Creating a Digital Identity in Jersey (Leveraging the Experience of the UK Identity assurance programme)

The findings of a Discovery Project

By Rob Laurence (Innovate Identity)
May 2016

Participants

About the Open Identity Exchange (OIX)

OIX is working directly with the private sector and governments to enable the expansion of online identity services and adoption of new online identity products, with a focus on the citizen.

OIX will help organisations create schemes leveraging or defining appropriate open identity standards. It will help create certification requirements for schemes and services that will be listed on an open registry in order to assist adoption and enable interoperability and competition in global markets.

OIX will accomplish its aims through communication, open workshops and collaborative projects, the results of which are always published in white papers, in order to achieve the collective aims of its members. Each project is conducted under IPR protection and a common set of rules, for the benefit of all stakeholders.

States of Jersey and the participants in this project are members of OIX.

Executive summary

States of Jersey is embarking on an eGovernment programme to improve customer service and make government a more efficient and "joined-up" business.

This requires transforming the way

- Services are designed and delivered
- Systems operate together
- Data is used across the business
- Systems and data are kept safe

A number of core components have been identified that will help enable this transformation. One of these is a common capability to verify and authenticate individual people online through the adoption of a digital identity scheme.

Across the world countries are developing national digital identity schemes. Designs vary. Some are based on existing national identity cards as in Germany. Some originate from the banking sector and have been adopted by government, as in Norway and Denmark. And some, as in the UK, have been developed from scratch by governments.

Small jurisdictions, such as Jersey, must choose whether they allocate resources to develop their own schemes from scratch or leverage the work done elsewhere through collaboration and shared experiences, with the aim of adopting an existing model framework.

States of Jersey commissioned an OIX Discovery project to explore how the knowledge, expertise and components of one of these models, the UK's GOV.UK Verify identity assurance scheme, could be leveraged to provide a cost-effective solution to meet Jersey's requirements.

The conclusions drawn from this project are as follows:

1. Jersey's history and culture is very close to the UK. It's financial, legal and administrative systems, whilst different to the UK, bear close resemblance. Many of the guiding principles that underline the design of the UK scheme could equally be applied to Jersey to meet its very similar requirements.
2. States of Jersey's requirements for a digital identity scheme align closely with the GOV.UK Verify model, with two exceptions. The first is assisted (face-to-face) identity proofing, which is currently the subject of an OIX project in the UK; the second is business identity which is due to be investigated in the UK later this year. Potentially, States of Jersey could collaborate with the UK, possibly through OIX, to provide a digital test bed to develop propositions to meet these requirements.
3. The UK Government Digital Service (GDS) has published a comprehensive set of documents relating to the specifications, design, build and operation of the UK scheme. These publications also cover third party procurement and service agreements. These are available to the States of Jersey and would potentially underpin a government-led programme of work to implement an equivalent digital identity scheme in Jersey.

4. Identity providers have designed and built their platforms for reuse across different jurisdictions, thereby spreading aggregated development costs. Currently, the UK is the first instance of this type of platform and Jersey would potentially be the first example of reuse.
5. The UK government envisages that eventually there will be many "certified" identity providers in the market. If Jersey was to follow the UK model, this number may need to be capped to ensure it is attractive and commercially viable for those selected identity providers.
6. First time citizen registration with an identity provider is based on matching the citizen's claimed identity with existing "footprints" in government registers, government issued documentation, financial "footprints" and evidence of current and past activity. In the UK this generally involves access to passport and driving licence data, electoral registers, and banking and credit history. The States of Jersey would need to make available comparable data sources to the identity providers.
7. The GOV.UK Verify model provides a gateway (hub) between central government service providers and identity providers. The hub permits a citizen to assert their identity digitally whilst maintaining anonymity between the two end points. This hub has been developed by GDS. Currently, it is not yet known whether this hub will be made available to other public sector bodies such as the NHS or local authorities, or whether they will need to develop or procure their own hubs. The assumption has been made that States of Jersey will need to develop or procure its own hub.
8. The UK programme has been delivered through a collaboration between GDS and the private sector over the past three years. States of Jersey would be able to leverage the knowledge and experience gained in the UK to implement a digital identity scheme in Jersey in a much shorter timeframe.

Overall, the findings of the project confirm that a scheme very similar to that in the UK could be implemented successfully in Jersey. There is sufficient interest from the UK's certified identity providers and European hub providers to suggest this approach should readily be achievable.

The knowledge gained from the UK programme, plus the significant investments already made by private sector companies, give rise to confidence in States of Jersey being able to commission a digital identity scheme quickly, at low risk, and with relatively low upfront costs.

Following the conclusion of this project, it is recommended that States of Jersey, in collaboration with other interested parties, considers undertaking an OIX Alpha project to build and test a prototype of an identity assurance hub for Jersey, based on the published GOV.UK Verify specifications. The project should also include user research into the design and development of user journeys to register for a digital identity and use this within the context of a government service.

Introduction

Table of Contents

The project set out to test the hypothesis that the UK government's identity assurance model could be adapted economically for Jersey, with the support of the certified UK identity providers and potential identity assurance hub providers, to meet the requirements of States of Jersey. The hypothesis also considered whether this will create an attractive market opportunity for one or more of these providers.

The project involved a collaboration between States of Jersey and three UK certified identity providers: Digidentity, Experian, and Verizon. Innovate Identity provided project management services and subject matter expertise.

Further to this, guidance was sought from the GDS privacy officer on the differences between the data protection legislation in the UK and Jersey, and the impact of the forthcoming EU General Data Protection Regulation (GDPR).

The principal aims of the project were to establish

(1) Whether the model for the UK's identity assurance scheme would fit with the requirements for States of Jersey
(2) Whether the current certified GOV.UK Verify identity providers could provide the same digital identity to States of Jersey as a commercially viable business model
(3) The requirements and technical design principles for an identity assurance hub

The project was conducted through a series of three workshops that addressed

- States of Jersey eGovernment strategy and requirements for a digital identity as a common component of service redesign
- how these requirements could be met by the existing identity providers' services
- where further development of these services would be required
- the high level requirements for an identity assurance hub
- commercial principles and models
- the citizen's rights to privacy and the law

The starting point for this project was to share an in-depth understanding of how the UK government's identity assurance model has been developed. This covered the recent history of the UK identity card and National Identity Scheme, and the reasons for its termination in

2010; the need for a digital identity assurance scheme and the adoption of a federated identity model.

The project team reviewed the approach taken by the UK government, through GDS, and how the privacy of the individual and security of their data was paramount in determining the future design. The UK's Privacy and Consumer Advisory Group's Identity Assurance Principles were considered in the context of the Data Protection (Jersey) Law 2005.

The project team moved on to consider the architecture of the UK scheme and where there may be variances from this. Areas investigated included whether there should be one or more identity providers, the need for an identity assurance hub, and the availability of trusted sources of data to underpin the identity proofing process. These are discussed later in the report.

The project team also recognised the contribution of OIX in the UK and how it promotes collaboration, transparency and shared learning between the public and private sectors; and how this collaboration has been a crucial factor in giving the private sector identity providers the confidence to invest significant time and resources to develop services in support of the UK scheme.

In this paper the relationship of Jersey to the UK is examined, where there are close similarities but also where there are differences and the potential impact that might have on the ability to adopt a scheme close to the UK's. States of Jersey's requirements for digital identity are reviewed and the appropriateness of the UK scheme is considered, not only to meet business and user needs but also to be commercially viable for all stakeholders. Finally, consideration is given to the collateral and support that would be available to States of Jersey and how it might be leveraged to deliver the digital identity scheme.

Jersey and its relationship with the UK

Jersey, along with Guernsey and the Isle of Man, is a Crown Dependency of the UK with the same constitutional monarchy. It is a self-governing parliamentary democracy with its own financial, legal and administrative systems, and the power of self-determination.

As a Crown Dependency, the Crown is ultimately responsible for "good governance", ratification of island legislation (through Royal Ascent), international representation and defence. Jersey has a separate international identity to that of the UK. It is not a member of the European Union but has a special relationship with it, notably being treated as within the European Community for the purposes of free trade.

Jersey has a population of approximately 100,800. At the last census, this was split by birth place as follows:[1]

Place of Birth	Persons	Percentage
Jersey	48,653	50
British Isles	30,223	31
Portugal / Madeira	7,031	7
Poland	3,133	3
Republic of Ireland	1,880	2
Other European country	3,146	3
Elsewhere	3,791	4
Total	**97,857**	**100**

Despite its historical connections with France, less than 1% of the population was born there.

Similar legislation and regulation

In terms of legislation and regulation pertinent to the subject of this paper, Jersey has the following.

Data Protection (Jersey) Law 2005

The law implements the European Data Protection Directive 1995 and is modelled on the UK Data Protection Act 1998. The independent statutory authority that oversees its implementation is The Office of the Information Commissioner.

Jersey Financial Services Commission

The Commission is responsible for the regulation, supervision and development of the financial services industry in Jersey. The Commission is a member of several international regulatory bodies and participates in regulatory seminars and forums both within the UK and EU, and further afield.

Jersey has primary and secondary legislation covering anti-money laundering and counter terrorist financing[2].

eGov strategy

The programme's objectives are to create:

- Enhanced customer services: Re-engineered services organised around customers and delivered online.
- A more efficient public sector: Best use of data, stripping out duplicated activity, cutting across internal boundaries.

[1] See report from Jersey census 2011
http://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/R%20CensusBulletin2%2020111214%20SU.pdf
[2] Full list can be found at http://www.jerseyfsc.org/anti-money_laundering/legislation.asp

- Stimulation of the local digital industry: Spending money in local industry to build and deliver services and products and ensuring skills transfer when buying in services from off-island.

In support of these objectives, four work streams – Enterprise Architecture, Enterprise Data, eGovernment Infrastructure and Access Jersey together with foreground projects and programmes will be delivered in the period 2015-18.

The UK identity assurance programme

A brief history

In 2012 the UK government published the Government Digital Strategy (subsequently updated in 2013[3]). Government Digital Service (GDS) was formed within the Cabinet Office to implement this strategy.

This strategy initially contained 14 actions for the government to undertake to become digital by default. One of these, to lead in the definition and delivery of a new suite of common technology platforms to underpin the new generation of digital services, resulted in the creation of the identity assurance programme and, ultimately, GOV.UK Verify.

The identity assurance programme's brief was to develop a framework to enable federated identity assurance to be adopted across government services in due course. All of the work in this area was guided by the Identity Assurance Principles drawn up by the Privacy and Consumer Advisory Group[4].

The identity assurance programme comprised teams of user researchers, technical architects and developers, with legal and privacy representation.

GDS became a board member of the Open Identity Exchange (OIX) and collaborated with private sector organisations to develop aspects of the programme, including the participation of identity providers.

Six major government departments have been engaged in a series of Discovery, Alpha and Beta projects to transform 15 government services, many of which require users to identify themselves. The identity assurance scheme has been developed foremost around user needs to ultimately deliver the business requirements.

[3] https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy
[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

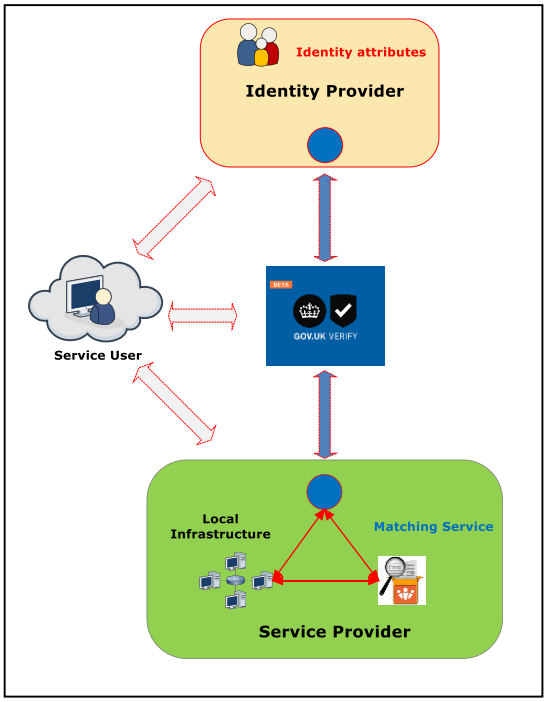
GOV.UK Verify Launched

In October 2014, the UK government's identity assurance scheme was branded as GOV.UK Verify and launched in a series of public Beta services.

The scheme comprises a GDS-developed identity assurance hub, approved identity providers and government service providers.

The hub manages communications between users, identity providers and government service providers. It allows users to select and register with an identity provider of their choosing, and then use their assured identity to access digital services.

By April 2016, more than 500,000 people had registered for a digital identity with the identity providers with more than 1.3 million "sign-ins" to government services.



A full list of the published GOV.UK Verify specifications and documents is shown in Appendix A.

GOV.UK Verify

The UK government has developed GOV.UK Verify, a new way for citizens to safely and securely prove they are who they say they are entirely online when accessing digital public services provided by central government. GOV.UK Verify uses certified private sector companies to conduct identity verification checks according to published government standards. The user chooses which certified company they would like to use to establish their digital identity. A set of nine principles guides the design of the identity assurance system. A digital identity created with a certified company through GOV.UK Verify can currently be used to access an increasing range of central government services on GOV.UK. In future, citizens might also be able to assert their digital identity in transactions with local government, NHS and the private sector. How this would operate in practice has yet to be established.

Jersey's requirements for a digital identity scheme

Background

States of Jersey has carried out an analysis of its business requirements for a digital identity in support of the eGovernment transformation programme. This analysis involved internal and external stakeholders across government departments and the public sector.

In addition to this analysis, States of Jersey has reviewed the implementation of a number of digital identity schemes across Europe, considering cultural, social, economic and political influences, as well as technical developments and standards.

A set of requirements has been drawn up to be met by any future digital identity scheme. The principal requirements are shown in the following table.

Requirement	Comment	How Verify meets these requirements
Citizen's privacy is respected and has control of how personal data is shared and used	The scheme must comply with current States of Jersey Data Protection Law and the proposed EU General Data Protection Regulation.	Verify was designed on a set of identity assurance principles, independently formed and based on the Data Protection Act 1998.
Compatibility and interoperability with national schemes	The scheme should be compatible with other national schemes being developed within the EU and capable of interoperability within the forthcoming eIDAS framework. This means a citizen with, for instance, a UK or Portuguese digital identity should be able to use this in States of Jersey.	The UK government has been proactive in the formation of the EU eIDAS Regulation and Verify has been designed to meet future interoperability and mutual acceptance criteria.
Operates as a Service	The scheme can be procured as an existing service adaptable with minimal changes for use in States of Jersey.	This is the Verify scheme model.
Costs scale in proportion to take-up	Cost of service aligned to user registrations and usage.	This is the Verify scheme model.
End-to-end solution	A complete scheme comprising one or more identity providers and hubs that relying parties (States of Jersey service providers) can connect to in a common manner.	This is the Verify scheme model.

Open standards	The scheme must not be restricted by current technology or proprietary software.	This is the Verify scheme model.
Equivalence to GPG44 and GPG45 levels of assurance (see note below)	The verification, registration and authentication of citizens must be equivalent to LoA2 as defined by the UK guidance. Some future States of Jersey services may require higher levels of assurance.	This has been implemented within Verify. Certified identity providers have to provide all levels of assurance.
Assisted identity proofing	The scheme will need to support face-to-face and assisted identity proofing.	This is a future requirement of Verify that is under investigation within an OIX project.
Business identity	The scheme will need to be capable of supporting authorised and delegated identity assurance within a business reporting function to States of Jersey.	This is a future requirement of Verify that will be explored this year in an OIX Discovery project.
Extendable to private sector	Citizens could use the same digital identity to access private sector services, eg opening a bank account.	GDS is engaged with the private sector and is sponsoring several OIX projects to look at take-up by the private sector.

Note. These Good Practice Guides (GPGs) are issued jointly by CESG, the UK's National Technical Authority on Information Assurance, and GDS. Links to these guides can be found in Appendix A.

Adopting the UK model in Jersey

The UK model is attractive as it meets today all but two of the high level requirements of a scheme for Jersey. These two exceptions are future requirements of the UK scheme. Some specific areas pertinent to Jersey have been considered at a more detailed level. These are set out below.

Single versus multiple identity providers

The project team considered two scenarios. The first of these assumed one identity provider, the second several identity providers.

The following tables identify the strengths and weaknesses of each scenario.

Table 1. A single identity provider.

Strengths

- White labelled for States of Jersey
- Simplify branding – one Jersey brand

Weaknesses

- No choice for citizen
- Stifles competition and innovation
- No downward pressure on costs
- Limited approach to registration and authentication
- Creates central identity database "honeypot"
- Risk if identity provider fails future audit
- Risk if identity provider leaves marketplace or is taken over
- Creates problem at end of contract – complex exit arrangements

Table 2. Multiple identity providers.

Strengths

- Creates competitive environment with downward pressure on costs
- Citizen has choice of identity provider
- Promotes identity provider differentiation to help reach different sectors of market
- Option to sanction / remove non-performing, non-compliant IdPs
- Promotes innovation and opportunity for identity providers to develop new services
- No central database

Weaknesses

- Initially more confusing for citizen to understand digital identity model
- Administratively more time-consuming

The conclusions drawn were that the multiple identity providers' scenario was preferable as it better met the privacy by design principles and provided a more robust and future proof environment to take forward.

Availability of an identity assurance hub

The identity assurance hub manages communications between users, identity providers and government service providers. It allows users to select and register with an identity provider and then use their assured identity to access government services.

The presence of the hub ensures many of the principles of identity assurance can be delivered securely and with integrity, maintaining user confidence in the scheme.

In a single identity provider scenario, the hub has limited value; but in a multi identity provider environment, it is essential.

In the UK, GOV.UK Verify makes use of a single hub that has been built by GDS. The short to medium term direction is to establish a market for private sector hubs, developed using published specifications for sharing identity attributes (OASIS SAML 2.0)[5], that will potentially meet public and private sector needs. Currently though, this market does not exist although several organisations have developed similar hubs elsewhere.

States of Jersey has two options to consider. The first to build its own hub, the second to buy from the private sector.

The following table looks at the pros and cons of each approach.

Build

- Could be based on published GOV.UK Verify technical profiles
- Totally under States of Jersey's control
- Higher initial cost
- Possible development and technical constraints

Buy

- Could be based on published GOV.UK Verify technical profiles
- Wider acceptance by private sector
- Competitive procurement process possible

GDS has developed two additional services that operate in conjunction with the hub.

The first of these is the Matching Service that returns identity attribute data to the service provider from the identity provider. This aids the matching process to an existing user account within the service provider's environment.

The second is the Document Checking Service that is used by the identity providers to verify user-supplied passport and driving licence details with the source datasets within Her Majesty's Passport Office (HMPO) and the Driver and Vehicle Licensing Agency (DVLA).

[5] https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions

Initial discussions with GDS suggest that these services could be made available to States of Jersey. It is the intent of GDS to go Open Source with the hub to stimulate a new market of private sector hub providers.

Sources of identity evidence in Jersey

Identity providers are responsible for identity proofing an individual. Comprehensive guidance is set out in the publication: Good Practice Guide No. 45. Identity Proofing and Verification of an Individual[6]. Within the context of data sources, this document provides guidance regarding the acceptability, validation and verification of identity evidence. Examples of identity evidence are provided.

The sources of identity evidence in Jersey has been mapped to those presented as examples in the UK. The results of this are shown in Appendix B.

The conclusions reached are as follows:

1. Sufficient equivalent government and financial services sources of identity evidence exist in Jersey to enable identity proofing to be performed both online and, where needed, in person.
2. Changes in legislation may be required in some instances to permit access for such purposes (this isn't currently viewed as a major issue).

Standards and certification of operation

In the UK, identity providers are contracted to provide services to government that meet the requirements set out in the IPV Operations Manual[7].

These requirements cover the identity management timeline from registration to deregistration. Standards for validation, verification, authentication, countering fraud, and maintaining accurate data fall within this. Comprehensive guidance is provided to show how identity providers can demonstrate they are acting in line with good industry practice.

Identity providers' operations are assessed and certified by independent organisations – themselves assessed and certified by government as being capable of providing such services.

Assessment takes place over a period of months. It is resource consuming and costs identity providers in excess of £100k. Subsequent audits and reviews are undertaken to ensure requirements continue to be met.

For a Jersey model based on the UK scheme, it is envisaged that assessment would be fast-tracked for UK certified identity providers. The assessment and certification would be based on the requirements of States of Jersey which vary from the UK scheme, resulting in different operating standards and guidance.

---

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383109/IPV_Operations_Manual_v2.3.1_Redacted.pdf

Meeting future requirements

Over and beyond the initial considerations to launch a service in Jersey, three further requirements need to be addressed soon after:

1. In-person identity proofing
2. Business identity
3. Use by the private sector

These areas are currently subject to initial review in the UK and are expected to progress during the course of the next 12 months.

In-person identity proofing

In-person or face-to-face identity proofing requires the citizen to visit an approved location in order to complete the registration process to obtain a digital identity. This might be a States of Jersey or parish office, or it could be an organisation such as a bank. There are a number of possible cases where in-person identity proofing may be necessary:

1. A citizen is unable to complete the online registration for a digital identity with an identity provider.
2. A citizen is unwilling to try online registration, perhaps through a lack of confidence or trust, and seeks assistance and assurance.
3. A higher level of identity assurance is required by a service that can only be achieved through the vetting of specific identity documents or through the capture of biometric data.

GPG45 covers in-person proofing standards and guidance.

A straightforward approach to implement this would be to allow identity providers to set up "agency" agreements with third parties to provide services on their behalf. An alternative approach would be for States of Jersey offices to act as intermediaries between the citizen and the chosen identity provider and "vouch" for the individual's identity from identity evidence produced.

The concept of in-person proofing is to be investigated in the UK as part of OIX project due to commence mid-2016.

Business identity

States of Jersey will require all businesses to fulfil statutory reporting online. It is envisaged that company employees with delegated authority (from their employer) to complete this function will need to obtain a digital identity. The mechanism to do this has yet to be determined, although it is desirable that this could be achieved using the identity providers and linking digital identities specifically to business role and responsibility through some sort of delegated approval process.

GDS has stated that it wishes to investigate this as an OIX Discovery project later in 2016.

Extending the States of Jersey scheme to the private sector

The financial services sector in Jersey is keen to embrace new technology and reduce the costs of compliance for firms and improve the customer experience. In 2015, the Jersey Financial

Services Commission undertook a consultation on electronic Customer Due Diligence (CDD) proposals and the provision of guidance on how devices such as smartphones and tablets could be used within CDD processes[8].

Although this didn't go as far as addressing digital identities, these devices play an important role in any future deployment of a digital identity scheme.

Jersey has a thriving Fintech community spanning many areas from cryptocurrency to KYC. Digital identity fits within KYC as a technology that has the potential to transform CDD processes. States of Jersey would like to see a collaborative approach taken across government, the Fintech community and financial services sector, and other areas of the private sector, to develop a common digital identity scheme.

Interoperability with the UK and eIDAS

The UK government provides a small number of services to Jersey, the processing of passport applications being one. Travel between the mainland and Jersey is driven by business and leisure activity. Sometimes there is a need for UK citizens to interact with services in Jersey (eg healthcare) and vice versa. Reciprocal arrangements are in place.

Today, Jersey citizens are able to obtain a digital identity through GOV.UK Verify.

States of Jersey has a strongly desirable requirement that digital identities issued under either scheme to be interchangeable to access services, both in the public and private sectors. For example, a UK citizen could use their digital identity obtained from the Verify scheme to identify themselves in Jersey, with reciprocal arrangements applying.

Going forward, the European Union's Electronic Identification and Trust Services (eIDAS) Regulation mandates mutual recognition of electronic (ie digital) identities by member states from mid-2018. Although Jersey is not a member of the EU, it has a special relationship that means the island is treated as part of the European Community for the purposes of free trade in goods.

Today, almost 20% of Jersey's population are nationals from European countries, other than the UK. A future digital identity scheme needs to support all Jersey's citizens and residents, and its position within Europe. Interoperability, as part of the eIDAS Regulation, is a requirement of the scheme.

Higher levels of assurance

In the UK the Government Digital Strategy is initially targeting services for transformation that have a high usage and require digital identities that meet Level of Assurance (LoA) 2. This is defined as "*a claimed identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the applicant is the owner of that identity might be offered in support of civil proceedings*".

There are two additional levels, 3 and 4, defined. Higher levels of assurance may be required where there are higher risks associated with privacy, safety and security. For example, in the

[8] http://www.jerseyfsc.org/pdf/Consultation-Paper-No-9-2015-E-CDD.docx-.pdf

disclosure of medical records. LoA4 is unlikely to be required outside of Defence. The UK has yet to address these areas in practice, although the standards and guidance are in place.

Similarly, States of Jersey will potentially have need for higher levels of identity assurance.

Risks and risk mitigation

The project team considered the risks involved in adopting the UK model and how these could be mitigated.

Risk	Comment	Mitigation
Availability of the GDS Document Checking Service (DCS) to verify passport information used as identity evidence.		Further discussions will need to ascertain if this service could be made available to States of Jersey. The alternative could be for HMPO to provide a separate API to the hub or IdPs.
Ability of a private sector hub provider to build the hub based on GDS published information.	GDS wishes to stimulate a market of private sector hub providers through a number of OIX projects. Initially, these are focusing on reuse of digital identities in the financial services sector.	Scope an OIX Alpha project to develop a hub and conduct end-to-end testing with an identity provider and relying party stub.
Access to Jersey data sources including driving licences.	These are required as trusted sources of data available to the identity providers, to enable online registration for a digital identity.	States of Jersey has raised this with internal lawyers and the Data Protection Commission.

Commercial principles and models

UK model

The UK has contracted with a number of identity providers to provide citizen registration and digital identity authentication services. Currently, there are 8 certified identity providers.

The commercial model is fundamentally a registration based model. Once a citizen has registered with an identity provider and been issued with a digital identity, the identity provider receives a payment on the first use of the digital identity with a government service provider. The payment covers an unlimited number of citizen “sign-ins” to government services over a period of 12 months.

After 12 months and on the occasion of the next citizen "sign-in", the identity provider has to perform a further set of checks of the citizen's identity, for which it receives a further payment to cover the next 12 months' usage. Payment in second and subsequent years is less than the first year.

The commercial model is designed to seed the market for digital identities and help identity providers recover development costs which, anecdotally, have run to 7 figures for some. (The cost of certification alone can exceed £100k).

Going forward, the UK government is keen to extend the permissible use of digital identities into other areas of the public sector (eg local government and health) and the private sector (eg financial services and travel). This may change the commercial model, perhaps reducing and eventually removing payments aligned to registration and first use to a fully usage (ie sign-in) based model.

States of Jersey model

The fundamental difference between the UK and Jersey is one of scale. Does the commercial model adopted by the UK fit with a population that represents only 1% of this? Would this present a sufficiently attractive commercial proposition both for States of Jersey and the identity providers?

The identity providers participating in this project have developed multi-tenanted platforms or platforms that can be easily replicated. Some development would be required to access data registers in Jersey; aside from that, minimal development is envisaged to meet the States of Jersey requirements and deliver services that closely align with the UK scheme.

Given this situation the commercial model would need to allow identity providers to recover their additional development costs, operating costs and obviously make a profit.

The view of those identity providers is that it would be commercially viable provided the number of participating identity providers is limited to, say, 3.

The commercial model would need to be extended to cover the identity assurance hub. Hubs have been built by a number of companies in the UK and Europe that could be readily adapted to meet the States of Jersey scheme. The project team envisage that the hub could be provided using a transaction-based usage model.

One point of significance. The UK hub has been developed by GDS using an agile approach. There has been, and continues to be, ongoing development and refinement of the web pages and user interface in line with user research and findings. Any future commercial model should allow for this within States of Jersey.

Although the starting point for the States of Jersey model may be as has been deployed in the UK, there may come a time when States of Jersey's aspirations and/or timescales start to diverge from the UK. In these circumstances there could be cost implications.

Leveraging the experience of the UK identity assurance programme

The UK identity assurance programme has been delivered with full transparency. A set of principles, guidelines, specifications, standards and procurement frameworks has been published, supported with more than 3 years' history of blog posts, articles and presentations.

A full list of supporting information can be found in Appendix A.

Through a collaborative approach, the programme has utilised consultants and private sector companies, notably encouraging start-up and SME organisations to participate. This has led to a talent pool of experienced people in the fields of

- Developing standards
- User research
- Visual design
- Technical architecture
- Agile development
- Service design and delivery
- Project management
- Privacy and security
- Certification
- Procurement
- Law

Many in this talent pool would be available to States of Jersey to assist with the development of a local scheme.

Jersey has a thriving digital technology community, encouraged and supported through initiatives developed by Digital Jersey. Jersey has the opportunity to develop into a test bed and reference site for new applications of the digital identity scheme (such as business identity), harnessing the talent pools in Jersey and the UK, perhaps with support from Digital Jersey.

Digital Jersey

Digital Jersey is an independent industry body, set up with funding from States of Jersey, to act as an industry association and accelerator for the digital economy and a digitally enabled society.

Conclusions

The project set out to test the hypothesis that the UK identity assurance scheme could be adapted economically for Jersey, with the support of the certified identity providers and potential identity assurance hub providers, to meet the States of Jersey requirements.

The findings of this project support the hypothesis for a number of reasons.

1. Jersey's history and culture is very close to the UK. It's financial, legal and administrative systems, whilst different to the UK, bear close resemblance. The principles upon which the UK scheme has been designed are equally applicable to Jersey, reflecting not only past history and culture but specifically data protection law, future European data protection regulation and adopting best practice in the use of personal data in a digital world.

2. All but two of States of Jersey's requirements can be met within the existing UK model. The two outstanding requirements are on the UK roadmap and investigation into how these will be delivered is expected to commence this year.

3. The identity providers have developed their platforms for reuse across different jurisdictions. The citizen identity verification process would need to be modified to access alternative data sources in Jersey. That aside, little or no development is currently envisaged.

4. The assumption has been made, at this stage, that an identity assurance hub will need to be procured. There are several potential hub providers in the market. GDS has published technical standards and interface protocols sufficient to enable a private sector company to replicate the functional currently provided within GOV.UK Verify.

Recommendation

Following the findings and conclusions of this project the project team sets out the following recommendation.

States of Jersey, in collaboration with other participants, undertakes an OIX Alpha project to build a prototype identity assurance hub for Jersey, based on GOV.UK Verify and the published information. This would connect one or more of the certified IdPs and a service provider 'stub'. End-to-end technical level testing would be performed.

As part of this project, clickable visual pages (no logic behind pages) would be built to represent the user journey through the hub to register with an identity provider and thereafter to assert this identity with a States of Jersey service provider. User research would be conducted to gain insight into the registration process in Jersey that would involve different data sources to that in the UK.

The findings would be presented as a white paper.

Appendix A. List of published GOV.UK Verify specifications and documents

The table below sets out the publications available relating to the Verify scheme. The table also includes documents that have not been published. In part, this is due to matters of security. Further discussions will need to take place with GDS.

Document Name	Published Yes / No	Latest Version / Date	Location
Government Digital Strategy	Yes	2013	https://www.gov.uk/government/publications/government-digital-strategy
PCAG Identity Assurance Principles	Yes	V3.1	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf
Government Approach to Assisted Digital	Yes	2013	https://www.gov.uk/government/publications/government-approach-to-assisted-digital
Digital by Default Service Standard	Yes	2015	https://www.gov.uk/service-manual/digital-by-default
Good Practice Guide 43	Yes	2012	https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services
Good Practice Guide 44	Yes	2014	https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services
Good Practice Guide 45* * links to other GPGs embedded	Yes	2014	https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
GOV.UK Verify Onboarding Guide for service providers	Yes	2016	http://alphagov.github.io/identity-assurance-documentation/
GOV.UK Verify: IPV Operations Manual (Redacted)	Yes	2014	https://www.gov.uk/government/publications/govuk-verify-ipv-operations-manual-redacted
GOV.UK Verify: IPV Operations Manual (Original)	No		To be discussed with GDS.

GOV.UK Verify Hub: various profiles to connect to the Hub	Yes		https://www.gov.uk/government/publications/identity-assurance-hub-service-saml-20-profile https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-saml-attributes https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-authentication-contexts
GOV.UK Verify Hub: technical design principles			GDS intend to go Open Source.
GOV.UK Verify Hub: source code			GDS intend to go Open Source.
GOV.UK Verify Document Checking Service			Further discussions required with GDS and HMPO.
IdP procurement round 2			http://ted.europa.eu/udl?uri=TED:NOTICE:114997-2014:TEXT:EN:HTML&src=0 https://www.gov.uk/government/publications/govuk-verify-procurement-2-contract-summary http://www.techuk.org/services/international-opportunities/item/2292-information-for-companies-interested-in-becoming-identity-providers

Appendix B. Sources of identity evidence available in Jersey

Key:
X in Box = Good Practice Guide No. 45 Example Evidence
Green Box = Jersey Example Evidence
Red Box = Jersey does not have (example UK Driving License issued by DVLA)

Identity Evidence	Citizen	Money	Living
Level 1 Identity Evidence			
Fixed line telephone account			X
Gas supply account			X
Electricity supply account			X
Police bail sheet	X		X
Level 2 Identity Evidence			
Firearm Certificate	X		
DBS Enhanced Disclosure Certificate	X		
HMG issued convention travel document	X		
HMG issued stateless person document	X		
HMG issued certificate of travel	X		
HMG issued certificate of identity	X		
Birth certificate	X		
Adoption certificate	X		
UK asylum seekers Application Registration Card (ARC)	X		
Unsecured personal loan account (excluding pay day loans)		X	X
National 60+ bus pass	X		X
An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)	X		
An education certificate gained from a well recognised higher educational institution			X
Residential property rental or purchase agreement		X	X
Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)			X
Police warrant card	X		
Freedom pass	X		X
Marriage certificate	X		X
Fire brigade ID card	X		
Non bank savings account		X	

Identity Evidence	Citizen	Money	Living
Mobile telephone contract account		X	X
Buildings insurance			X
Contents insurance			X
Vehicle insurance			X
Level 3 Identity Evidence			
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004	X		
Northern Ireland Voters Card	X		X
US passport card	X		
Retail bank/credit union/building society current account		X	
Student loan account		X	X
Bank credit account (credit card)		X	X
Non-bank credit account (including credit/store/charge cards)		X	
Bank savings account		X	
Buy to let mortgage account		X	X
Digital tachograph card	X		X
Armed forces ID card	X		
Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number)			X
Secured loan account (including hire purchase)		X	X
Mortgage account		X	X
EEA/EU full driving licences that comply with European Directive 2006/126/EC	X		X
Jersey Driving License that complies with European Directive 2006/126/EC	Jersey		Jersey
Level 4 Identity Evidence			
Biometric passports that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g. UK/EEA/EU/US/AU/NZ/CN)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	X		
UK Biometric Residence Permit (BRP)	X		
NHS staff card containing a biometric			X

The following table provides examples of activity events that could be used to demonstrate a history of activity.

UK Examples

Citizen	Money	Living
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

Jersey Examples

Key: Yellow Box Needs Confirmation

Citizen	Money	Living
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

Glossary

certified identity provider	See identity provider.
Data Protection Act 1998 (DPA)	UK legislation covering the processing, transporting and storing of personal data.
Data Protection (Jersey) Law 2005	States of Jersey legislation covering the processing, transporting and storing of personal data.
digital identity	The digital representation of an entity that's authenticated through the use of a credential.
eIDAS	The EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market.
Good Practice Guides (GPGs)	Issued by the UK's National Technology Authority, part of CESG, for the purposes of issuing advice to UK government, public sector organisations and/or related organisations.
Government Digital Service (GDS)	The organisation within the Cabinet Office with the responsibility for transforming government and delivering common platform capabilities such as identity assurance.
GOV.UK Verify	The identity assurance scheme developed by the UK government that enables citizens to prove they are who they say they are entirely online when accessing digital public services provided by central government.
hub (identity assurance hub)	The website that manages communications between users, relying parties and identity providers for the purpose of authentication to a service operating in a federated identity system. It provides a clear divide between the identity providers and service providers, avoiding complex many-to-many integrations between identity and service providers. It also ensures privacy and security during authentication transactions.
identity	The attributes of a person that make them unique from other people; who a person is. In the case of identity assurance, this is the description of being who or what an entity is, defined by a collection of attributes.
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 'trust'.
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 uniquely 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). Also called a certified company. Holder of the source of authority database to which a credential is bound and managed.
matching service adapter	The service that matches data from the identity provider to the transaction's local data store in order to tie the principal's identity to their transaction account.
matching data set (MDS)	The minimum data set of name, address, date of birth and gender sent by the identity provider to the relying party matching service for the purpose of matching.
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.
personal data	Data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
personal details	A combination of personal name and at least one of date of birth or address. Not to be confused with personal data as defined by the Data Protection Act.
principal	The person whose identity is being assured.
Privacy and Consumer Advisory Group	Established to help the UK government develop an approach to identity assurance and come up with the Identity Assurance Principles.

privacy principles	A set of principles set by the Privacy and Consumer Advisory Group that aim to protect an individual's privacy when using identity assurance.
relying party (RP)	A government service, such as HMRC or DVLA, that needs proof of a person's identity to complete a transaction. In SAML specifications, a relying party is a system entity that depends on receiving assertions from an asserting party (a SAML authority) about a subject, eg an assertion of identity from an identity provider.
service provider (SP)	Provide government services to users. Service providers are referred to as 'relying parties' to avoid confusion between those providing the government service to the user and those providing the identity service to the user.
sign in	The name for the process of using identity assurance to access digital transactions on GOV.UK.
single sign-on	A user's single authentication ticket, or token, is trusted across multiple IT systems or even organisations.
standards	The quality levels that need to be met by the identity providers and specifications that they should be compliant with.
transaction	The thing the user wants to do or get from a government service. An individual online service that a government service offers, eg renew a passport.
user journey	The steps a user takes to complete a task online.
user	The person accessing the government or local government service. Not necessarily the same as the principal, eg could be a carer filling in a form on behalf of the person that they care for.