could it be implemented, what would be the benefits and challenges of such an approach?

1. ONS UK Internet Use http://visual.ons.gov.uk/internet-use/
2. UK Retail Online Sales https://econsultancy.com/blog/66007-uk-online-retail-sales-to-reach-52-25bn-in-2015-report/
3. This is Money http://www.thisismoney.co.uk/money/news/article-2719087/ONS-Three-quarters-Britons-shop-online-half-use-internet-banking.html
4. BBC Mobile Banking http://www.bbc.co.uk/news/business-26816148
5. ONS UK Internet Use http://visual.ons.gov.uk/internet-use/
6. Cifas Fraudscape 2015 - https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-A5%20Fraudscape%20insert%20LOW%20RES.pdf
7. Hackers steal 650 million http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html
8. Belgian government takes Facebook to court. http://www.computing.co.uk/ctg/news/2413350/belgian-privacy-commission-takes-facebook-to-court-over-privacy
9. ICO, Data Protection Rights: What the public want and what the public want from Data Protection Authorities, May 2015 https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf
10. Symantec - State of Privacy Report 2015 (February 2015) http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf
11. 4th Money Laundering Directive http://www.sbcnews.co.uk/europe/2015/06/17/eu-publishes-4th-anti-money-laundering-directive/
12. PSD2 http://ec.europa.eu/finance/payments/framework/index_en.htm
13. Carphone Warehouse 2.4 Million Personal Records Compromised http://www.wired.co.uk/news/archive/2015-08/10/carphone-warehouse-hack-data-breach

2. Background to this Project

Over the past few years the Cabinet Office has developed GOV.UK Verify from within its Government Digital Service. GOV.UK Verify has created a federation between identity services supplied by the private sector and public service providers from across central government departments. GOV.UK Verify allows users of public services to create a privacy protecting, secure digital identity through a private sector organisation when accessing a digital public service.

GOV.UK Verify will be the first UK population scale deployment of a high assurance digital identity scheme. Beyond reducing costs and protecting the privacy and security of British citizens, it has an aspiration to be a catalyst that can help unlock data assets across industry sectors to improve citizen inclusion in online services.

Federated identity systems are different from the many point solutions available today, and work on the premise of verify once, use many times. With GOV.UK Verify the user should not have to go through separate registration processes for each part of central government with which he/she interacts digitally. The aim is to make things quicker, easier and more secure for users.

Whilst in the longer term benefits are clear, creation of federated identity systems is complex in the short term, and requires a high degree of collaboration across organisations. So what are the private sector needs in relation to identity assurance?

There are requirements in many private sector verticals from 'Know Your Customer' in finance, through to 'Customer Due Diligence' in the legal profession, which are currently addressed by point solutions. Does the private sector want to continue with the current sector specific approach? Would the private sector want to adopt a cross industry or federated approach to identity? If the private sector favoured a cross industry approach, what would be the benefits and also the challenges?

OIX UK has developed a process for investigating unknowns in the emerging identity ecosystem through open collaboration, working with multiple stakeholders from both public and private sector. This process is described on the OIX UK website, and forms a series of projects called discovery, alpha and beta projects. This discovery project seeks to understand the answers from industry to the questions posed above and others.

3. Project Scope - Identity

The scope for this discovery project is focussed on the needs within identity and not the wider scope of attributes. Identity can be defined as who the person is. For a natural person this is their identity attributes; these are usually represented by their name, date of birth and address. Trusted attributes may be associated with a person's verified identity for the purpose of eligibility. Examples of this include their qualifications, geographical location, etc.

Another example of an attribute which is often associated with identity is age checking. In order to gain a simple yes/no response to an "are you over 18 question" to access age restricted goods or services, does not require to know someone's full identity details. Whilst not covered in the scope of this project. the work on age is important and is therefore being led by the policy team in the Department of Media Culture and Sport (DCMS) who are currently analysing the needs for age attributes within the UK.

There are organisations who require to know the identity *and* the date of birth of an individual for regulatory requirements, Know Your Customer (KYC) or fraud prevention. These companies include online gambling companies and retailers respectively. These organisations are included in the scope of work within this discovery project.

4. Process and Participants

OIX UK engaged KPMG to run an initial discovery workshop on the 28th of May 2015 to bring sectors from across UK organisations, both public and private. This initial workshop was focused on organisational needs in identity rather than end user needs. In order to facilitate this workshop, KPMG used a model they call U-Collaborate, which is designed to allow competing organisations to work together and reach consensus on complex topics, such as digital identity.

The sectors represented included various organisations from financial services, telecoms, retailers, online gambling, central government, local government, sharing economy, identity providers and subject matter experts.

OIX used the workshop to engage with the participants to work through the details of four potential market models, to understand if the UK private sector might want to move from the market as is today, to a future vision of collaboration around needs for identity assurance services.

The four models of identity were discussed and are later described in this document. The process aimed to find a consensus about which market model/s would work the best for all participants across public and private sector. This consensus was reached by identifying the model with the most overall benefits.

5. UK Identity Market Models

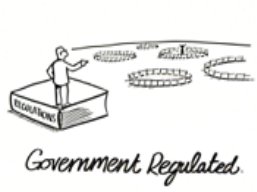
During the cross sector workshop, four generic market models were discussed in groups. These models describe how the UK identity market works today in its various forms. The aim of the exercise was to discuss both the benefits and challenges of each, with a view for the participants to reach consensus on a model, or models, which might work best for the UK, including the option of staying with the status quo.

Users have many multiples of login credentials. There are many point solutions for identity verification and authentication, but they are not interoperable or open. Users have to identify themselves in many different ways, multiple times.

There are federated silos which are driven by the dominant internet players such as Facebook, Google and Apple. Users have little or no control over their personal data. There is a maximum of personal data transferred both inside and outside of the UK, this data is transferred often without users understanding how they have consented to the transfer.

This is an "Industry Silo" or segmented market. In this market, industry 'solves' identity federation for their sector; e.g. government (GOV.UK Verify) or the US BioPharma.

Users require a digital identity for each silo which works for that silo or sector, but they do not federate between. Each silo has its own governance body, and there is no standardisation between each one in respect to privacy, user control or assurance levels.



This market is a "Government Regulated" market. Regulations are applied to the increasing number of industry sectors to prevent abuse of personal data and increase trustworthiness of digital transactions.

Regulations drive identity silos for each segment e.g. financial services identity silo, gambling industry identity silo, legal sector identity silo etc.

This is "Cross Industry" market, it has agreed interoperable identity standards and a governance framework. It has a widely adopted approach to identity assurance across multiple industry sectors.

Users have few digital identities and can use them across all transactions and sectors as they wish. Users are in control of their identity and associated data. Parallels can be drawn with schemes such as Visa and MasterCard when thinking about cross industry models in operation today.

6. Findings from the Workshop

Consensus was reached on the "Cross Industry" model. This is described as a market with agreed interoperable identity standards, a consistent approach and a governance framework.

The table shows just a few of the high level benefits and challenges that were discussed on the day about a cross industry model and how consensus was reached. Below is a comment from one of the participants taken as part of the project:

"Of the people that come to our site and attempt registration, around 35 - 40% fail the Know Your Customer process and we have to turn them away. This hurts our business two-fold; through wasted cost of acquisition, and the opportunity cost of lost business. For us having a cross industry digital identity scheme could mean more customers, more revenue and we would save money."
Alex Letts - Ffrees Family Finance Ltd

Benefits to Organisations

Description	Resulting Benefit through Industry Collaboration
• Manual paper based processes can be replaced with online options • Allow focus on developing core products or services rather than spending time on verifying customer identity • The cost of verifying an identity is usually highest at registration, if identities could be used across sectors, verify once use many times, this would have a positive impact	Cost savings through improved operational efficiencies
• Verifying identity first time can be a real challenge particularly for those who do not have an existing online footprint or identity documents. If the customer already had their identity verified	More customers, increased revenue and improved customer experience

elsewhere and it could be trusted, this would remove barriers, enable them to transact freely and create a better customer experience • Transfer existing customers to new products with less barriers	
• Higher assurance that the identity was real and belonged to the person presenting it	Reduce fraud and bottom line cost
• Having to comply with regulations is a burden for businesses • Holding customer data is a security risk and cost • Fraudsters exploit the differences in standards (regulatory and risk vectors) across sectors	Reduce the cost of compliance through common standards Reduce fraud and risk across sectors through consistent approach

Challenges

So far the process and participants have identified the challenges listed below. The purpose of the expansion of the discovery project is to gain more insight from a wider group of participants to flesh out these questions in more detail.

Challenge	**Resulting Questions**
No rules	There are no rules on how to do a cross industry model. How would work start? Would there need to be a set of scheme rules to support the commercial and legal aspects of the model?
Liabilities	Who is liable in a cross industry model?
Commercials	How does money flow in a cross industry interoperability model? Who pays for identities to be verified? Who pays for the setup of such a scheme?
Brand	How is a cross industry model branded? How would this affect company brands?
Technical	What technical standards would be required to support an interoperable framework? Would technology be needed to support a cross industry model? How would it be deployed?

Differing identity level requirements and regulation	Different sectors have different requirements for identity, for example 'Know Your Customer' checks in finance are different to identity verification checks in retail, and how would a set of "standards" deal with this?

The parties at the workshop recognised that there were benefits from an open standards based interoperable market for digital identity.

Cross industry or interoperable markets ultimately stand to return the highest gains, but they are the hardest to do and there are many challenges. How can a group of industry rivals find common ground to collaborate and where to compete? The private sector is very diverse and requirements differ from sector to sector. The pace of change is dramatic, therefore achieving the desired goal will be complex. The starting point is therefore to identify and analyse needs.

7. High Level UK Identity Requirements

The list below is not exhaustive but highlights some of the existing and new requirements within the private sector where assured identities are required. It is with these industries and others that this project seeks to understand the requirements of in more detail.

Sector	Identity Requirements	Relevant Regulation or Guidance or Information
Financial Services (including banking, investments, insurance etc)	Financial Service Providers have to establish the identity of the customer under KYC and AML regulations	Financial Conduct Authority
Pre-Employment Screening (Background screening used by financial services, NHS, education, taxi services, recruitment agencies etc)	Identity and Criminal Record Checks	Disclosures and Barring
Retail	Many retail organisations try to establish the identity of an individual in an attempt to prevent fraud. For some products they also have to verify that the individual is over a certain age. Age checking is an attribute.	Video Recordings Act 1984 Children and Young Persons (Protection From Tobacco) Act 1991 Offensive Weapons Act 1996 Cigarette Lighter Refill (Safety) Regulations 1999 Licensing Act 2003 Fireworks Regulations 2004 Pyrotechnic Articles (Safety) Regulations 2010
Online Gambling		Gambling Act 2005

	Online gambling providers have to establish the identity of the customer under KYC and AML regulations. Gambling companies also have to verify that the individual is over 18. Age checking is an attribute.	
Peer to Peer	Identity for fraud prevention	Government Response to the Sharing Economy Report 2014
Landlord & Tenant	Identity Checking. These organisations also have to verify that the applicant has the right to rent the property. Establishing the right to rent is an attribute. For some products they also have to verify that the individual is over 18. Age checking is an attribute.	GOV.UK Right to rent immigration checks: landlords' code of practice
Legal and Professional	Customer Identity Checking (Customer Due Diligence)	The Law Society Guidance

8. Conclusions and Next Steps

So what is the opportunity for collaboration or co-opetition? Can the UK create a market where the public and private sector work together to create trustworthy digital infrastructures for identity? And how can organisations who are seemingly competitors, work together on this complex subject?

In order to accelerate the development of the investigation into this optimised identity market, immediately address some of the challenges that were identified in the initial workshop, and to identify what sectors would specifically want from a collaborative digital identity ecosystem, the OIX has developed a further scope of work to be completed during September and October 2015.

The scope of work is defined in two stages:

1. Further identification of industry market needs
2. Identification and confirmation of user needs

Industry needs will be assessed through a survey, the details of which can be found in the appendix to this document. The responses will be collated and analysed by the type and size of organisation.

A series of sector specific workshops will also be held for financial services, telecoms, the sharing economy, the gambling sector, employment sector, privacy groups, identity providers and others.

These workshops will be held to help participants understand the context to the survey in relation to that specific sector, answer any questions relating to the survey and to bring the level of understanding up in relation to the potential cross sector benefits of collaboration around identity services identified in the initial industry workshop in May 2015.

Identification of user needs will be addressed through user research in a test lab. This research will take real potential users of a cross industry approach to identity services, and understand their attitudes to a proposed federated identity ecosystem.

All findings will be collated and presented in a white paper at the end of the process in November 2015 and the white paper will be published on the OIX website.

The report will make specific conclusions and define a practical pathway about how this important topic will progress.

If you would like to be involved in the project, attend the workshops and respond to the survey please email oixuk@openidentityexchange.org and you will be sent the details for the workshops and a link to the online survey.

APPENDIX

The survey questions below will be either a range between 0-7, a YES / NO or open text response.

1. IDENTITY MARKET NEEDS

- In what circumstances does your organisation need to know who the customer is?
- How do you currently initially identify your customers and how do you authenticate them when they use digital services?

2. IDENTITY MARKET DEVELOPMENT

- In your own words, if the identity assurance market develops successfully in the next 3 years, what will be the 3 most important characteristics of the market at that point?
- In your opinion what are the 3 main opportunities from the rapid and successful development of this identity market in the UK?
- In your opinion what are the 3 main barriers to the rapid acceleration of a UK identity market?
- Is there anything else you would like to add?

3. STANDARDS

The Government has developed a range of standards covering different aspects of identity assurance, and GOV.UK Verify has been built to meet those standards. These standards are designed to enable diverse technical solutions to be developed that are interoperable and meet common levels of assurance.

You can read the standards being used by GOV.UK Verify here:

Title	Background
GPG43	http://bit.ly/1i5iOLB
GPG44	http://bit.ly/1CNt4vH
GPG45	http://bit.ly/1BSkznK
IPV Operations Manual	http://bit.ly/1NXQfJW

Questions:

- Upon reading the Good Practice Guides 43, 44 and 45 and the operations manual how well would you say you understand them?
- How relevant are these documents to your industry?
- Does your industry have a standard for identity proofing and verification and / or authentication?
- Does your organisation need to verify other attributes about customers, apart from their identity?
- Please list any transactions you are responsible for that you have assessed as requiring LOA2 identity proofing and verification as defined by government standards.
- What further checks would you need to do, if any, to reach the required level of identity assurance for these transactions?

4. CERTIFICATION

GOV.UK Verify identity scheme requires companies to be certified. Certification adds costs but provides assurance that standards are being met by the certified organisations. Different mechanisms of certification exist; certification by a third party/audit amongst others.

Title	URL Link
What it means to be certified	http://bit.ly/1Kvo1bb

To be able to trust a digital identity asserted by a third party organisation, would this organisation have to be:

- independently certified against a set of standards for identity proofing and verification, and authentication
- self-certified under an industry scheme

Questions:

- How well do you understand the certification requirements for government identity providers?
- How important is it for you, in consuming identity assurance services from third parties, that providers of identity assurance are certified as meeting defined standards?
- As a provider of identity assurance services, how valuable is it for you to be certified as meeting defined standards?

- What do you think needs to happen next in the development of the market for certification services?

5. BRANDING

Brands have an important role to play in the communication of trust. They are also an important marketing tool for organisations. But the appearance of too many logos and symbols within a digital transaction can have the impact of confusing the user.

Title	URL Link
Trustmarks	http://bit.ly/1IRQyly
Pension Finder	http://bit.ly/1SPNv4F

Questions:

- How important is a cross industry brand / logo to communicate trust in a digital transaction?
- How valuable would it be for the GOV.UK Verify brand / logo to play any part in private sector digital transactions?
- How appropriate would it be for the GOV.UK Verify brand / logo to play any part in private sector digital transactions?
- Please explain your answer to question 2 and 3

6. IDENTITY ASSURANCE PRINCIPLES

A Privacy and Consumer Advisory Group (PCAG) was set up in 2012 to review the evolution and development of GOV.UK Verify. It has developed a number of identity assurance principles, a link to which can be found in the table below along with the privacy group blog. The UK Information Commissioner is part of PCAG and ensures work with the group to ensure that privacy is not a fixed deliverable, but a fundamental quality of the identity assurance programme, and GOV.UK Verify builds and maintains users' confidence that their privacy will be protected.

Title	URL Link
The 9 Privacy Principles	http://bit.ly/1IOmBmx
GDS Blog about PCAG	http://bit.ly/1NFhRql

Questions:

- Upon reading the 9 Privacy Principles, how well would you say you understand them?
- How important is it to have a published set of privacy principles for providers of identity assurance services?
- What is the best way for users to be assured that providers are meeting stated privacy principles?
- How relevant are the privacy standards to your industry?
    - If not, what would need to change to make them relevant?
- Outside the Data Protection Act, does your industry have a standard or guidelines for privacy?
- Do you think your industry would benefit from adopting the 9 Identity Assurance Principles?

7. POTENTIAL CROSS SECTOR VALUE

Within the initial industry workshop there were a number of benefits and challenges identified.
One of the challenges is the people who have difficulty establishing a digital identity at a high level of assurance because of the lack of data sources and infrastructure available to verify them. This is costly for organisations and a poor experience for users. A collaborative cross industry model would mean that organisations who have an existing relationship with those people, e.g. a mobile network operator, would be able to provide them with a digital identity. Then, through a federated cross industry model, an identity created in one context, e.g. with a mobile operator, could be used in another context, e.g. with a bank. A common approach to standards to identity across industry would span across fraud and risk vectors, potentially reducing the chance for fraudsters to exploit the different levels of identity assurance there are today.

Below are some of the white papers relating to the benefits and potential challenges around this topic:

Title	URL Link
Economics of Identity	http://bit.ly/1pbTFA6
Bridging the Digital Divide	http://bit.ly/1Kvola4
Investigating Challenges in Digital Identity	http://bit.ly/1GGZ60m
Digital Sources of Trust 1 & 2	http://bit.ly/1QPyimC

Questions:

- How valuable do you think it would it be to explore a cross sector approach?
- What do you think the main benefits would be of a cross sector approach?
- What would be the challenges of a cross-sector approach?
- Does your organisation have difficulty verifying customers?
- What characterises customers whose identities are difficult to verify?
- If these customers who were difficult to verify had a digital identity, what value would this have to your organisation?