UK PRIVATE SECTOR NEEDS FOR IDENTITY ASSURANCE

REPORT

THE OPEN IDENTITY EXCHANGE | INNOVATE IDENTITY

June 2016

Executive Summary

The UK economy has a fragmented approach to online identity, with many different regulations, requirements and methods. This makes the experience for users complex and users have very little control over how their personal data and identity is managed. For organisations it means they often try to solve the issue of online identity in their own industry sector, but fraud levels are still rising and there are segments of the population that cannot be verified online, creating operational inefficiencies and increasing cost.

This challenge is shared by organisations in both the public and private sector, therefore in order to progress this critical topic, the Open Identity Exchange has run two discovery projects to look at UK Identity Assurance needs to understand if there is an appetite for collaboration across private and public sector to solve the issue of online identity in the UK. A collaboration of this type would aim to solve identity across sector, rather than in sector silos, and would ensure that no one entity public or private sector owns the UK citizen's identity, putting consent and control back in the hands of the citizen.

This document reports in the second phase which was much wider reaching than the first, and included feedback from 80 organisations. Questions were asked generally about the market, and specifically about standards, certification, privacy and brand, as well as understanding the appetite to work collaboratively to solve some of the issues around identity.

These questions were asked to understand the potential reuse of GOV.UK Verify as there are a range of options about which part/s could be make available to the private sector. The survey was designed to understand the private sector's view on the value of each of those as well as their views on the market generally.

Financial services had the most respondents overall, followed by the sharing economy, identity providers and online gambling.

Respondents had a range of views around these topics, from majority acceptance on some, e.g. privacy principles, to mixed opinion on others, e.g. a GOV.UK brand to be used in the private sector. Some areas require further education, such as standards and certification as this was less well understood versus brand and privacy and likely impacted the survey responses in these areas. Although in some areas, for example certification, despite the lower level of understanding, respondents still felt it was important.

Many sectors cited that they would need access to additional attributes in order to allow them to meet their compliance requirements and verify the customers in their sector over and above the Good Practice Guide standards. This demonstrates not only the need for new sources of attribute data to be made available, but the requirement for those attributes to be exchanged in a transparent way, allowing the user to be at the heart of the transaction providing consent.

The main conclusion from this project is that there is significant appetite to pursue a cross industry collaboration to identity assurance needs, with 81% of organisations that responded to this question wanting to move forward with a cross industry approach.

There were many perceived benefits of collaboration, such as improved customer experience, time and cost savings, and portability. The project also exposed the challenges that could be faced, and would need to be addressed to make a cross sector approach work, such as different requirements and consensus on needs and standards, cross sector trust / liability and privacy.

In relation to where work would start, this project indicates that discussion should start with financial sector organisations, along with the sharing economy, identity providers and online gambling.

This project has shown from the organisations that responded that they want to actively pursue a public private cross sector approach to online identity needs. The recommendations are for a cross sector collaborative approach to set the rules of engagement, policies and legal frameworks to fully address the challenge of online identity in the UK.

How this now moves forward is going to be critical to the development of the UK identity market, and how online identity might be able to further underpin digital growth across sectors.

1. UK Identity Market Drivers

Solving the issue of trusted identities online has become one of the most compelling problems faced for UK online growth.

Throughout 2015 and 2016 reported hacking attempts have grown, resulting in an explosion in data breaches[1]. In late 2015 the Office for National Statistics released their annual report on fraud in England and Wales, this number has soared 70 percent after more than five million[2] cyber crimes and frauds were included in the total for the first time.

These cybercrimes affected four million people, of whom 2.6 million suffered financial loss as a result. In the wake of recent hacking there has been a reported spike in UK citizen concerns around privacy[3] and security.

All this is coupled with the desire for consumers to find quicker and more convenient ways to transact online: this Christmas alone online shopping sales increased by 16.2%. This desire from consumers to transact digitally is aligned with businesses to move consumers online, which has potentially significant cost savings.

Personal data loss, privacy and security is high on the UK consumer agenda. A recent Ofcom report[4] states that three in ten (28%) of those who use apps now have concerns, compared to two in ten (20%) in 2013 — with security/fraud or privacy (20%) being the most common concern.

Solving the issue of secure online identities has never been more important. Giving consumers and businesses a secure online way to transact with each other in an inclusive and privacy enhancing way is one of the UK's biggest digital challenges.

[1] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[2] http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html

[3] http://www.telegraph.co.uk/technology/google/11814471/google-reveals-spike-in-british-privacy-concerns.html

[4] http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf

2. Background to the 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 for 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 is the first UK population scale deployment of a high assurance digital identity program. 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.

The service went live in May 2016, has already verified more than 500,000 identities and will continue to grow in usage as more government services adopt it throughout 2016 and beyond.

Federated identity systems are different from the individual solutions available today, and work on the premise of verify once, use many times. GOV.UK Verify is aimed at making online interaction with government services quicker, easier and more secure for users. Fundamentally this service means that government does not own the citizen's identity, there is no single central database and citizens have a choice about which identity provider they use to verify and secure their identity. Each identity provider has a set of certification requirements to ensure they are adhering to the standards set for privacy, security and identity assurance.

The GOV.UK Verify service is currently only available for use for government transactions.

This project sought to gain feedback from private sector organisations on the component parts of the GOV.UK Verify service, from the open identity and authentication standards, to brand and through to the privacy principles.

The aim of taking this feedback was to understand which of the components that have already been developed might the private sector see as valuable, or not for their identity needs. How could identities created for government services be reused by the private sector, and would the private sector want to do this?

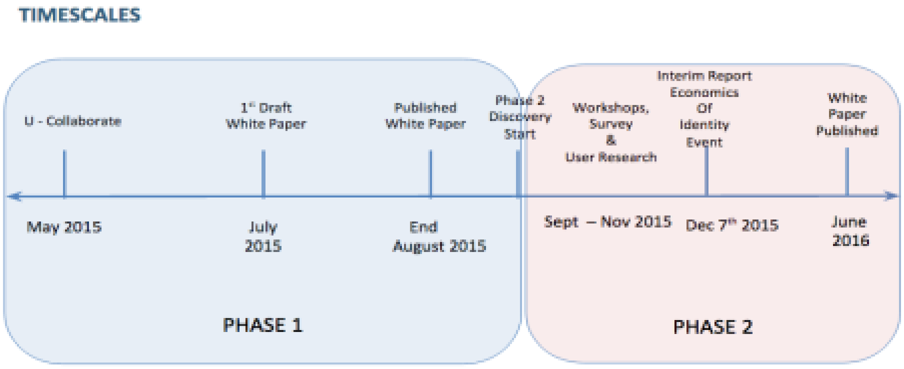
3. Participants

80 companies responded to the survey. We would like to thank all organisations who took part in the project. The names below have given permission for their details and logo to be published in this report, others wished to remain anonymous. A list of participants can be found in Appendix 1.

IdenTrust
under the doormat
UNIBET
Aol.
digidentity
carbon heroes
amadeus
SHARING ECONOMY UK
Adobe
playtech
HASSLE.com
BlaBlaCar
RGA
The PENSIONS Advisory Service
nucleus
HSBC
BARCLAYS
TeleSign
Echo
Fidelity INVESTMENTS
M&G INVESTMENTS
SAFRAN Morpho
taxcalc
ACI UNIVERSAL PAYMENTS
B&CE
Investec
GRUB CLUB
OLDMUTUAL WEALTH
Parmenion
iress
HARGREAVES LANSDOWN
vrumi
Compare and Share
Calastone
TISA
TIO
TIMPSON
consult hyperion
ffrees
Onfido
PAOGA
mydex
verizon
GBG

4. The Project and Survey

The diagram below shows the timescales and phasing of the discovery projects which have been focused on this topic.



This document details the second phase of a discovery process into private sector needs for identity assurance. The first phase of the project is described in the preceding white paper[5]. The second phase was designed to build on the first by widening the number of organisations that were involved. This second phase was an open process; any organisation from the private sector was free to respond to the survey.

A selection of survey questions was collated to gain feedback on the subject matter. A series of sector specific workshops were held for financial services sector, the I.T sector, the retail sector, the gambling sector and identity providers. These workshops were 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 and challenges around identity services identified in the initial industry workshop in May 2015.

The survey was then sent to 120+ companies across the UK through three methods:

1. Electronic survey
2. Paper based survey
3. Telephone interview

80 organisations across multiple sectors responded to the survey. A full breakdown of the responses by sector can be found in Appendix 1.

[5] http://oixuk.org/wp-content/uploads/2015/09/Discovering-the-Needs-for-UK-Identity-Assurance-V21.pdf

5. Response Summary

In relation to the potential reuse of GOV.UK Verify there are a range of options about which part/s could be made available to the private sector. The survey was designed to understand the private sector's view on the value of each of those as well as their views on the market generally. Full details of all questions, response breakdown and analysis can be found in Appendix 2.

<u>The Market</u>

The questions on the market were covered off under the themes of "Identity Market Needs" and "Identity Market Development". This section was designed to understand the current state of the market and what buyers of identity services felt had the most important needs for improvement over the next 3 years.

THE MARKET – SECTION SUMMARY

There were strong response rates across the board in this section from financial services, online gambling, sharing economy, identity providers. Identity documents, electronic checks (such as those with a credit referencing agency) and user names and passwords are the most commonly used methods for identity proofing and authentication. Some sectors use a multitude of solutions today for the purposes of identity verification and authentication, the sharing economy being the most notable example which gave the widest range of responses in relation to methods used.

The main characteristics of a fully operating identity ecosystem noted by respondents were security, ease of use and reliability / accuracy. There were a wide range of answers across the board for this question, demonstrating there is no clear and consistent view on the main characteristics. Some of the other highest rated answers were trust, high adoption, single / simple standards and time savings.

The main opportunities identified were collaboration with / expansion outside of government, a better customer journey and cost savings. The main challenges organisations see with the market developing were lack of trust, lack of access to data for verification (banking and government data were cited in this regard) and cost. The responses to this question showed there is an appetite for the private sector respondents to work with the public sector to create a successful identity market. "Lack of data" (for identity proofing) is often referring to people in the UK that do not have the usual identity proofing information, for example passports, driving licenses or that people are not present on the credit referencing file. The lack of data for verification purposes makes these individuals difficult to verify electronically. In many cases the information cannot be verified against the authoritative source and this can be exploited by fraudsters. An increase in "open data" would also be useful for improved levels of identity proofing, risk mitigation and increased fraud prevention

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.

The questions on standards were covered off under the questions relating to "Standards" in the questionnaire. The main highlights from this section were:

STANDARDS - SECTION SUMMARY

The understanding of the Good Practice Guide standards was relatively low with 52% stating they understood them well. Just over half (54%) of those that responded said the standards were extremely or very relevant to their industry with 17% stating they had slight or no relevance. The open standards used by the GOV.UK Verify program are relatively detailed methods of verification and authentication. A level of knowledge is required to understand them well. This is the likely reason for a lower response rate, and subsequent understanding. These responses indicate that a lower percentage of respondents understood these documents, but of those that did over half felt they were relevant

59% of organisations said they do not have an existing standard for identity and authentication. Those organisations that did state they have standards cited the Joint Money Laundering Guidance notes, Fourth Money Laundering Directive and Gambling Regulations. 72% stated they would need access to additional attributes outside of core identity attributes (name, address DOB, gender). This response is a clear indication that if GOV.UK Verify were to be used within the private sector that there would be a requirement for additional attributes to ensure organisations could comply or satisfy their identity requirements. This feedback paves the way for requirements around attribute exchange.

Respondents stated that some private sector transactions, but not all, could be satisfied from an identity and authentication perspective by the open standards of Level of Assurance 2 (LoA2). Some of those transactions noted that could be satisfied by LoA2 were financial services transactions (such as online banking, mortgage and loan applications), players at registration for online gambling and mobile phone contracts.

Additional attributes cited that would be required over and above LoA2 to allow companies to comply with their regulatory or risk management included identity documentation (outside of passports and driving licenses), location, education history / qualifications, travel history, disclosures and barring checks (DBS), right to work checks and credit ratings.

Certification

GOV.UK Verify identity program requires companies to be certified. Certification adds costs but provides assurance that standards are being met by the certified organisations.
The questions in this section related to the certification process adopted by the GOV.UK Verify program, the section was called "Certification". The highlights of this section were:

CERTIFICATION - SECTION SUMMARY

The understanding of the GOV.UK Verify certification process was relatively low with 46% stating they understood it well.

However, when asked if respondents thought certification was important, 80% said they felt certification in this context was very important. So, despite the lack of understanding of the specific government certification requirements, private sector organisations felt it was important for third party providers of identity services to be certified.

The main areas for development for certification were cross industry regulations / standards, education for the general public, making it simple and easy to understand, a liability model, trust framework, and a range of options for certification from self-certification to independently certified.

Brand

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. In considering the potential re-use of some or all of the capabilities built for GOV.UK Verify in the private sector, it is important to consider a range of options. These could include making the GOV.UK Verify brand available outside of central government, or allowing certified companies to re-sell their services outside of central government under other brands specific to particular sectors. The survey asked for respondents' views on this. Highlights of this section were:

BRAND - SECTION SUMMARY

The majority of respondents 67% thought that it would be very important to have a cross sector brand within a cross sector identity environment. However, 48% of respondents felt that GOV.UK Verify would be a valuable brand in this context and 40% felt the GOV.UK Verify brand would be appropriate for use in a cross sector context.

This response shows that there isn't a consensus view within or across sectors when it comes to the appropriateness or perceived value of the GOV.UK Verify brand being used within private sector transactions. There were also a wide range of mixed reactions across positive, neutral and negative when respondents were asked to explain their views on appropriateness and value of the GOV.UK Verify brand in this context.

These responses demonstrate that brand would need to be considered carefully, and that the GOV.UK Verify brand may not be the right brand to bring through to the private sector. The question is what brand(s) would work? How would this be decided on, and tested for effectiveness? Should there be different brands for different sectors, or one new brand for the private sector, with the GOV.UK Verify brand serving only public sector?

These responses also do not take into account citizen feedback, which should be tested to understand this feedback fully.

Privacy and Identity Assurance Principles

The questions in this section related to the 9 identity assurance principles were covered under the section "Identity Assurance Principles". Details of the 9 identity assurance principles can be found in Appendix 2. The main highlights from this section were:

IDENTITY ASSURANCE PRINCIPLES – SECTION SUMMARY

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 program, and GOV.UK Verify builds and maintains users' confidence that their privacy will be protected. Highlights of this section were:

Overall respondents felt strongly about this topic and the understanding of the privacy principles was high with 66% stating they had an excellent to very good understanding of the 9 privacy principles. 78% felt that having a set of privacy principles was very **important** to a cross industry identity approach with only 4% stating they felt they had no importance.

76% felt that the 9 privacy principles were very **relevant** to their sector or organisations – with only 4% stating they had no relevance at all.

When asked for feedback on each principle the majority of respondents felt it would be valuable for their organisation to adopt the 8 of the principles.

User control, transparency, data minimisation, data quality, certification and dispute resolution all had clear outcomes in relation to the perceived positive benefits for adoption. Multiplicity, user access and transportability, were still viewed in the main as appropriate but more respondents were unsure about the benefits. People were unsure about what principle 9 (exceptional circumstances) meant, which may bring into question education around this principle, and then further assessment of its appropriateness in this context.

The main ways respondents felt organisations should demonstrate to users they are meeting the privacy principles was through audit and certification, an industry body or watchdog or through their brand (i.e. risk to their brand if they did not fulfil the requirements).

These responses demonstrate that the privacy principles are understood well, the majority perceive them as both important and relevant across the private sector. This positive response indicates that respondents felt that some of the privacy principles could be adopted easily within a cross sector identity framework.

Cross Industry

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.

The questions in this section related to the view organisations had around a cross industry approach to identity. The main highlights from this section were:

CROSS INDUSTRY – SECTION SUMMARY

81% of organisations that responded stated they thought a cross sector approach to identity would be either extremely or very valuable. This positive response across vertical sectors is a clear indication that the private sector would like to continue investigating a cross sector approach to identity.

The top benefits from the respondents were improved customer experience, ensure portability, fraud reduction, cost savings, speed of on-boarding, economies of sales a definition of standards / one standard.

The top challenges cited were different market segments and requirements, cross sector trust and liability, competition, privacy, too many opinions slowing it down, regulatory acceptance.

The positive response towards collaboration would indicate an appetite from the private sector respondents to work together towards the benefits, and to work through the challenges.

6. Conclusions and Next Steps

The benefits organisations see in developing a fully operating cross sector identity framework are now clear, as well as the challenges and potential barriers that would need to be addressed to make it happen.

Financial services had the most respondents overall followed by the sharing economy, identity providers and online gambling.

There were many perceived benefits, such as improved customer experience time and cost savings and portability. The project also exposed the challenges that could be faced, and would need to be addressed to make a cross sector approach work such as different requirements and consensus on needs and standards, cross sector trust / liability and privacy.

Focus on the challenges is needed, including establishing liability models and understanding of the commercial model: who pays, how, and how much. Additionally, understanding how existing regulated markets, which have existing standards could adopt a cross sector approach to identity, for example how would the financial services or gambling sector regulators come to accept such an all encompassing program?

Those challenges will need to be solved through cross sector collaboration. However, the benefits are something that the majority of those organisations that responded felt strongly enough about to want to continue its investigation.

More data / data attributes will likely be required in order to answer the multifaceted identity requirements of the various industries, and to make a fully functioning identity ecosystem work. The survey responses showed that organisations felt banks and government might be able to provide this data, however many other required data attributes were also cited. This feedback clearly demonstrates the need for attribute exchange/s and further underpins the work being completed in Warwickshire through the Open Identity Exchange and elsewhere.

Questions were also asked about standards, certification, privacy and brand. Respondents had a range of views around these four topics, from majority acceptance on some, e.g. privacy principles, to mixed opinion on others, e.g. the GOV.UK Verify brand to be used in the private sector. Some areas require further education, such as standards and certification as this was less well understood.

In the example of certification, although the understanding level was low respondents still felt it was important. Therefore, this indicates that were there to be an interoperable identity program for public and private sector, some form of certification would be important to those organisations using digital identities.

When it came to the brand responses, these were mixed, therefore careful consideration about what brand might be used in a public private sector identity program is required.

The questions around the identity assurance principles were received positively by respondents, indicating it is likely these could be used, with minimal changes in the context of private sector identity transactions.

The main conclusion from this project is that there is significant appetite to pursue a cross industry approach to identity assurance needs with 81% of organisations that responded to this question wanting to move forward in a collaborative way.

In relation to where work would start, this project indicates that discussion should start with financial sector organisations, along with the sharing economy, online gambling and identity providers.

This project has shown from the organisations that responded that they want to actively pursue a public private cross sector approach to online identity needs. How this moves forward now is going to be critical to the development of the UK market, and how online identity might be able to further underpin digital growth across sectors.

APPENDIX 1 - Survey Response Rates and Respondents

The survey was responded to by 80 UK organisations, from banking, gambling, telecoms, sharing economy, insurance, retail, pensions providers, identity technology providers as well as others including industry experts and consultants. The detailed survey questions which can be found in Appendix 2 were provided by an online survey, paper based survey and also offered through telephone interviews.

A qualitative analysis approach was taken to the responses. The survey questions required some understanding of identity, therefore not all respondents answered all questions.

Total Survey Responses	Surveys 100% Complete	Surveys <100% Complete
80	**53**	**27**

Despite the identification of strong positive and negative opinions within the responses which could be considered outliers, 100 percent of responses were taken into account within the survey and no outliers were removed.

Responses by Sector

Sector	Overall Survey Responses Per Sector
Financial Services	28
Sharing Economy	10
Identity Providers	9
Gambling	6
IT	5
Telecoms	4
Retail	2
Others	16
TOTAL	**80**

The financial services sector had the highest number of responses with retail as the lowest.

Respondents

80 companies responded to the survey. We would like to thank all organisations who took part in the project. The names below have given permission for their details to be published in this report, others wished to remain anonymous.

- Nucleus
- iress
- Grub Club
- TIO
- Timpson
- Moresberg
- IdenTrust
- Onfido
- Consult Hyperion
- Under the Doormat
- Carbon Heros
- Hassle.com
- Amadeus
- Unibet
- The Pensions Advisory Service
- Echo
- ACI
- Parmenion
- BlaBlaCar
- Fidelity
- Frees
- Calastone
- Paoga
- Mydex
- Verizon
- GBG
- Safran Morpho
- Vrumi
- Barclays
- HSBC
- TISA
- Investech
- Aol
- Playtech
- Adobe
- RGA
- Old Mutual Wealth
- M&G Investments
- Compare and Share
- Digidentity
- Telesign

APPENDIX 2 – Questions, Detailed Responses and Analysis

The Market

The questions on the market were covered off under the themes of "Identity Market Needs" and "Identity Market Development". This section was designed to understand the current state of the market and what buyers of identity services saw has the most important needs for improvement over the next 3 years.

1) IN WHAT CIRCUMSTANCES DOES YOUR ORGANISATION NEED TO CONFIRM THE IDENTITY OF YOUR CUSTOMER?

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
On-Boarding /Registration	18	7	4	1	0	1	0	2	3
Part of AML / KYC	8	7	0	0	0	0	0	0	1
Where The Trigger Threshold is Met	3	0	3	0	0	0	0	0	0
Other Answers	19	6	2	2	1	1	3	0	4
Total	**48**	**20**	**9**	**3**	**1**	**2**	**3**	**2**	**8**

ANALYSIS

More than half of the overall organisations that responded to the survey answered this question. Financial services and gambling had the highest response rate.

AUTHOR'S COMMENTS

Financial services and the gambling sector have identity verification regulations. They have a clear requirement to confirm the identity of the customer, therefore it makes sense that they would have the highest response rate to this question.

2) IN RELATION TO YOUR CUSTOMERS AND THEIR USE OF DIGITAL SERVICES WITH YOU, HOW DO YOU CURRENTLY INITIALLY IDENTIFY YOUR CUSTOMERS WHEN THEY REGISTER OR OPEN AN ACCOUNT WITH YOU, AND HOW DO YOU RE-AUTHENTICATE THAT IT'S THEM WHEN THEY COME BACK TO YOU?

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Documents such as ID Cards, Passport or Driving License	17	6	2	3	1	0	1	1	3
IdP / Credit Bureau	15	10	2	0	0	0	0	1	2
Issue Login Details / Password / Passcode	13	5	2	0	0	1	2	2	1
Other Answers	38	12	1	3	0	2	13	1	7
Total	**83**	**33**	**7**	**6**	**1**	**3**	**16**	**5**	**13**

ANALYSIS

Organisations were able to give more than one answer to this question accounting for the number of overall responses. Overall the verification of identity documents is the most used method for verifying identities. Financial services, gambling and the sharing economy gave the most responses. The majority of sectors use the most popular methods of verification (identity documents, credit referencing agencies and passwords) this is with the exception of the sharing economy.

AUTHOR'S COMMENTS

The multiple methods of verification in the sharing economy varied from validation of email or social media profile through to a manual search of the web. This reflects that the sharing economy has a need for verification of identity but there are currently no standardised ways to do it, the industry is also exclusively online and therefore manual face to face methods are not a viable option. Verification is a current challenge for this industry and is highlighted in the 2014 report "Unlocking the Sharing Economy"[6]

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378291/bis-14-1227-unlocking-the-sharing-economy-an-independent-review.pdf

3) 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?	
First characteristic	
Second characteristic	
Third characteristic	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Security	22	7	2	0	0	1	1	2	9
Ease of Use	22	7	0	1	0	2	5	2	5
Reliable / Accurate	12	5	0	1	0	0	2	2	2
Other Answers	112	38	15	4	3	5	8	18	21
Total	**168**	**57**	**17**	**6**	**3**	**8**	**16**	**24**	**37**

Analysis

Security, ease of use and reliability / accuracy were the highest rated characteristics of a successfully developed identity assurance market. However, there were a very wide range of answers across the board some of the other highest rated answers were trust, high adoption, single / simple standards and time savings all ranked highly.

Author's comments

The high number and wide range of answers shows there is no clear consistent view on what the main characteristics of successful market would look like, this view may change with market maturity.

4) IN YOUR OPINION WHAT ARE THE 3 MAIN OPPORTUNITIES FOR THE RAPID AND SUCCESSFUL DEVELOPMENT OF THIS IDENTITY MARKET IN THE UK?	
FIRST OPPORTUNITY	
SECOND OPPORTUNITY	
THIRD OPPORTUNITY	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Collaborate With / Expand Outside of Government	14	6	0	3	0	2	0	3	0
Better Customer Journey / Easy Access to Services	10	6	1	0	0	0	0	2	1
Cost Savings	8	3	0	0	0	2	1	1	1
Other Answers	90	35	11	2	3	5	7	10	17
Total	**122**	**50**	**12**	**5**	**3**	**9**	**8**	**16**	**19**

ANALYSIS

Opportunities to collaborate with or expand outside of government, a better customer journey and cost savings were the highest rated opportunities of a rapid and successfully developed identity assurance market. However, there were a very wide range of answers across the board some of the other highest rated answers were shared standards, interoperability, reduced fraud and increased digitisation.

AUTHOR'S COMMENTS

The high number and wide range of answers shows there is no clear consistent view on what the main opportunities could be. However, the survey shows there is an appetite for the private sector to work with the public sector to create a successful identity market, there are a number of options for how this could work including the re-use of GOV.UK Verify within the private sector.

5) In your opinion what are the 3 main barriers to the rapid acceleration of a UK identity market?	
First barrier	
Second barrier	
Third barrier	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Lack of Trust / Confidence	20	5	5	0	1	0	2	3	5
Lack of Access to Data (Government and Bank Data)	13	3	1	1	0	0	3	4	1
Cost	11	3	2	1	0	0	1	1	3
Other Answers		**39**	**6**	**2**	**2**	**10**	**6**	**9**	**30**
Total	**148**	**50**	**14**	**4**	**4**	**10**	**12**	**17**	**39**

Analysis

Lack of trust / confidence, lack of access to data and the cost were the highest rated barriers to a rapid acceleration of an UK identity market. There were a wide range of answers across the board some of the other highest rated answers were lack of consumer understanding, lack of adoption, cost and lack of standards.

Author's comments

The lack of trust or confidence is a subjective response, however this is coupled with the lack of consumer understanding and would create a lack of adoption which were issues stated elsewhere in the responses. The consumer communication of an interoperable program would be critical to its success. “Lack of data” (for identity proofing) is often referring to people in the UK that do not have the usual identity proofing information for example passports, driving licenses or that people are not present on the credit referencing file. The lack of data for verification purposes makes these individuals difficult to verify electronically.

Increased availability of data from other sources would make the verification of these individuals easier, and allow them to create a digital identity. The creation of a digital identity would allow them to access more services online, quicker and easier than before. This would make it more cost effective for organisations offering services to them.

In many cases the information cannot be verified against the authoritative source and this can be exploited by fraudsters. An increase in “open data” would also be useful for improved levels of risk mitigation and increased fraud prevention.

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

6) Upon reading the Good Practice Guides 43, 44 and 45 and the Operations Manual how well would you say you understand them?

	Don't understand at all	Slight understanding	Moderate understanding	Good understanding	Excellent understanding

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Excellent Understanding	6	1	0	0	0	0	0	1	4
Very Good Understanding	18	2	3	2	0	1	2	4	4
Moderate Understanding	14	6	2	0	1	1	1	1	2
Slight Understanding	2	0	0	0	0	0	1	0	1
Do not Understand	**6**	**2**	**1**	**0**	**0**	**0**	**1**	**0**	**2**
Total	**46**	**11**	**6**	**2**	**1**	**2**	**5**	**6**	**13**

Analysis

Over half of the overall respondents answered this question. Just over half (52%) of those that responded had a very good or excellent understanding of the standards with the remainder stating moderate, slight or no understanding.

Author's comments

The open standards used by the GOV.UK Verify program use relatively detailed methods of verification and authentication. A level of knowledge is required to understand them well. This is the likely reason for a lower response rate, and subsequent understanding.

7) HOW RELEVANT ARE THESE DOCUMENTS TO YOUR INDUSTRY?					
	NOT RELEVANT AT ALL	SLIGHT RELEVANCE	MODERATELY RELEVANT	VERY RELEVANT	EXTREMELY RELEVANT

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Relevant	6	1	0	0	0	0	0	1	4
Very Relevant	19	3	3	2	0	1	2	4	4
Moderately Relevant	13	5	2	0	1	1	1	1	2
Slightly Relevant	2	0	0	0	0	0	1	0	1
Not Relevant	**6**	**2**	**1**	**0**	**0**	**0**	**1**	**0**	**2**
Total	**46**	**11**	**6**	**2**	**1**	**2**	**5**	**6**	**13**

ANALYSIS

Over half of the overall respondents answered this question. Just over half (54%) of those that responded said the standards were extremely or very relevant to their industry with 17% stating they had slight or no relevance.

AUTHOR'S COMMENTS

This response in combination with the previous question indicates that few people understood these documents, but of those that did over half felt they were relevant. In order to gain a wider assessment of the relevance of these documents across the private sector would require further engagement to enable further understanding, more informed respondents and then increased feedback.

8) DOES YOUR INDUSTRY HAVE A STANDARD FOR IDENTITY PROOFING AND VERIFICATION AND / OR AUTHENTICATION?	
YES	
NO	
DON'T KNOW	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Yes	18	8	3	1	0	1	1	1	3
No	32	4	4	1	1	2	6	5	9
Don't Know	4	3	3	0	0	0	0	0	1
Total	**54**	**15**	**7**	**2**	**1**	**3**	**7**	**6**	**13**

ANALYSIS

33% stated they did have a standard, 59% of respondents stated their industry did not have standards for identity proofing or verification, and 7% didn't know.

AUTHOR'S COMMENTS

This was one of the more surprising responses in the survey in relation to the financial services and online gambling sectors, both are regulated with clear guidance for identity proofing (JMLSG and Gambling Act). The identity provider response was also unexpected as there are clear standards in place for identity providers (Good Practice Guides), however this could be explained by the fact that many of the identity providers sit in their own vertical sectors, it is likely that the responses from the identity providers related to the sectors they are in.

9) IF YES, PLEASE LIST THE STANDARDS

ANALYSIS

Standards that were listed were the following:

- Gambling Commission (Gambling Act)
- 4th Money Laundering Directive
- JMLSG (Joint Money Laundering Steering Group)
- FCA (Financial Conduct Authority)
- RGA (Remote Gambling Association)
- Regulatory right to work and right to rent/DBS guidelines (Disclosures and Barring Service)
- Stork

- eIDAS
- GOV.UK Verify IPV standards
- PCI (Payment Card Industry)
- NSTIC (National Strategy for Trusted Identities in Cyberspace)

10) Does your organisation need to verify other attributes about customers, apart from their identity?	
Yes	
No	
Don't know	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Yes	34	10	4	2	0	1	4	3	10
No	12	3	1	0	1	1	2	2	2
Don't Know	1	1	0	0	0	0	0	0	0
Total	**47**	**14**	**5**	**2**	**1**	**2**	**6**	**5**	**12**

Analysis

72% stated they did need to verify other attributes apart from identity and 25% of respondents stated their industry did not need to verify other attributes.

Author's comments

The survey did not distinguish between a requirement for the actual data or whether there was a requirement for simply evidence of entitlement e.g. D.O.B verses over 18. However, this response is a clear indication that if GOV.UK Verify were to be used within the private sector that there would be a requirement for additional attributes to ensure organisations could comply or satisfy their identity requirements. Work being completed by the Open Identity Exchange[7][8][9][10] and elsewhere will be key to the development of a fully functioning identity proofing ecosystem. There will also be a requirement for attributes to become available for the purposes of attribute exchange, some of those listed below are challenging for organisations to access electronically from the issuing or authoritative source. This aligns with previous survey feedback that organisations felt they needed access to "more data" (Question 5).

[7] http://oixuk.org/wp-content/uploads/2014/05/OIX-IWG-AX-report-Sept-2015-v0.3.pdf

[8] http://oixuk.org/wp-content/uploads/2015/08/WCC-2-alpha-white-paper-final-draft.pdf

[9] http://oixuk.org/wp-content/uploads/2015/08/WCC-2-alpha-white-paper-final-draft.pdf

[10] http://oixuk.org/wp-content/uploads/2014/09/WCC-2-white-paper-FINAL.pdf

11) IF YES, PLEASE LIST THE ATTRIBUTES

Below is a list of attributes that organisations felt they would need in addition to "identity" to allow them to complete the transactions in their industry. This is an overall list rather than one of importance.

ATTRIBUTES

- Mortality
- PEPS/Sanctions
- Civil proceedings
- Entitlement to benefits
- Evidence of economic content
- Location
- Source of funds
- Age
- Credit worthy
- Employment/education history
- Facial recognition
- Skill level
- Travel history
- Vehicle status
- Membership accounts
- Suitability
- Place of operations
- Bank account
- Credit card/payment information
- Criminal records
- Qualifications
- Propensity for fraud
- Insurance policy number
- Company registration
- Immigration
- NINO (National Insurance Number)
- Current and past addresses
- Device ID

12) PLEASE LIST ANY TRANSACTIONS YOU ARE RESPONSIBLE FOR THAT YOU HAVE ASSESSED AS REQUIRING LOA2 IDENTITY PROOFING AND VERIFICATION AS DEFINED BY GOVERNMENT STANDARDS.

Below is some of the transactions organisations stated that private sector organisations felt could be satisfied by Level of Assurance 2 proofing and verification.

- Online banking
- Trigger threshold (anti money laundering trigger)
- Mortgage applications
- Mobile phone contract

- Payout transaction
- Assessing insurance information
- Access car information
- Payment accrued pension benefits
- Loan applications
- All players at registration (gambling sector)
- GOV.UK Verify
- Account opening
- Revalidation

AUTHOR'S COMMENTS

This list gives an indication that private sector organisations do think there is an opportunity for UK citizens to use their digital identity (initially created to unlock government transactions at Level of Assurance 2) across private sector transactions.

13) WHAT FURTHER CHECKS WOULD YOU NEED TO DO, IF ANY, TO REACH THE REQUIRED LEVEL OF IDENTITY ASSURANCE FOR THESE TRANSACTIONS?

Below is some of the additional checks organisations would need to do (over and above a Level of Assurance 2 identity) to satisfy the identification requirements in their sector.

- Right to work in the UK
- Disclosure and barring check
- Right to hold directorship
- Credit ratings
- Biometric
- Documentation
- Age
- Enhanced due diligence for high value customers
- Bank details

AUTHOR'S COMMENTS

Many of these align with the attribute list stated above, and reinforce the requirement for attribute exchange mechanisms which would allow users to use a digital identity (e.g. Level of Assurance 2 identity) PLUS additional attributes to unlock further private sector transactions. These attribute exchange mechanisms would likely be required to have user consent and control at the heart to ensure consistency with the privacy principles.

Certification

GOV.UK Verify identity programme 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 program

14) HOW WELL DO YOU UNDERSTAND THE CERTIFICATION REQUIREMENTS FOR GOVERNMENT IDENTITY PROVIDERS?

	DON'T UNDERSTAND AT ALL	SLIGHT UNDERSTANDING	MODERATE UNDERSTANDING	GOOD UNDERSTANDING	EXCELLENT UNDERSTANDING

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Excellent Understanding	9	2	0	1	0	0	0	2	4
Very Good Understanding	14	4	3	1	0	0	1	2	3
Moderate Understanding	10	3	1	0	1	1	1	1	2
Slight Understanding	6	3	1	0	0	1	0	0	1
Don't Understand	10	3	1	0	0	1	2	0	3
Total	**49**	**15**	**6**	**2**	**1**	**3**	**0**	**5**	**13**

ANALYSIS

46% stated they have an excellent or very good understanding of the certification process, 20% have a moderate understanding and 32% have a slight or don't understand the certification process.

AUTHOR'S COMMENTS

The certification requirements for government identity providers is specific to that sector, this could explain the lower level of response to this question. In order to gain a wider assessment of the understanding of this certification process across the private sector would require further engagement to enable further understanding, more informed respondents and then increased feedback.

15) 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?					
	NOT IMPORTANT AT ALL	SLIGHTLY IMPORTANT	MODERATELY IMPORTANT	VERY IMPORTANT	EXTREMELY IMPORTANT

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Important	29	9	2	1	1	3	3	3	7
Very Important	10	3	3	1	0	0	2	0	1
Moderately Important	5	2	0	0	0	0	0	0	3
Slightly Important	4	0	0	0	0	0	1	1	2
Not Important	1	0	1	0	0	0	0	0	0
Total	49	14	6	2	1	3	6	4	13

ANALYSIS

80% of organisations felt it was extremely or very important for third party providers of identity assurance to be certified as meeting defined standards. 10% stated it to be of moderate importance, and 10% of slightly or no importance.

Despite the lack of understanding of the specific government certification requirements, private sector organisations felt it was important for third party providers of identity services to be certified.

AUTHOR'S COMMENTS

If there were to be an interoperable identity program for public and private sector, this feedback indicates that some form of certification would be important to those organisations using digital identities.

16) WHAT DO YOU THINK NEEDS TO HAPPEN NEXT IN THE DEVELOPMENT OF THE MARKET FOR CERTIFICATION SERVICES?

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Regulations, Standards and Trust Framework (Cross Industry)	11	4	1	0	0	0	1	4	2
Certification (motivation, validation, annual audits, range of standards)	9	2	1	0	1	0	2	1	2
Education Drive for General Public / Make it Simple and Easy to Understand	6	2	1	0	0	0	1	0	3
Other Answers	14	2	2	2	0	2	1	1	4
Total	**37**	**10**	**5**	**2**	**1**	**2**	**5**	**6**	**11**

ANALYSIS

There were a wide range of answers to the question about certification, and respondents had the option to give more than one response. The mention of standards featured most strongly amongst the answers given.

AUTHOR'S COMMENTS

It is clear that the private sector feel that some kind of certification is required, however there were some concerns raised in the workshops around the potential cost of a certification process.

These are valid concerns and should be considered as part of any further steps.

Brand

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

17) HOW IMPORTANT IS A CROSS INDUSTRY BRAND / LOGO TO COMMUNICATE TRUST IN A DIGITAL TRANSACTION?

	NOT IMPORTANT AT ALL	SLIGHTLY IMPORTANT	MODERATELY IMPORTANT	VERY IMPORTANT	EXTREMELY IMPORTANT

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Important	17	10	0	1	0	0	1	2	3
Very Important	19	2	2	1	1	2	2	2	7
Moderately Important	11	3	2	0	0	1	2	1	2
Slightly Important	6	2	2	0	0	0	0	0	2
Not Important	0	0	0	0	0	0	0	0	0
Total	**53**	**17**	**6**	**2**	**1**	**3**	**5**	**5**	**14**

ANALYSIS

67% of respondents felt that it was either extremely or very important for a cross sector brand to communicate trust in a transaction, 21% though it was moderately important and 12% thought it was slightly important. No organisation thought that a brand was not important to communicate trust.

AUTHOR'S COMMENTS

This is a clear indication that private sector feel a brand would be important to communicate trust in this context. Examples of brands that communicate trust or understanding in digital transactions today are the likes of Verified by Visa, Mastercard 3D Secure etc.

18) HOW VALUABLE WOULD IT BE FOR THE GOV.UK VERIFY BRAND / LOGO TO PLAY ANY PART IN PRIVATE SECTOR DIGITAL TRANSACTIONS?					
	NOT VALUABLE AT ALL	SLIGHTLY VALUABLE	MODERATELY VALUABLE	VERY VALUABLE	EXTREMELY VALUABLE

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Valuable	12	6	1	2	0	0	0	1	2
Very Valuable	14	4	1	0	0	2	1	2	4
Moderately Valuable	13	3	0	0	0	1	3	1	5
Slightly Valuable	9	2	2	0	1	0	1	0	3
Not Valuable	3	2	2	0	0	0	1	1	0
Total	**54**	**17**	**6**	**2**	**1**	**3**	**6**	**5**	**14**

ANALYSIS

48% of respondents thought the GOV.UK Verify brand could play an extremely or very valuable part in private sector transactions, 24% felt it would be moderately valuable and 22% felt it would be slightly or have no value.

AUTHOR'S COMMENTS

This response shows that there isn't a consensus view within or across sectors when it comes to the value of the GOV.UK Verify brand being used within private sector transactions. This shows that brand would need to be considered carefully, and that the GOV.UK Verify brand may not be the right brand to carry through to all areas of the the private sector. The question is what brand(s) would work? How would this be decided on, and tested for effectiveness? Should there be different brands for different sectors, or one new brand for the private sector, with the GOV.UK Verify brand serving public sector?

These responses also do not take into account citizen feedback, which should be tested to understand this feedback fully.

19) How appropriate would it be for the GOV.UK Verify brand / logo to play any part in private sector digital transactions?

	Not appropriate at all	Slightly approprite	Moderately appropriate	Very appropriate	Extremely appropriate

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Appropriate	9	4	1	2	0	0	0	1	1
Very Appropriate	12	6	0	0	0	2	1	0	3
Moderately Appropriate	16	3	2	0	0	0	3	2	6
Slightly Appropriate	8	3	0	0	1	0	1	2	1
Not Appropriate	8	1	3	0	0	0	1	0	3
Total	**53**	**17**	**6**	**2**	**1**	**2**	**6**	**5**	**14**

Analysis

40% of respondents thought the GOV.UK Verify brand would be extremely or very appropriate in private sector transactions, 30% felt it would be moderately appropriate and 30% felt it would be slightly or would not be appropriate for use in private sector transactions.

Author's comments

The view on the level of appropriateness of the GOV.UK Verify brand fell against the perceived value within private sector transactions. This response cements the view from the previous question, that a different / new brand would need to be created to carry across into the private sector. More detailed analysis of brand considerations is required including user/citizen testing rather than just an organisational view.

PLEASE EXPLAIN YOUR RESPONSES TO THE PREVIOUS 2 QUESTIONS

Below are the responses in relation to the question about the value and appropriateness of GOV.UK Verify in private sector transactions, this demonstrates the range of views across the private sector.

POSITIVE

- Need to be confident it's a government led initiative
- As long as they understand would give comfort
- Good enough for government, good enough for me
- GOV.UK Verify would create trust, then leave a trustmark
- Gives consumer confidence
- Rallying flag so if see the logo then know it works
- Most important is underlying brand principles
- ID needs to be controlled at a government level
- Supported by regulators and governing bodies
- For younger organisations gives trust
- Useful to know it's being used by government
- Bi lateral consuming of data would be very good
- Anything 3rd party would look weaker in comparison

NEGATIVE

- Concerns over consumer privacy
- Could be confusing
- Brand not relevant
- Why use government logo in a private sector transaction?
- Consumers may worry about an attempt by the government to establish an electronic ID card
- Verify brand already toxic
- Government not a trusted brand
- Verify brand not well enough established
- Hesitant sharing information with government/keep personal separate
- Across all private sector brand would seem invasive
- Too over government relationship, big brother fears
- Brand important, government not necessarily the right one

NEUTRAL

- Need transparency
- GOV.UK would have to be the authority with customer deals
- Add verify as a brand but take away government
- Avoid scams

- Need to be clear with consumer what data is being used/how being protected
- Supporting materials but not that logo
- Logo only valuable if user knows to look
- Not sure if government positive or negative. At the moment positive but could become a liability
- Government equals security but could be seen as snooping
- Make it financially viable for government brand

Privacy

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 program, 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

20) UPON READING THE 9 PRIVACY PRINCIPLES WELL WOULD YOU SAY YOU UNDERSTAND THEM?

	DON'T UNDERSTAND AT ALL	SLIGHT UNDERSTANDING	MODERATE UNDERSTANDING	GOOD UNDERSTANDING	EXCELLENT UNDERSTANDING
.					

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Excellent Understanding	6	1	0	0	0	0	1	1	3
Good Understanding	23	5	3	2	0	3	2	3	5
Moderate Understanding	15	7	0	1	1	0	1	1	4
Slight Understanding	2	1	1	0	0	0	0	0	0
Don't Understand	0	0	0	0	0	0	0	0	0
Total	**46**	**14**	**4**	**3**	**1**	**3**	**4**	**5**	**12**

ANALYSIS

63% said they have an excellent or very good understanding of the privacy principles, 33% had a moderate understanding, with only 5% saying they have a slight understanding and no-one with no understanding at all. The levels of understanding of the privacy principles in comparison to other areas e.g. standards, is much higher.

AUTHOR'S COMMENTS

This demonstrates that the privacy principles are well understood across all sectors. The privacy principles were written by the PCAG, and relative to the more complex standards and certification areas are relatively shorter and could be considered easier information to consume, this is likely the factor driving the higher level of understanding.

21) How important is it to have a published set of privacy principles for providers of identity assurance services?

	Not important at all	Slightly important	Moderately important	Very important	Extremely important

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Important	25	9	3	2	0	2	2	3	4
Very Important	15	5	1	0	1	1	1	1	5
Moderately Important	8	3	0	0	0	0	2	0	3
Slightly Important	2	0	2	0	0	0	0	0	0
Not Important	1	0	0	0	0	0	0	1	0
Total	**51**	**17**	**6**	**2**	**1**	**3**	**5**	**5**	**12**

Analysis

78% said they thought it was extremely or very important to have a published set of privacy principles, 16% said it was moderately important, with only 6% saying it was only slightly or not important.

Author's comments

The fact that the majority of private sector organisations feel that having transparent privacy principles is not a surprising result. Privacy has become a topic increasingly in the public eye with high profile news when organisations are not taking consumer privacy into account. The majority of privacy principles used as part of GOV.UK Verify are not tied to public sector, and therefore could easily become principles for use across private sector. If the European General Data Protection Regulations are still adopted by the UK, they could further reinforce the need for clear policy and procedures around privacy.

22) WHAT IS THE BEST WAY FOR USERS TO BE ASSURED THAT PROVIDERS ARE MEETING STATED PRIVACY PRINCIPLES?

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Audits and Certifications	14	5	3	0	0	2	1	1	0
Associate the Orgs Brand	6	0	0	1	0	0	3	2	0
Industry Body / Watchdog	5	2	0	0	0	1	1	0	1
Other Answers	21	7	2	1	1	3	0	2	5
Total	**37**	**14**	**5**	**2**	**1**	**6**	**5**	**4**	**9**

ANALYSIS

There were a wide range of answers to this question, from no formal assurance (brand risk if the principles were not adhered to) through to audit and certification.

AUTHOR'S COMMENTS

The question around this is important to organisations but also to the users of the service. It is hard to separate how this question was responded to by participants in the survey, were they answering on behalf of their organisation or really putting themselves in the shoes of the user? Whilst we have a wide range of answers here it would be valuable to understand what end users might want as assurance that organisations are adhering to the privacy principles.

23) How relevant are the privacy standards to your industry?

	Not relevant at all	Slightly relevant	Moderately relevant	Very relevant	Extremely relevant

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Relevant	22	8	1	2	1	1	1	4	4
Very Relevant	15	2	2	0	0	1	2	1	7
Moderately Relevant	10	5	1	0	0	1	2	0	1
Slightly Relevant	2	0	2	0	0	0	0	0	0
Not Relevant	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total	**49**	**15**	**6**	**2**	**1**	**3**	**5**	**5**	**12**

Analysis

76% said they thought it was extremely or very relevant, 20% said they were moderately relevant, only 4% said they were slightly relevant and no-one stated that privacy principles were not relevant. The highest response rates came from financial services.

Author's comments

These answers clearly demonstrate that the privacy principles are not only considered important but relevant too. In any cross sector identity framework answers indicate that they would be a welcome requirement.

24) OUTSIDE THE DATA PROTECTION ACT DOES YOUR INDUSTRY HAVE A STANDARD OR GUIDELINES FOR PRIVACY?	
YES	
NO	
DON'T KNOW	

Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Yes	12	4	3	0	0	0	0	0	5
No	30	9	3	1	1	2	5	4	5
Don't Know	7	2	0	1	0	1	0	0	3
Total	**49**	**15**	**6**	**2**	**1**	**3**	**5**	**4**	**13**

ANALYSIS

The majority of organisations (61%) responded that they do not have any privacy standards outside of the Data Protection Act. Some gambling and financial services companies thought they did have some, these are outlined below.

AUTHOR'S COMMENTS

The DPA is still the main driver for privacy within organisations, it will be interesting to see how this develops with the introduction of the General Data Protection Regulation.

25) IF "YES" PLEASE NAME THE STANDARD OR GUIDELINE

ANALYSIS

There were a few additional guidelines stated in addition to the DPA. These stemmed mainly from the financial services and gambling industries, likely because these industries have clear regulations.

- Balliwick of Guernsey - Gambling
- BBA Data Sharing Principles - Financial Services
- ISO27001
- Fairdata certification - Other
- Data Protection Policy - Gambling
- PCI DSS - Other

26) Do you think your industry would benefit from adopting the 9 Identity Assurance Principles?

	Yes	No	Unsure
User Control	39	5	2
Transparency	38	3	5
Multiplicity	25	5	12
Data Minimisation	35	4	3
Data Quality	37	4	3
Service User Access and Portability	28	2	15
Certification	35	4	6
Dispute Resolution	36	1	8
Exceptional Circumstances	20	7	16

Analysis

User control, transparency, data minimisation, data quality, certification and dispute resolution all had clear outcomes in relation to the perceived positive benefits for adoption. Multiplicity, user access and transportability and exceptional circumstances, were still viewed in the main as beneficial but more respondents were unsure about the benefits.

Author's comments

In the workshops there were a number of questions about what "exceptional circumstances" meant. Despite the majority saying they understand the privacy principles well, without context some of the way these principles would actually be implemented could be lost. Therefore, it would make sense to further educate the private sector about the meaning of the principles, particularly those where it is not clear (from the responses given).

However, in the main, this is a positive response that some of the privacy principles could be adopted easily within a cross sector identity framework.

10. Cross Industry

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

27) How valuable do you think it would it be to explore a cross sector approach?					
	Not valuable	Slightly valuable	Moderately valuable	Very valuable	Extremely valuable

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Extremely Valuable	21	8	2	1	1	1	1	2	5
Very Valuable	21	7	2	1	0	2	3	1	5
Moderately Valuable	6	0	1	0	0	0	1	1	3
Slightly Valuable	2	1	1	0	0	0	0	0	0
Not Valuable	2	0	0	0	0	0	0	1	1
Total	**52**	**16**	**6**	**2**	**1**	**3**	**4**	**5**	**14**

Analysis

81% of organisations stated they felt it would be extremely or very valuable to explore a cross sector approach to identity, 11% said they thought it would be moderately valuable, and 8% stating they thought it would be slightly or not valuable. Financial services, gambling, telecoms, IT, the identity providers and the sector under "other" were all positive as a percentage of the overall respondents. The sharing economy was positive but the response rate was relatively low.

Author's comments

This positive response across vertical sectors is a clear indication that the private sector would like to continue investigating a cross sector approach to identity.

28) WHAT DO YOU THINK THE MAIN BENEFITS WOULD BE OF A CROSS SECTOR APPROACH?

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Improved and Consistent Customer Experience	13	4	1	0	1	1	0	0	6
Time and Cost Savings	10	1	0	1	0	1	1	1	5
Portability	8	3	0	0	0	1	0	0	4
Other Answers	27	5	5	1	0	4	3	4	5
Total	**43**	**13**	**6**	**2**	**1**	**7**	**4**	**5**	**20**

ANALYSIS

The top answers for this question were:

- Improved and consistent customer experience
- Time and cost savings
- Portability

Below shows the detail all the other answers provided as part of the responses that were received:

- Speed of on-boarding
- Enable customer view
- Single point of contact for customers
- Reduce complexity for consumer
- Users can use across different sectors
- Ubiquity and consistency to customers
- Drive adoption as use the same credential
- ID market larger, more supply, lower prices
- Safety in numbers
- Less fragmentation
- Wider reach of resources
- Tapping into wider communities
- Share security
- Economic growth
- Unified ID services
- It would remove ID's that are not robust enough
- Level the playing field
- Sharing information
- Data monitisation
- Increased adoption
- A single method
- Quicker development
- More thorough

- Definition of common requirements and framework
- One standard
- Uniformity
- Inform government as to how private industry works
- Reduce fraud/risk
- Recognisable brand

AUTHOR'S COMMENTS

This shows that there are a large range of perceived benefits of a cross sector identity approach within the private sector, and further confirms the response that organisations would like to continue with this approach. What is interesting is that the top benefit was a benefit for the customer (improved customer experience). Many organisations, particularly in financial services are likely realising that identity is a critical part of getting customers through the on-boarding process and able to access and use their products.

29) WHAT WOULD BE THE CHALLENGES OF A CROSS-SECTOR APPROACH?

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Different Market Requirements / Consensus on Needs and Standards	15	2	1	0	0	2	2	2	6
Cross Sector Trust / Liability	5	2	0	0	1	0	0	1	1
Privacy	4	1	0	0	0	0	0	1	2
Other Answers	27	7	4	3	0	3	2	1	7
Total	**43**	**12**	**5**	**3**	**1**	**5**	**4**	**5**	**16**

ANALYSIS

The top answers to this question from across the sectors were:

- Different market requirements / consensus on needs and standards
- Cross sector trust / liability
- Privacy

Below shows the detail all the other answers provided as part of the responses that were received.

- Apathy
- Lack of trust in government

- Customer education
- Acceptance
- User participation
- Security
- Distinction between sharing data to keep people safe and for marketing
- Quest for monetisation
- ID card by a different name
- Competing objectives
- Slow time to market
- Trusted scheme
- Cross sector trust
- Too many opinions slowing it down
- Creating legal entities
- Co-ordination and logistics
- Agreeing what data to share
- Competition
- Reliability
- Engagement and getting large corporates to act
- Regulatory acceptance
- Getting enough industry to comply
- Data protection
- Level of due diligence
- Technology interfaces
- Very broad

AUTHOR'S COMMENTS

There are many challenges that will need addressing if a cross sector approach is to be successful. How these would be approached would need careful consideration. The liability model for example will need to be addressed in order to allow one sector e.g. financial services, to accept an identity that has been verified in another sector e.g. government. In regulated sectors the regulations and regulators will need to be part of the agreements made in this regard, therefore others like the Financial Conduct Authority, treasury, gambling commission and so on would need to be consulted with.

30) DOES YOUR ORGANISATION HAVE DIFFICULTY VERIFYING CUSTOMERS?	
YES	
NO	
DON'T KNOW	

Top Answers	Total	FS	Gambling	Telecoms	Retail	IT	Sharing Economy	Identity Providers	Other
Yes	25	11	1	1	0	1	2	3	6
No	15	3	5	1	0	0	1	1	4
Don't Know	3	0	0	0	0	2	0	0	1
Total	**43**	**14**	**6**	**2**	**0**	**3**	**3**	**4**	**11**

ANALYSIS

58% of organisations said they had difficulty verifying customers, 35% don't have difficulty and the remaining 7% didn't know. The sector with the most problem with verification was financial services, with most the gambling respondents stating they do not have difficulty.

AUTHOR'S COMMENTS

The challenges in verifying customers leads back to the main benefit of a cross sector approach identified by respondents, a better customer experience. Not being able to verify people, particularly in regulated businesses like financial services is not only a frustration for the organisation, but for the customer in that it creates a poor customer experience, often ending up with the customer having to send lots of documentation through the post or going into a branch or store to have their identity verified. This is a poor experience, costs more money through marketing costs plus a decrease in operational efficiency for the organisation, and potentially if the customer cannot be verified, they cannot be on-boarded. The increase in competition online for all organisations means they need to create an on-boarding experience which allows as many customers through the process as possible. Federation of identities is one way to do this, by taking an already verified customer, and allowing them to use those credentials to open an account with an organisation in another sector.

33) WHAT CHARACTERISES CUSTOMERS WHOSE IDENTITIES ARE DIFFICULT TO VERIFY?

The characteristics below detail some of the areas identified as being problematic for organisations.

- Documents from another country
- Lack of digital evidence
- Lack of access to UK Gov verified attributes
- Verifying the history they give us
- Verifying IP against country
- Those not using credit cards
- Vulnerable clients
- International elements
- Smaller organisations
- Thin file
- Age restricted/younger
- Fraud characteristics
- New to country/immigrants
- Financially excluded
- Armed forces
- Benefits
- Duplicate customers
- Source of data not always being up to date
- Multiple email addresses
- Not eligible to vote
- Those moving around a lot

AUTHOR'S COMMENTS

Collaboration around the individuals whose identities are hard to verify is not only good for organisations but also good for customers. Individuals who are unable to be verified can end up in a cycle of being unable to access online services, for example if these individuals are in the low income bracket, and then cannot access online services which may be provided cheaper than alternatives this creates a downward spiral. This is just one example, but there are many other benefits of collaboration in this area to create increased digital inclusion for every UK citizen.

34) IF THESE CUSTOMERS WHO WERE DIFFICULT TO VERIFY HAD A DIGITAL IDENTITY WHAT VALUE WOULD THIS HAVE TO YOUR ORGANISATION?

The answers below detail some of the areas identified valuable for organisations:

- Cut cost, save time decrease risk
- Could accept more clients
- Speed up process
- Decrease fraud and risk

- Increase customer experience
- Decrease compliance burden
- Great for those on benefits
- Improve accessibility
- Improve transparency
- Engage more rapidly
- A little useful
- Increase trust for customers
- Increase efficiencies
- Depending on appetite to accept in our risk framework, could be very valuable

AUTHOR'S COMMENTS

The responses are a clear indication that there are perceived benefits in relation to the potential that a digital identity could provide to organisations.