ACHIEVING FRICTIONLESS CUSTOMER ONBOARDING

Defining the commercial business case for adopting federated digital identity in the financial service sector

Project Sponsor:

Project Participants:

Survey respondents:
HSBC, Barclays, TSB and a leading credit card provider

Written by Tony Lamb
Head of Strategy, Royal Mail Data
July 2017

Executive summary

Context

Today's consumers are interacting with online services in a variety of methods, including web browser, mobile browser and smart device apps, and have come to expect a consistent experience across all channels. Poor user experience has been shown to directly impact an organisation's financial performance, as consumers quickly choose to go elsewhere if presented with unacceptable barriers to accessing a service.

At the same time, the increase in cyber fraud is requiring greater levels of customer verification and ongoing assurance of a customer's identity. In turn, this is creating further potential barriers to customer acquisition and retention.

With the launch, and increasing take-up, by citizens of the UK Government's digital identity, GOV.UK Verify, there is an opportunity to reuse this digital identity to access non-government, commercial services in a more efficient way.

Scope

The project sought to test the hypothesis that:

> There is a commercial business case for financial service providers to accept digital identities that meet Government standards

Four leading financial service providers were surveyed and asked to rate the importance of 25 statements. The rating, and the reasons for giving these scores, informed the conclusions and recommendations for this paper.

The key questions answered in this report are

- Can a digital identity enable a frictionless and secure customer experience for financial service providers?
- What are the key considerations for the financial sector in the acceptance of digital identities?
- What are the next steps to deliver a digital identity service for the financial sector?

Conclusions

The financial service providers surveyed within the project showed enthusiasm for the concept of a reusable digital identity that meets government standards. They raised many specific questions that need to be answered before they can firmly commit to adoption.

The providers stated challenges exist in how they currently verify their customers' identities through online channels. For many application journeys, this results in the providers requiring the customer to step out of the digital. As the traditional face-to-face channel is required in order for the provider to meet their Customer Due Diligence obligations. This is particularly true for growth demographics such as:

- New to country customers
- Younger customers (<20 y/o)
- Socially and financially excluded

Top financial sector needs

- Alignment of regulatory standards to support the reuse of the digital identity
- Regulatory endorsement
- Good customer awareness
- Broad demographic reach
- Sufficient scale of verified customer identities
- Support the achievement of a fully online customer journey
- Deliver operational efficiencies and cost reduction

Modernised regulation within the European Union is driving change within the financial service sector, particularly in convenience, privacy, consent, choice and competitiveness. In an increasingly digital world, a trusted identity can support the ambition to allow customers to transact securely in the channel of their choice. As GOV.UK Verify aligns to the broader European standards, it provides a means for the financial sector to provide services in a globally interoperable way.

The financial service providers in this report placed significant value on the endorsement by their regulator of any third party provided digital identity. The current guidance for meeting their Customer Due Diligence obligations would need to be updated to support the use of digital identities. A sector-wide approach to modernising customer identity verification during on-boarding, and for ongoing relationship management, is required to drive financial service adoption. With regulatory endorsement of the GOV.UK Verify digital identity, the providers could accelerate adoption.

Having Government standards for identity, operating within a commercially driven framework, was seen as a sound business model, as it allows the freedom to develop services that meet the sector's needs of security, customer convenience, operational efficiencies and cost reduction. This framework should provide a cross sector approach to federated identity (see Glossary).

A partnership approach is also required to build customer awareness of GOV.UK Verify to allow it to be used across sectors. A collaboration of public and private sectors can work together to deliver the broad demographic reach, accessibility and the scale of verified customer identities that will drive the operational efficiencies and cost reduction for the UK economy as a whole.

Overall, this project has demonstrated how the reuse of a Government endorsed digital identity can modernise online customer verification for financial services.

Recommended next steps

Based on the responses of the financial services providers in this project, the key next step is to clarify the next level of detail in the proposals, to allow financial services organisations to fully evaluate the opportunity offered. To achieve this, the formation of a cross party working group is recommended. This group should be comprised of:

- Financial service providers
- Government Digital Service
- Identity Providers
- Regulators and Industry bodies

The working group should be tasked with the following deliverables:

1. Define the detailed target operating model
    - its governance framework
    - the resultant new risk model, and
    - an initial commercial structure to support participation
2. Alignment of the GOV.UK Verify digital identity and the financial sector standards
3. Update of regulation, guidance and industry good practice to reflect the adoption of federated identity by the financial sector.
4. A detailed growth plan for GOV.UK Verify over the next 6 months to:
    - Increase the level of knowledge and awareness of GOV.UK Verify services with citizens and financial sector providers
    - Accelerate short term uptake within Government departments
    - Provide a joint roadmap for medium term adoption cross sector
    - Outline a marketing plan for increased customer advocacy

To maintain the enthusiasm shown by the financial service providers, in parallel the Alpha phase of the project should work with willing parties to further explore the key findings, and deliver against the priority needs of the financial service sector.

Background

GOV.UK Verify is the new way for UK citizens to prove who they are to access Government services online. The UK Governments' Cabinet Office Identity Assurance Programme has contracted commercial organisations to perform the role of Identity Providers to allow consumers to create a digital identity via GOV.UK Verify. It gives safer, simpler and faster access to Government services like filing a tax or checking the information on your driving licence.

In the next four years, UK Government is forecasting to create c20million (or c40% of the UK adult population)[1] verified digital identities for UK citizens.

This paper was conceived to explore the considerations around a commercial business case for the financial sector to reuse the digital identity to access financial services products. The project was run under the Open Identity Exchange (OIX) UK.

Motivation / benefits

The UK is rapidly becoming a digital economy. Consumers increasingly expect to be able to open a bank account through digital channels easily and quickly without having to visit a branch[2]. Financial and Identity fraud are becoming more sophisticated, with physical sources of verification evidence becoming less robust e.g. Utility bills.

Regulators expect financial service providers to maintain high standards for identity verification of new customers including those who, increasingly, do not originate from the UK. Adoption by financial service providers of a digital identity that meets high Government standards may present a solution to these challenges.

EU and UK initiatives

There is a new EU Regulation on electronic identification and trust services for electronic transactions in the internal European market (eIDAS. See Glossary). eIDAS makes it possible to know how much trust sits behind a digital identity issued in any European country, allowing, at a technical level, users to assert their digital identity wherever they go in Europe. It will also facilitate activities such as electronic signatures and pre-employment screening and vetting.

A federated digital identity scheme, GOV.UK Verify, has been created in the UK in line with the eIDAS regulation. In the UK, it uses robust standards to verify identities and is being adopted across UK digital public services.

Updates to financial regulations are taking place that will drive significant change in the market over the next 3 years:

- Implementation of the EU Payment Accounts Directive (PAD) in September 2016 requires banks to offer accounts to customers located in any EU member state. The financial service providers face challenges to their processes of identification and verification of individuals across borders
- Phillip Hammond, the UK Chancellor, announced in his 2016 Autumn statement that the Government had agreed with The Joint Money Laundering Steering Group (JMLSG) that they will modernise their guidance on electronic ID verification to support the use of technology to access financial services
- Changes in the 4th Money Laundering Directive, to be implemented in June 2017, should allow organisations to rely on each other more for identity, creating the opportunity for new models for KYC to develop
- The Competition and Markets Authority is implementing a wide reaching package of reforms that ensure customers benefit from advances in technology and increased market competition. These remedies require that banks implement Open Banking by 2018 to allow consumers and small business to access and share their data securely with other banks and with third parties

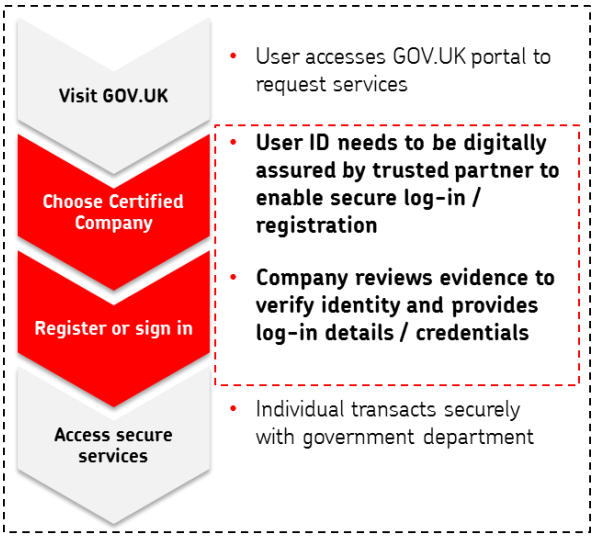
[1] Identity Assurance Programme, Market Briefing Event 2014
[2] Forrester Predictions 2016: Financial Services Execs Wake Up to Digital Transformation

- Also in 2018, the Second Payment Services Directive (PSD2) will come into force, enabling efficient and secure cross-border payments, and also requiring Open APIs to allow fair competition to new market entrants and established providers to develop innovative services
- The EU General Data Protection Regulation (GDPR), applicable from May 2018, provides new protections to customers in the storage and processing of their personal data. Enhanced privacy, consent and transparency is afforded to the customer with new obligations placed on data controllers and processors to protect the interests of the customer to whom the data relates

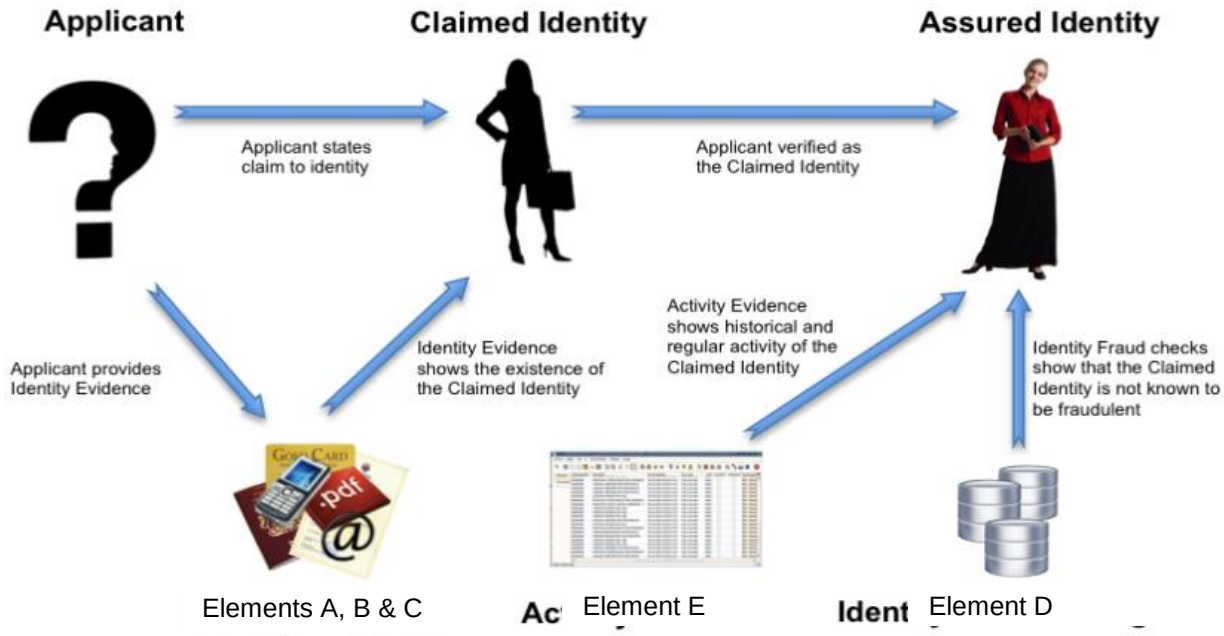
Central to these updated regulations is the need for strong customer authentication and identification that can be transacted in a quick, secure and simple way.

GOV.UK Verify

The existing GOV.UK Verify service verifies the applicant's details online, using certified third party Identity Providers. The summarised user journey is as follows



To 'identity proof' an individual using GOV.UK Verify, five elements (A to E) are captured and checked to achieve a Level of Assurance (LoA2, and soon to be launched, LoA1) verified digital identity.



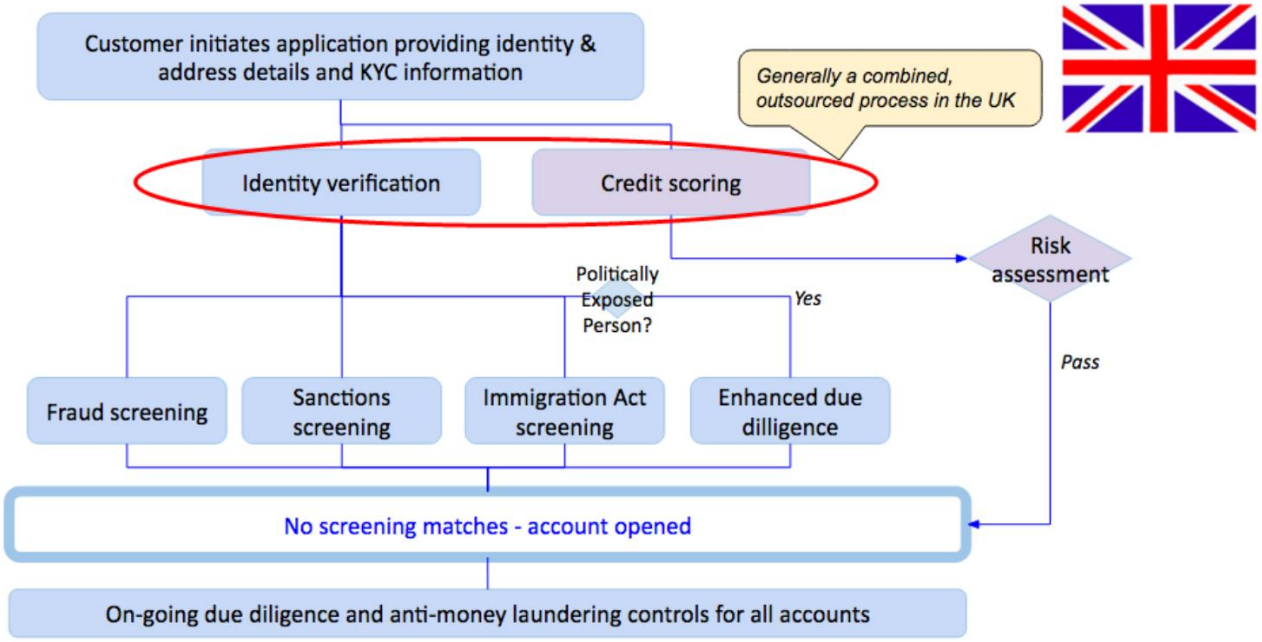
Source: Cabinet Office Good Practice Guide No. 45 Identity Proofing and Verification of an Individual

The opportunities for financial service providers

The current process to open a bank account involves seven core processes:

1. Verifying an identity and confirming the link between the applicant and the claimed identity
2. Know Your Customer (KYC) and Customer Due Diligence (CDD) processes to deter and protect the banks from being used by criminals for money laundering/terrorist financing activities, and to aid in better understanding their customers and their financial dealings to manage their risks prudently
3. Customer screening against reference data including Sanction and PEP lists
4. Enhanced Due Diligence (EDD) to further investigate applicants where an increased risk is identified
5. Product suitability for the applicant
6. Other data e.g. verified mobile number, location of device
7. Anti-impersonation requirements for non face-to-face business

This process may involve many individual steps, including physical documentation checks and their associated time delays



Source: OIX project - Digital identity across borders: opening a bank account in another EU country

The opportunities the financial service providers are looking to capitalise on are summarised as follows

- Increasing access to financial services to a wider section of the UK population that have historically had issues in opening new accounts
- Improving the customer experience during the application and authentication process, whilst not compromising security
- Reducing the level of manual intervention to process a “new to bank” application
- Optimising the ongoing process of maintaining customer information
- Providing a lower cost approach to complying with future legislation requirements

Survey Findings

The project tested the following hypothesis:

There is a commercial business case for financial service providers to accept digital identities that meet Government standards.

This assumes two use cases:

- An individual with an existing GOV.UK Verify digital identity could reuse this to apply and access financial service products.
- An individual without an existing GOV.UK Verify digital identity could obtain one during a financial service product application process and then be used to access other services in future.

To inform the conclusions and recommendations of this paper, financial service providers were surveyed. Their responses were used to identify and prioritise the key considerations for creating a commercial business case for the reuse of GOV.UK Verify digital identities.

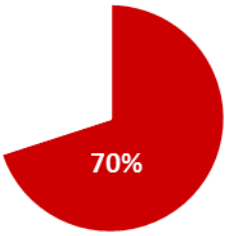
The respondents rated 25 statements, with 1 being not important, 5 being critical. The individual scores were then aggregated to derive an overall percentage score based on the importance to the financial service providers. (e.g. four responses at Critical = 100%, four responses at Not at all Important = 0%)

HSBC, Barclays, TSB and a leading credit card provider all responded, with their individual question ratings, and explanations in support of these.

The key points for each of the commercial business case considerations are summarised, along with the relative importance stated by the financial service providers surveyed.

1. User Experience

The user experience offered by a previously established digital identity is better than the identity verification experience in existing application journeys



User experience is an important consideration for financial service providers as it is directly linked to financial performance. Therefore having a service that is as good as, or better than current processes was important.

The verification process for GOV.UK Verify requires around six steps, once the applicant has selected their identity provider.

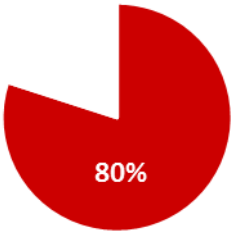
Different financial services have different risk profiles, and therefore the required proof attached to each varies. A typical bank application process for a current account involves 20-80 steps, and covers both the identity verification and the risk management activities.

Current processes can include manual confirmation of the applicant's residency at the physical address and the applicant's identity documents. Making the process work entirely online for customers would bring significant benefit to them and the financial service providers.

Once an individual has successfully created an assured identity, the existing GOV.UK Verify login process utilises strong authentication. If successful this is a good user experience, providing swift and secure access.

It is likely that in the short term, financial service providers would retain their existing login processes as they generally use more authentication factors, than GOV.UK Verify, and comply with existing requirements. This hypothesis may change as the service offering matures, and the user experience insights increase.

A reusable digital identity supports an end-to-end entirely digital journey

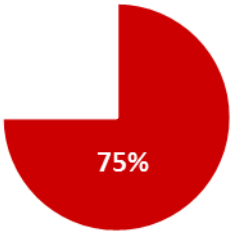


A complete end-to-end digital customer application process is a core requirement for future financial offerings.

Increasingly customers expect and demand processes that are easy-to-use and consistent with their experiences outside financial services. In addition, all the providers also saw translating this good user experience to mobile devices as "Very important".

As the GOV.UK Verify service is in an early stage of maturity, user journeys and back end processes are being optimised to maximise the successful approval of valid applicants, whilst still preventing fraudulent applications.

The reusable digital identity has a high level of customer awareness

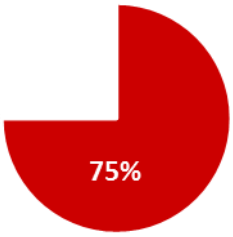


Respondents believe that increasing awareness of GOV.UK Verify, as the way to access Government services, is important to its reuse by non-Government services.

The banking sector has already done a lot of work to support customer education on existing security processes. So there needs to be comfort that consumers are able to understand the GOV.UK Verify service and what they need to do to keep themselves safe when using online services.

This needs to happen as the use is extended to financial services, otherwise there is a risk that fraudsters could leverage this confusion. This could otherwise result in a large number of vulnerable people having their identities compromised and funds stolen.

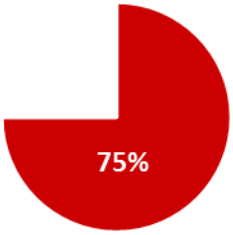
A reusable digital identity enables simple integration with mobile-first digital journeys



The digital strategies of financial services providers are frequently adopting a mobile-first philosophy. As the most frequent customer interactions are being undertaken on smart devices through mobile browsers or apps.

Any identity verification method would need to support this mobile-first philosophy by providing a good customer experience designed for smart device accessibility.

Successful verification rates are greater than 60%



For GOV.UK Verify to be adopted into the processes for new customer on boarding the rate of successful identity verification needs to be high.

However, it is important to make the distinction between a service, which successfully meets the identity verification element of the application process and whether the provider should, or wishes to, approve it.

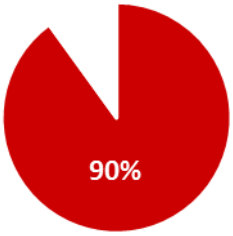
Further analysis of the verification success rates for motivated and willing customers (e.g. those who do not abandon the user journey) on GOV.UK Verify is required to benchmark it against success rates for existing financial service applications.

2. Regulatory considerations

The use of a digital identity meets the provider's regulatory approved standard for identity verification

The requirement that GOV.UK Verify aligns to common regulated industry standards was viewed as the most important of all the areas by all of the financial service providers. The existing standards are the level to which the Financial Conduct Authority (FCA) expects all providers to deliver. To maintain comfort that the providers are operating within the regulator's expectations, as well as their own risk appetite, any future solution should also deliver to this standard.

The re-verification regime for reusable digital identities meets the regulatory and risk requirements of the financial service providers

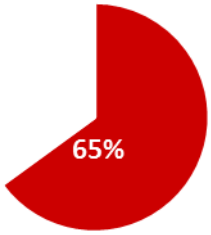


Financial service providers have a requirement to undertake certain customer due diligence checks at the point of application. GOV.UK Verify carries out checks at the time of initial verification and performs some of these checks again on a periodic basis. Currently there is a timing mismatch for performing specific identity checks

The financial service provider would either have to perform these additional checks separately, or the GOV.UK Verify service would need to be extended to include them, or the regulatory guidance would need to be changed.

The providers stated that it was important that there was future alignment on the regulatory requirements, financial service provider needs and the GOV.UK Verify re-verification regime.

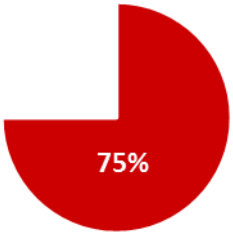
The data exchanged from the identity provider meets the financial sector's regulatory obligations



In addition to the core identity check, other data is needed to satisfy elements of customer due diligence. There is a separation between identity and entitlement. GOV.UK Verify is unlikely to provide these other attributes, but it may be a logical evolution of the service to enable entitlement checking which leverages the verified identity.

An evaluation of the data provided was out of the scope of this project and is being evaluated in a separate OIX project.

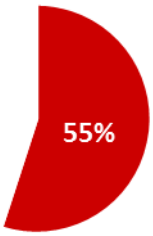
Regulatory change may need to happen to enable the complete digital application process



The updated JMLSG guidance notes around good practice in countering Money Laundering and the UK regulations supporting the Fourth Anti-Money Laundering Directive are key outstanding components. As these are not anticipated until mid 2017, a timing challenge exists in gaining the required regulatory clarification in the short term.

If GOV.UK Verify does not match the regulatory requirement for financial services this is likely to prohibit uptake.

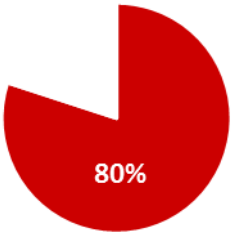
Government is the driving force for regulatory change



Whilst the Government has a role to play in setting the standard for identity, it is the respondents view that the financial sector should operate in a collaborative working group to effect regulatory change. Regulatory change to reflect the operation of eIDAS compliant digital identities could be a driver to support financial service providers in enabling the digital single market and meeting upcoming legislation in the sector.

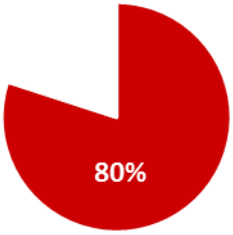
3. Population coverage

A reusable digital identity is accessible for all of the eligible UK population



The financial service providers stated that it was important that GOV.UK Verify was available to all. The service should not have any artificial barriers to access, meaning if customers have the means to verify their identity in a real world context today, a digital verification process should also support their use of the service in the future.

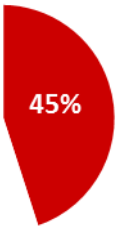
In particular, a reusable digital identity covers socially, financially and digitally excluded demographics



If GOV.UK Verify provided penetration of key segments of the population, who are currently difficult and costly to verify in a digital-only channel, this would be valued by the financial sector. Examples of excluded demographics are those aged under 20, individuals who are new to country and those with a 'thin' credit file.

The financial sector is committed to providing inclusive access to services for the societal benefit. Meeting regulatory requirements often drive these customers from digital and into more costly and less convenient traditional in-person channels. Being able to satisfy the identity part of the regulatory challenge will be beneficial for all.

The number of existing available digital identities is significant for the population



Currently, around one million digital identities exist for GOV.UK Verify, representing 1-2% of the UK adult population. In the next 4 years, UK Government have forecast that GOV.UK Verify will create c20m (or c40% of the UK adult population) verified digital identities for UK citizens.

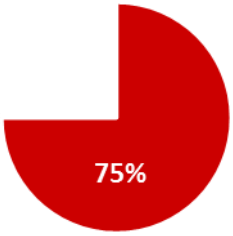
The investment into adoption of GOV.UK Verify by the financial service sector would require a critical mass of pre-existing identities. From a timeliness perspective, the surveys revealed that having five million verified identities by June 2017 would be somewhat important before the financial service sector would widely adopt the reuse of GOV.UK Verify. Therefore, it is scale, rather than speed to achieve it, that is the key requirement

Currently, c40k new GOV.UK Verify accounts are being created per month[3]. Accelerating the growth of verified identities will make a more compelling case for financial sector reuse. An agreed growth strategy for Government to increase the population coverage of GOV.UK Verify will be valuable to support financial service providers in developing a commercial business case for adoption.

Subsequent to undertaking this research, an LoA1 standard has been defined, with intention being to provide a lower entry bar to access certain services and increase social inclusion requirements.

4. Standardised federated digital identity

All customers are verified to the same robust level of assurance



Financial service providers would be satisfied with single level of identity assurance, providing that this covered a sufficient proportion of the population across a broad demographic.

The current proposition is built around assuring identities to LoA2. This standard requires a recently updated referenceable data source to match the identity to. Availability of data sources for elements C and E of the proofing process can be problematic for those aged under 20 or new to country, and individuals with a 'thin' credit file. This is one of the key challenges of the process today.

Government and the Identity Providers are working together to understand how the current solutions can be optimised to increase successful applications without increasing security risk. The LoA1 entry standard, and new forms of verification, including reusing the credentials for individuals already validated to a robust standard, are being assessed.

[3] https://www.gov.uk/performance/govuk-verify

There is a single method for digital identity proofing of customers

Financial service providers did not see having a single means of digital identity verification as an important consideration in whether to adopt reuse of GOV.UK Verify. The key point is the level of assurance, rather than the source. The introduction of LoA1 has already responded to this demand for multiple assured standards.

In considering the reuse of GOV.UK Verify identities, financial service providers also need to agree how to cater for customers without an existing digital identity. The following options are available:

1. The existing application process for financial services could be maintained for customers without an existing GOV.UK Verify identity. This would mean two systems need to be maintained, potentially increasing costs, and causing customer confusion.
2. The ability to create a new GOV.UK Verify identity within the financial service application journey. With LoA1 this would create a two level identity standard, requiring the demise of existing financial services verification processes and a commercial model to allow this.
3. A standalone process operated outside the GOV.UK Verify process by commercial organisations, and used to access financial products and potentially create a new GOV.UK Verify account.

The impacts of each option would need to be assessed to understand the risk / benefit profile. This includes the costs for adoption, potential efficiencies from a new identity process and ensuring there are no barriers to adoption.

A standards-based digital identity program is operated by Government

Whether the GOV.UK Verify service is delivered by Government or a Commercial organisation was not seen as an important consideration by the financial service providers.

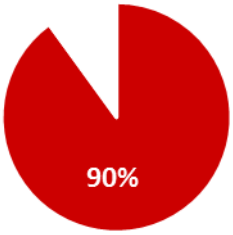
The financial service providers required that customers trusted the service, and that the identity has legal and regulatory approval. The value of Government setting the identity proofing standards and maintaining the integrity of the service to deliver a secure, safe and simple customer experience was though recognised.

A suggested optimal hybrid approach would be a commercially operated hub, with Government setting and governing the service and assurance standards. This would allow the service offering to quickly evolve in response to market forces and demand, but with the confidence gained from a Government endorsed identity standard. A previous OIX report, UK Private Sector Needs For Identity Assurance[4], had also concluded that the optimal structure would be from a public private cross sector approach to online identity needs.

[4] http://oixuk.org/wp-content/uploads/2016/09/UK-Private-Sector-Needs-for-Identity-Assurance.pdf

5. Commercial considerations

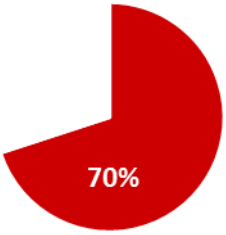
The reuse of an existing digital identity delivers operational efficiencies and cost reductions



Financial service providers stated that the replacement of several existing manual, and time-consuming, processes was a key benefit. In particular, this related to the processing costs for customers who were classified as exceptions, which are significantly higher than for customers on-boarded through wholly digital means.

Overall, the relative benefits of increased income from new customers, migration of customers to digital channels, operational efficiencies and compliance risk reduction will drive the business case.

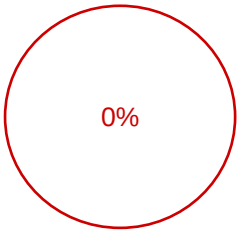
The cost for reuse of an existing digital identity is lower than current methods



The cost of currently verifying an identity needs to be understood for a range of customer types. However, the general principle is that the cost of reusing a digital identity needs to be lower than the existing model, or the benefits greater, to justify a change.

The cost also relates to the overall benefits of increasing access to financial services to a wider section of the UK, particularly those that have historically had issues opening new accounts. If the cost of reusing GOV.UK Verify was too high it could prove prohibitive for lower revenue generating financial service products.

An annual licensing model for reuse of an existing digital identity is used

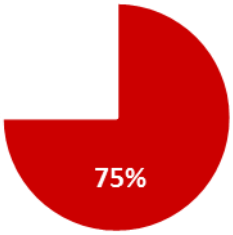


Whether the payment model was based on a transactional or a licence structure was not at all important to the financial service providers.

New commercial terms will need to be agreed with the existing Identity Providers to allow verified identities to be used outside of the existing GOV.UK Verify agreement. The differences in the risk and benefits profile between a private sector Verify solution enabling access to financial rather than Government services, and the Target Operating Model for this, needs to be considered as part of these terms.

If a commercial hub is required, the hub provider will require payment for their service. Once again, further definition of the service requirements, user demand and the risk model will be required before this can be considered. Dependent on the services offered, different parts of the value chain would require payment. The identity market is likely to evolve over time as the ecosystem matures.

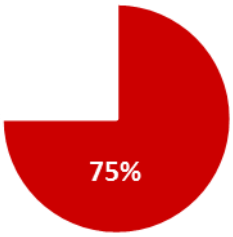
The capital cost to integrate the reuse of an existing digital identity into financial service application process provides a short term return on investment



In the survey, a suggested investment amount of under £10million was proposed. There was a range of responses from “Important” to “Critical”. Some responses focused on the value of the end benefits, while others pointed out that high entry costs would limit the adoption by smaller providers.

6. Risk management

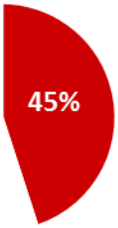
The model for risk management and redress recognises the use of a standards based digital identity



Current FCA regulation underpins the existing risk model in the market. Therefore, the risk implications of the proposed process changes will need to be reviewed by the FCA. In the current verification model the financial service provider will, on certain occasions, make the decision on whether a customer is verified, based upon third party inputs. For example, based on information from a Credit Reference Agency.

In the new model, the provider would rely on a third party to provide this verification. The risk relationship therefore needs to be assessed in this new arrangement and the impact of this considered. Who the contracting parties are needs to be defined, and therefore what the risk model is for all the parties involved (service provider, Government, hub provider, identity provider). If the risk is simply passed onto the other parties in the process, this may provide a level of risk a service provider would be unwilling to accept. The process for resolving error or fraud driven issues also needs to be defined.

The financial services providers confidence in the digital identity is greater than with existing processes



As part of the customer due diligence processes, financial service providers have existing digital means of verifying identities. Current processes would need to be reviewed to determine the impact of accepting a third party digital identity:

- Predicted fraud losses under the new process
- Compliance with new and existing regulatory requirements, and the impact of not meeting them
- The appropriate systems and controls that need to be in place, and the risk of not having these
- Regulatory requirements around anti-impersonation and the increased risk presented in a transaction where the customer is not physically present

The risk profile of the digital identity is lower than with existing verification methods

A number of areas will need to be assessed for risk once the new operating model is understood. These may have a positive or negative impact on the business risk profile. Key consideration areas suggested by the financial service providers include:

- Reputational and revenue risk from an inferior service and/or negative customer reaction
- Weighing up the risks/opportunities between physical documents and digital identity including any supporting information provided to obtain it.

7. Other considerations

Financial service providers can choose the Identity Providers they accept identities from

GOV.UK Verify digital identities are currently created by seven Identity Providers. The market share of verified identities will vary with each identity provider.

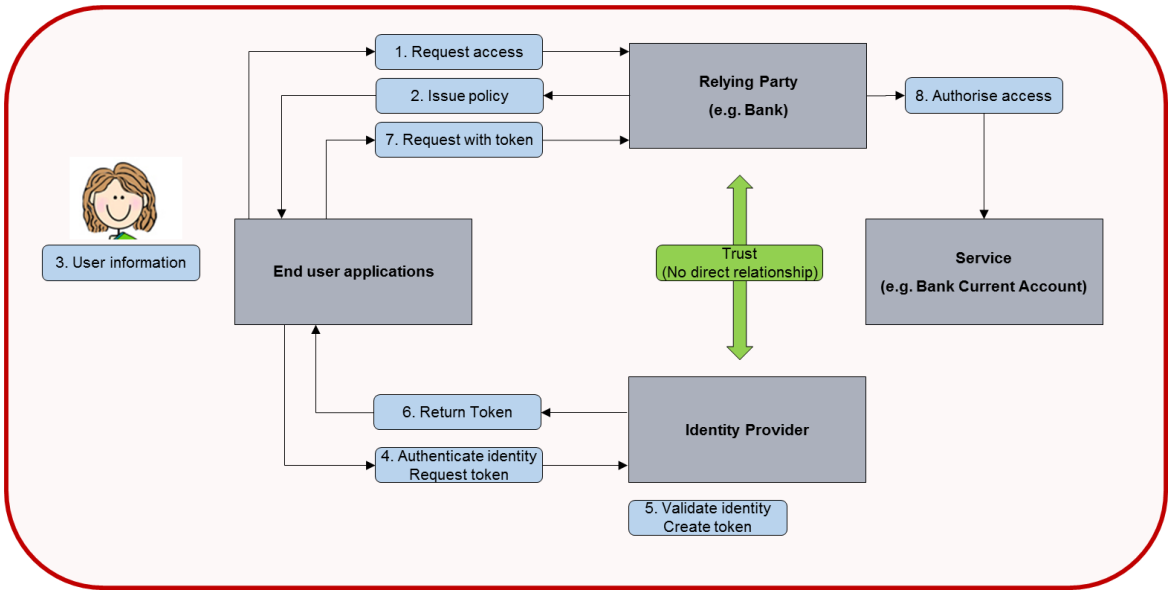
Brand recognition was, the research showed, a key determining factor in consumers' selection of Identity Provider, other elements also influence the end distribution of customers. For a financial service provider to gain maximum benefit from the reuse of GOV.UK Verify, the participation of all Identity Providers would be required. To begin adoption, it may be adequate for only those identity providers with the majority of customers to participate.

The digital identity service is available for adoption to begin and for customers to use in 2017

To assess any timing considerations, it was suggested that the GOV.UK Verify service was live for reuse by June 2017. The financial service providers did not see this as important. Having the time to define and assess the service requirements against the benefits of a standards based digital identity would be beneficial. It was seen as more important to get the service right than to make it available quickly. The window of opportunity needs to be seized in the next six months to provide a clearer view of the scale of the opportunity.

Appendix

A model for clear separation of roles when dealing with digital identities



Survey Methodology

The following organisations participated in the survey in September 2016 that underpins this paper; HSBC, Barclays, TSB and a leading credit card provider.
Two use cases were assessed when answering the questions

i. An individual with an existing Government Digital ID could reuse this to apply and access financial services products
ii. An individual without an existing Government Digital ID could use a Verify process to obtain a Digital ID that would allow access a specific financial services product, but then be used to access others

To undertake the survey, an initial shortlist of key commercial considerations was created. These criteria were then structured into 25 statements, and a summarised hypothesis. Each organisation rated each statement (1 being not important, 5 being critical) and the hypothesis, and provided explanations for their rating.

The survey was then followed up with a phone interview to capture additional key points behind the answers provided, and gain approval to publish the results.

At the time of the survey, a single assured identity standard at LoA2 was offered under the Verify service. Following this, in March 2017, a new LoA1 assurance standard was issued. Comments in the report have been added to reflect this change in assurance level, though the take-up of this new standard and use by Government departments are to be determined later in 2017

Glossary

Digital identity

The digital representation of a user that's authenticated through the use of a credential.

Identity assurance

The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity. Proving you are who you say you are to a certain level of confidence.

Open identity exchange (OIX)

A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon). Members advance their market position through joint research and engaging in pilot projects to test real world use cases. The results of these efforts are published via OIX white papers and shared publically via OIX workshops.

Identity Provider (IDP)

Private sector organisations paid by the Government to verify a user is who they say they are and assert verified data that identifies them to the relying party. The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority).

Relying Party

The organisation using the Federated Identity. The relying party trusts an identity provider who can verify the correctness of the identity or other claimed statement. A relying party authorises based on statements (claims) verified by an identity provider. This mechanism is typically called claims-based security.

Federated Identity

Describes the technologies, standards and use-cases that serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user administration

eIDAS

EU regulation of electronic identification and trust services for electronic transactions in the internal European market (eIDAS). Will allow users to assert their digital identity wherever they go in Europe, to access Government and Commercial services. It will also facilitate activities such as electronic signatures and pre-employment screening and vetting. https://ec.europa.eu/digital-single-market/en/e-identification