OPEN IDENTITY EXCHANGE

ADAPTING THE GOV.UK VERIFY MODEL FOR THE STATES OF JERSEY

The findings of an Alpha Project

By Rob Laurence (Innovate Identity)

August 2017

Participants

States of Jersey

C5 alliance

<sitekit>

ID research

BARCLAYS

digidentity™
your key to a safe ID

innovate identity
experts in id

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 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.

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

Executive summary

In the preceding Discovery project, the suitability of the GOV.UK Verify model, as a basis for a digital identity scheme for the States of Jersey, was explored. The findings of that project concluded that this could be a viable approach for Jersey but further investigation was recommended to address aspects of the model where assumptions had been made and potential risks may lie.

The Crown Dependencies – Jersey, Guernsey and the Isle of Man – are each self-governing and are not part of the UK. This precludes them from participation in the current Government Digital Service (GDS) project to extend the use of GOV.UK Verify to local authorities. Jersey has been exploring the possibility of creating its own replica of GOV.UK Verify as a potential solution to the Island's digital identity requirements.

Three aspects of the model were identified for further exploration:

1. User acceptability
2. Technical capability to build an identity assurance hub
3. Data availability, sufficient to enable a significant majority of citizens and residents (90% plus) to complete identity verification online and obtain a digital identity to Level of Assurance 2 (ie a recognised level sufficient to stand a test in English Civil Law)

The approach taken to explore these aspects, together with the findings and conclusion reached, are summarised below.

User acceptability. Digital transformation is about providing users with a digital service experience so much better than existing service channels that they prefer to use it. A government-wide digital identity scheme is key to delivering these digital services, where there are inherent privacy and fraud risks to users and government departments.

Three rounds of qualitative user research were carried out in a laboratory environment, to understand users' views on digital identity, using two government services as use cases.

The findings mirrored much of the user research carried out with the GOV.UK Verify scheme.

Users' acceptance of the need for a digital identity was influenced by two factors: the first being the direct benefit to the user when compared to the effort expended; and the second the perceived security risk within the digital service. Users were positive where there was benefit and convenience but less so where there was little perceived need to strongly verify their identity and be authenticated before accessing a service.

Some users struggled to understand the journey to obtain a digital identity, questioned the role of the certified identity providers and the amount of personal information being used to prove their identity. However, users were trusting of government and, by association, extended this trust to the identity providers.

All of this should be put into context. This was the users first exposure to a digital identity of this type and, with familiarity and use, the benefits of a common approach to identity across all government services should counter most of the users' concerns.

Technical capability. The GOV.UK Verify model requires a hub to link relying parties to identity providers. The hub ensures that many of the privacy principles that were established at the outset of the programme are enabled. As part of this project, a prototype identity assurance hub was designed and built to replicate the core-functionality of the GOV.UK Verify hub.

The design was based on the Microsoft Azure platform, used extensively for developing cloud-based applications. A new Microsoft business-to-consumer identity service, not yet generally released, was also employed.

Difficulties were encountered during this project, not atypical for a project that was effectively Beta testing the new service platform.

Following an extended testing period, however, a working prototype of the hub was successfully completed.

Data availability. Online verification of a user's identity is achieved by checking data presented by the user, typically from a document in their possession, against the originating sources of that data.

As part of the project, a number of public and private-sector data sources were evaluated that could underpin the identity verification of Jersey residents. Successful verification would lead to the issuance of a digital identity that could be used with government digital services.

In the UK model, data provided by the user from government-issued documents (passports and driving licences) to the identity provider are checked back to source using the GDS-developed Document Checking Service. Jersey-born Islanders have British passports that could be checked in the same way but an equivalent service would need to be developed to check Jersey driving licences which are issued locally rather than by the DVLA.

Jersey has other data sources of high quality and population coverage that could potentially be used for user verification. The social security database and tax database could be used to verify user-supplied reference numbers and other attributes. A Jersey document checking service would need to be extended to include these. Legislation may need to be changed to permit access for this purpose.

The primary private-sector data sources used in the UK are held by the credit reference agencies (CRA). Coverage in Jersey, though, is less complete as not all financial institutions contribute. Jersey's electoral roll data is not currently shared with the CRAs. In addition, the Island has smaller, independent utility companies and mobile network operators and these also do not participate in the sharing of credit information with the CRAs. The identity providers would need to consider how they would address some of the checks required to meet an acceptable level of assurance.

At this stage, there are still some concerns as to whether the target 90% plus of citizens and residents could successfully be verified online. The experience borne out in the UK does nothing to alleviate this, although Jersey could consider a variance to the UK identity proofing and verification standards to place greater emphasis on government data sources and less on financial information.

To conclude, there remain areas of uncertainty that would need to be investigated further, notably that of identity proofing and verification. These may have an impact on cost budgeting and programme timescales and, thus, the economic viability of adopting the GOV.UK Verify approach for Jersey.

Introduction

Table of Contents

The preceding Discovery project examined whether the GOV.UK Verify scheme could be economically adapted to meet the requirements of States of Jersey. The findings of the project concluded that this could be a viable approach.

This Alpha project set out to establish with more certainty the viability of such an approach. Emphasis was put on two areas that would be different to the UK scheme: an alternative hub and the data sources available for identity proofing. User research was conducted to determine whether citizens of Jersey would exhibit the same traits as in the UK or whether there were marked differences.

Three hypotheses were tested.

Citizens of Jersey would be willing to use a digital identity, based on the GOV.UK Verify model, to access a States of Jersey service.

A Jersey-based digital technology company, with appropriate support, could build a prototype of an identity assurance hub that replicates the GOV.UK Verify hub functionality, to enable the States of Jersey relying party to request a Level of Assurance 2 (LoA2) identity from an identity provider.

Trusted sources of data are available with sufficient demographic coverage to enable most Jersey residents to obtain a digital identity online.

To test the first hypothesis, a prototype user interface was designed and built as a variant of the GOV.UK Verify hub, to gain insight into users' views and expectations of obtaining and using a digital identity to access a mocked-up government service.

To test the second hypothesis, a prototype identity assurance hub was built, equivalent to the GOV.UK Verify hub. The hub was designed and built using published GDS hub specifications and SAML profiles.

To test the third hypothesis, States of Jersey government sources of data, considered suitable for identity proofing, were investigated, together with third-party sources such as credit files.

The project involved a collaboration between States of Jersey, C5 Alliance, Sitekit, ID Research and two UK certified identity providers: Barclays and Digidentity. Innovate Identity provided project management services and subject matter expertise.

Context: Jersey's requirement for a digital identity scheme

The Island of Jersey has the ambition to become a digitally enabled society. The Island is competing against other jurisdictions across the world to attract inward investment to create a thriving digital industry as a new pillar of the economy, which is currently dominated by financial services.

The Island continues to prosper with a strong economy and balanced budget but, in common with many other places, Jersey faces economic challenges. The cost of government services continues to grow, set against a flat tax take and an aging society.

The last ten years have seen a succession of spending cuts for Jersey's government. The current savings round is one of the measures intended to prevent a possible budget deficit within the next two years.

It is evident that self-service is considerably more cost-effective than traditional customer service channels, provided those traditional channels are replaced (as opposed to duplicated). The last three years have seen an increase in transactions that islanders can carry out entirely online. The channel shift effort, though, has been hampered to some extent by the inability of Jersey government departments to identify who the customer is. It is not desirable or feasible to extend the current approach, with departments having their own identification methods, and expecting customers to maintain an ever-increasing number of usernames and passwords. There should be a single process to register for online government services, with each service identifying the user in a standard way.

Digital identity is seen as a foundational piece in Jersey's eGovernment platform and a pre-requisite to an acceleration of the introduction and uptake of new online services.

In the preceding Discovery project, a set of requirements drawn up by the States of Jersey were used as a basis for the investigation. These are included for reference in this report, in Appendix A.

User research. Would citizens be willing to use a digital identity?

Objectives and methodology

A qualitative research project was undertaken to investigate, principally, whether people in Jersey would be willing to use a digital identity (based on the GOV.UK Verify model) to access government services.

Of interest were citizens' (the users) views and expectations on

(1) creating and using a digital identity;
(2) providing and viewing personal data within a transaction;
(3) security of the service;
(4) the different brands within the service;
(5) how they would choose and identity provider;
(6) the benefits and value they saw in the service

Three rounds of user research were conducted in a purpose-built research facility in St Helier, Jersey. After each round, the findings were analysed and adjustments were made to the prototype, discussion guide and user recruitment specifications, based on what was learnt.

In Round 1, five sessions of research took place with members of the public. Users were asked to submit a tax return and subsequently amend information on their return. Users were mostly very digitally literate and had recently submitted their own tax returns.

In Round 2, six sessions were run. The primary task was changed to one that was thought to have broader relevance, notifying the Jersey government of a change of address. Submitting a tax return was the secondary task.

In Round 3, eight sessions were run with members of the public with lower levels of digital literacy, with a bias towards older and retired people. In this round, motivating factors of users were explored with users being presented with two tasks from the following list:

(1) submitting a tax return
(2) claiming a benefit
(3) checking electoral registration status
(4) renewing a passport

In all three rounds the digital identity scheme was branded as Jersey Verify and was accessed from within the States of Jersey website, GOV.JE. Real and fictitious identity provider brands were tested.

Findings

Using a digital identity with different services

Jersey Verify was tested in association with three different digital services: claiming income support, submitting a tax return and informing States of Jersey of a change of address.

Users' responses differed across these services:

- **Claiming income support:** All users were happy to be verified for this service.
- **Submitting a tax return:** Most, but not all users were happy to be verified for this service.
- **Informing States of Jersey of a change of address:** Most users reported they would abandon the task before completion.

The choice of service had a significant impact on users' motivation to complete verification and will be important in successful outcomes. Feedback from users suggested these responses were driven by a small set of common factors: effort vs. reward, security and comparisons with other channels. Understanding these may help with predicting which services are the best match for the proposed scheme.

Effort vs. reward. Most users in the early stages of rollout of a digital identity scheme will experience identity verification within the full registration journey. This introduces significant effort to the task.

All those claiming income support felt the effort was worthwhile, whilst all those changing their address felt it was not. Users claiming income support expect the real and tangible benefit of additional income from doing so, whilst there is little tangible benefit to informing States of Jersey of a change of address. Perceptions of submitting a tax return were more mixed, with some seeing value in the convenience of doing so online, but for less digitally literate users, submitting online had little or no inherent value.

> *"I'm not sure why they'd need to know your address had changed… don't want to set up a Verify account" – Alan, Round 2*

> *"I'm not happy that it takes ten minutes, ten minutes seems like a long time" – Peter, Round 2 (verification for change of address)*

Security. Users had a better experience when they were clear about why additional security was required.

For example, those claiming income support understood that identity verification would prevent someone making a fraudulent claim. Most of the users changing their address did not see the requirement for such stringent security procedures. This led them to view the process as an unnecessary imposition.

> *"The security bit was good, but it was weird how much you need to give… it was a bit extreme" – Dina, Round 1*

> *"I think it's good, but maybe a little heavy handed for this?" – Paul, Round 1*

Comparisons to other channels. Users respond more negatively when they knew they could complete their task through other channels where they would not need to verify their identity.

Many of those users who were asked to submit a tax return or to change their address, wondered why they needed to verify their identity when they knew this was not required for existing, offline means of completing the task.

For these users, the presence of Jersey Verify in the digital service was a disincentive, and some reported they would prefer to complete the task offline to avoid this.

Understanding and expectations

From the research it was evident that, whilst most people understood the basic concept of identity checking, few understood how Jersey Verify's identity verification process worked.

Throughout the testing the negative impact of poor comprehension was evident, with users interpreting content and interactions in ways that corresponded to their misapprehensions and misconceptions. Speculating on how some parts of the interactions worked, led to more negative perceptions than might otherwise have been, had users been familiar with the process at the outset.

The most common misconceptions were confined to two areas.

The first was a lack of understanding about how their identity was verified, with some users thinking it was through a single piece of information such as a Jersey social security number. Others thought it may be through past interactions with the identity provider. Few users understood that multiple identity methods are required to verify an identity; as a result, requests for the variety of personal data required were often seen as being excessive and intrusive.

The second misconception arose around the role of certified identity providers, with few users able to understand and explain why they were involved.

Many of the benefits that a digital identity offers users are being missed due to these fundamental issues of comprehension. This is especially the case when it comes to the federated nature of the scheme and the privacy and security benefits inherent in this.

In the Jersey Verify user interface, aspects of the service were explained. The research illustrated the difficulty in providing sufficient educational material to help users without introducing too much, which tends to have a negative impact with the users who do not see this as relevant to the primary task.

Trust and privacy

As users progressed through the journey, they were asked to share more and more private data to verify their identity: personal details, identity documents, banking information and answers to identity questions. Users were uncomfortable with this, feeling increasingly exposed and at risk.

Where users trusted the identity provider they had chosen, they interpreted requests for personal information more positively and were more willing to share this data and continue. Where there was less trust, these requests were viewed with suspicion and, in a few cases, users were unwilling to complete the interaction.

Trusting Jersey Verify. Most users trusted GOV.JE, although in some cases, they questioned whether they should do so. Almost all believed the government could be trusted and that there were checks and balances in place that would prevent such a public service from acting in a way that harmed their interests.

Where a few users had a trust issue with the Jersey Verify hub, it was more likely to be a suspicion that this may not be a genuine site and, therefore, not really part of GOV.JE, rather than a lack of trust in government itself.

> *"It keeps coming back to banks...Is this a real site?" - Dina, Round 1*

> *"It's not a States of Jersey phone number, this isn't a real site!" - Alan, Round 1*

Trust in identity providers. Trust in identity providers was more varied and complex. The context of the identity provider within a government service implied a certain level of trust for most. Users felt that this public context, and the clear association with government, ensured that sufficient checks and balances were in place to prevent wrongdoing. Elements of branding that tied the identity provider with the Jersey Verify hub were useful in reinforcing this.

The other element of trust was based on familiarity with the provider, past experiences and existing perceptions. Letting users choose identity providers that they already trust will improve experiences and outcomes, as users will be more willing to share personal data and more likely to interpret any uncertainty in a positive light. In addition to this, it is important that the hub continues to do as much as possible to impart the inherent trust in government to these identity providers. Current approaches to this, such as the companies being 'certified' as meeting standards set by government and the co-branding of the companies' user journeys with Jersey Verify logos, appeared to be effective.

The trust users have with their identity provider is reflected in their views and concerns around privacy and the information they are being asked to share. Broadly, the greater the trust, the less the concerns around privacy.

Some users commented that they would have abandoned the registration process with an identity provider due to privacy concerns, caused by a lack of trust. This reaction was more common amongst users who did not understand why they were being asked for this information.

At the end of most transactions, users were shown pages containing information taken from their account with the relevant government department that had originated from the identity provider. However, rather than seeing this as any kind of invasion of privacy, users saw this as a positive.

The visibility of their personal information confirmed to them that the system was working correctly and increased their confidence, and none had any concerns around the level of security in place to protect this information.

> *"It's good to see that it's all joined up" – Dina, Round 1*

Initial communications

To explore the impact of supporting communications, users were presented with a leaflet introducing Jersey Verify before research sessions.

In the first round, one half of the sample was shown this leaflet, the other was not. It was evident that users who had seen the leaflet were more trusting of the service and had better outcomes. In the second and third rounds, all users were therefore shown this leaflet.

This leaflet had a positive impact on trust. It reassured users that the service was real and not a phishing site attempting to steal their data.

> *"I need to see this come through my door, to let me know that it's a real thing" – Alan, Round 1*

The leaflet's impact on users understanding of the service was less clear. When users were questioned about what they had learnt from the leaflet it appeared that they had better understanding. When this was not done, the effect was less obvious. It was also clear that the leaflet presented further risks of misunderstanding, with a few users interpreting the identity providers listed on the leaflet as being companies where they could use a government verified identity.

These results suggest that there is a benefit to simply increasing awareness of the service before interaction, to give users confidence that this is a real service. Whilst findings discussed earlier suggest there would be benefit from increased understanding, it is not clear how easily this can be achieved in the real world: our evidence suggests that it is not enough to simply read about the service, even when the time elapsed since doing so is a matter of minutes.

Building an identity assurance hub

Part of the project tested the hypothesis that a prototype of an identity assurance hub could be built that replicated the GOV.UK Verify functionality to enable a States of Jersey Department (ie the relying party) to request a Level of Assurance 2 (LoA2) identity from an identity provider.

The Microsoft Azure Active Directory B2C identity service was selected to act as the broker between the identity provider and the relying party.

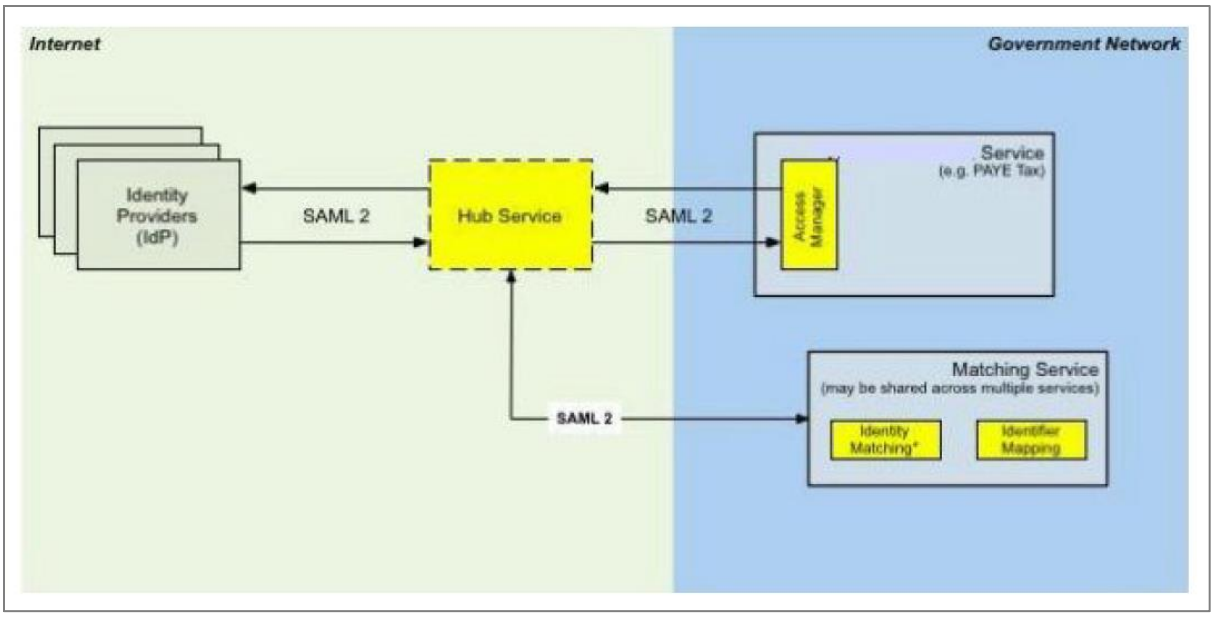
Architecture

The architecture included two simulated digital services as relying party applications:

1. A basic service to obtain a digital identity
2. An application indicative of a service to be offered by States of Jersey (eg tax submission)

OpenID Connect vs SAML 2.0

The GOV.UK Verify architecture is illustrated below.



SAML 2.0 and OpenID Connect are the two dominant standard protocols for authentication. Microsoft Azure Active Directory B2C supports both protocols. Communication with the identity providers would be via SAML 2.0 in order to not require them to make any changes to their GOV.UK Verify compatible systems to accommodate Jersey Verify. However it was decided that OpenID Connect would be used in this experiment to interface to the relying party systems in lieu of SAML 2.0 in order to test Azure's ability to mix and match protocols. OpenID Connect is an identity layer on top of OAuth 2.0 and provides a means of achieving the same goals as SAML 2.0. Subsequent testing proved that the SAML 2.0 approach would have also been successful (although not tested to the same extent with regards to encryption).

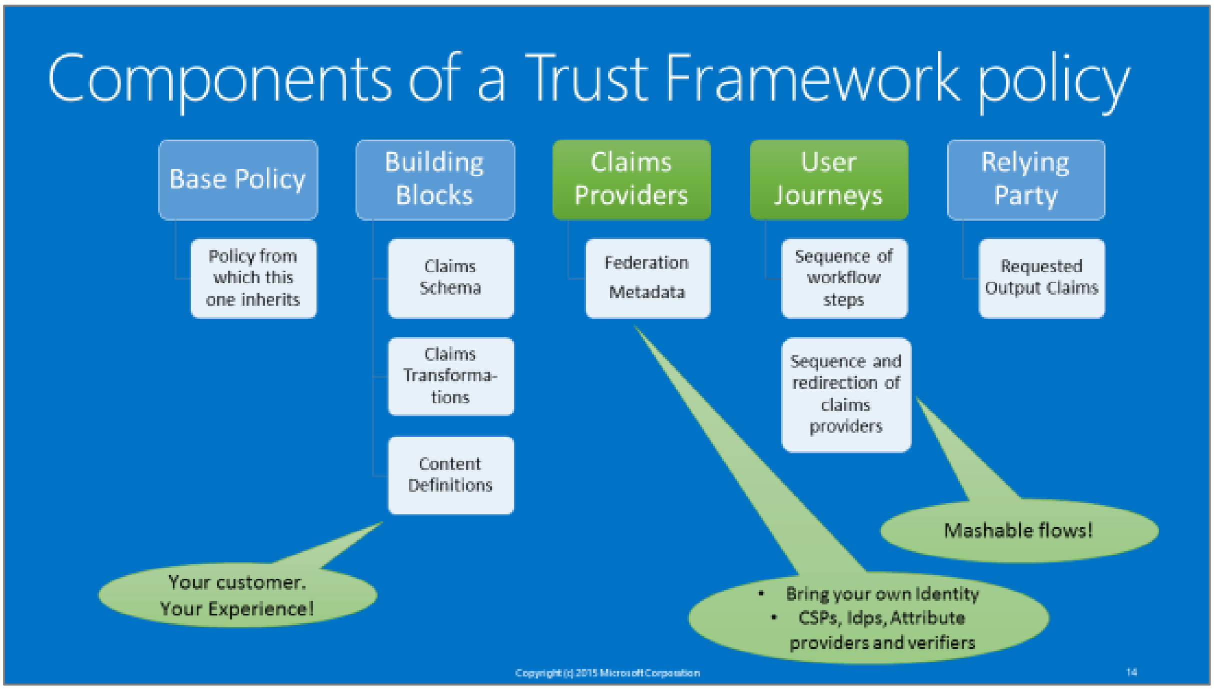
Azure Active Directory B2C

Azure AD B2C (B2C) is a secure and resilient cloud identity service the can be customised to act as the hub service for this prototype.

At the time of this project, B2C was on General Availability (production) in the US regions and in Preview (pre-production) in the EU data centres.

B2C Trust Framework

The trust framework includes the following elements.



Components of a Trust Framework policy

Base Policy
- Policy from which this one inherits

Building Blocks
- Claims Schema
- Claims Transformations
- Content Definitions

Claims Providers
- Federation Metadata

User Journeys
- Sequence of workflow steps
- Sequence and redirection of claims providers

Relying Party
- Requested Output Claims

Your customer. Your Experience!

- Bring your own Identity
- CSPs, Idps, Attribute providers and verifiers

Mashable flows!

Copyright (c) 2015 Microsoft Corporation

14

The following sections show the elements that were configured for the prototype.

Policies

B2C has an extensive policy framework which provides a degree of flexibility to configure the user experience, including user journeys and enforcement of data flows and privacy.

A single registration policy was configured that included the following list of elements:

- The set of HTML and CSS pages that are scrubbed for security compliance (e.g. cross-site scripting vulnerability) and then presented to users
  - *Basic styling was added*
- User journeys – the visual experiences through which the customer progresses in a given policy
  - *A user journey reflecting the "happy path" for each scenario*
- Identity providers
  - *A trust relationship was set up with Barclays and Digidentity test identity provider platforms*

- Relying parties who can use the policy
    - *Two relying parties were configured; one for each of the scenarios*
- Authentication requirements, including multifactor orchestration
    - *A basic authentication configuration was setup*
- Integration with claims verifiers
    - *The matching service was such a claims provider/verifier*
- Protocol Conversion (SAML, OAuth2, and OpenId Connect)
    - *SAML was used to speak to the identity providers and converted to OpenId Connect*

The following list of available elements were not implemented as part of the prototype:

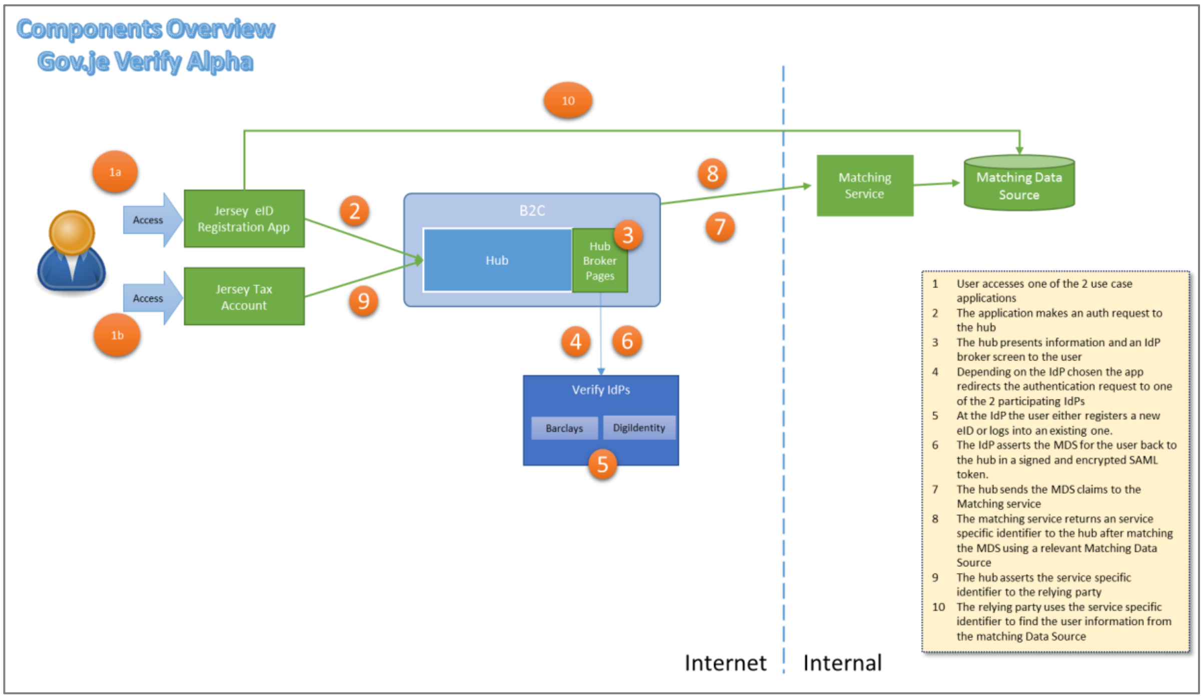
- Shared schema and mappings to participants (different systems name things differently)
- Claims transformations and data minimisation (hashing and/or transformation of attributes revealing Personally Identifiable Information into non-identifying demographic attributes)
- Blinding and encryption
- Claims storage
- Web Service calls and workflow initiation

User journey

The user journey comprised the following steps.

1. Informational page asking user to register
2. Selection page asking the user to select an identity provider
3. Claims Exchange
    - Once the identity provider (Digidentity) had been selected, and the user has verified their identity, the chosen identity provider returned the Matching Data Set (MDS) claim set back to the hub
4. User matching service
    - RESTful web service that sent the claims received from the identity provider to a matching service that matches the claims to an identity reference that is relevant for the relaying party; e.g. Tax Reference, Social Security ID, and issued a token to the relying party
5. Return of claims to the relying party

The annotated diagram on the following page illustrates this user journey.



1 User accesses one of the 2 use case applications
2 The application makes an auth request to the hub
3 The hub presents information and an IdP broker screen to the user
4 Depending on the IdP chosen the app redirects the authentication request to one of the 2 participating IdPs
5 At the IdP the user either registers a new eID or logs into an existing one.
6 The IdP asserts the MDS for the user back to the hub in a signed and encrypted SAML token.
7 The hub sends the MDS claims to the Matching service
8 The matching service returns an service specific identifier to the hub after matching the MDS using a relevant Matching Data Source
9 The hub asserts the service specific identifier to the relying party
10 The relying party uses the service specific identifier to find the user information from the matching Data Source

Scenarios

A single registration policy was configured to deal with the “happy path” scenarios as follows:

New user standalone registration. This scenario catered for the case where a user would register simply to obtain a Digital ID with an identity provider, with no actual service being fulfilled other than the creation of that ID. The relying party would be a standalone website able to detect the result of a user’s registration with an identity provider.

New user registration to complete a form. This scenario required a user to identify themselves by registering (or signing in) as part of a process to engage with a particular service (e.g. submit income tax return).

Matching service

A local matching service was developed as a simple service stub. The dummy matching service could deal with “match” and “no match” test use cases.

Identity providers

One existing identity provider was used in a test capacity to integrate with the hub: Digidentity.

Findings

B2C service is a cloud identity service architected for standards-based integration of applications (relying parties) and identity providers. The GOV.UK Verify architecture, as described earlier in this document, consists of the same parties that the B2C implementation is designed for, with the communication between parties achieved using industry-standard SAML 2.0.

The version of B2C used for the build was in a Preview (non-production) state. Effectively, this build amounted to a Beta test of this platform. Several issues were encountered that required Microsoft fixes before the tests could be completed successfully.

Trusted sources of data for identity proofing and verification

The process of identity proofing and verification (IPV) of an individual within the GOV.UK Verify scheme is set out in Good Practice Guide (GPG) 45[1].

The key principle of the IPV process is that it should enable a legitimate individual to prove their identity in a straightforward manner whilst creating effective barriers for individuals claiming to be somebody they are not.

The IPV process follows a logical sequence of steps.

1. The individual expressly declares their identity.
2. The individual provides evidence to prove their identity.
3. The evidence is verified as genuine and belonging to the individual.
4. The identity is checked to confirm it exists in the real world and has done so for a period of time.

The breadth and depth of identity evidence and checking required, differs according to the level of assurance needed about the identity of the individual.

The method used to assure an identity will vary from identity provider to identity provider. Common checks undertaken in the UK include

- Verification of data keyed or scanned from a driving licence and passport with data sources held by the issuing authorities (HMPO and DVLA)
- A check of the individual's claimed name and address against the Electoral Register
- A check of the individual's financial footprint with a credit reference agency
- Knowledge Based Verification (KBV) of the individual through an interactive question and answer session using a data source such as a credit reference file
- A check that the individual has activity over a period of time; for example, a series of payments that appear in a credit reference file
- Checks of the individual against independent deceased, movers and known fraudsters data sources.

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

Identity evidence is categorised as Citizen, Money and Living. The individual must present on request from the identity provider at least one item of evidence from each of these categories. Some items of evidence may fall into more than one category but only one category may be used during the IPV process.

Data sources available in Jersey differ in part from those in the UK. These are discussed in the next section.

Data sources

In the UK, there is at present a reliance on government-issued documents such as the driving licence and passport, presence on the electoral register and, for the money category, credit history with a Credit Reference Agency.

IPV success rates range from as little as 30% to over 70% depending on the demographic segment being verified. Consequently, identity providers are being encouraged to embrace new data sources that can address the shortfalls in these demographic areas.

New technologies - such as photo ID document scanning and comparison with a "selfie" - are also being trialled that give higher levels of assurance around documents being presented and, thus, reduce the overall number of checks that are required.

Comparing data sources in Jersey to those in the UK identifies some areas where Jersey may be stronger but also areas of apparent deficiency.

In the following two tables, the government data sources have been categorised as primary or secondary, depending on their population coverage and accuracy. The third table shows private-sector databases that may be available.

Primary Government Data Sources	
Passport	The UK government has a duty to represent Jersey at an international level. As such, Her Majesty's Passport Office (HMPO) is responsible for the provision of British passports to Jersey-born Islanders. The existing Document Checking Service (DCS) could be used by the identity providers to check Jersey passports, subject to agreement with GDS and HMPO.
Driving Licence	Each of the 12 parishes in Jersey has responsibility for issuing driving licences as compared to the central agency (DVLA) that covers England, Wales and Scotland. A project is underway to replace the existing LICAR system that is used by the parishes to record drivers' details and licences issued. This is expected to be implemented in 2018.

	Data quality is not currently considered to be of a high standard. A data cleanse exercise is planned as part of the migration exercise to the new system. Approximately 80,000 driving licences that are current have been issued, held by some 85% of the adult population. This is a higher percentage than in the UK where some 78% of the adult population hold driving licences. Discussions have taken place with GDS to ascertain if the DCS could be developed to provide access to LICAR (and/or its replacement). In principle, this would be feasible.
Social Security	The social security system, NESSIE, contains records of 120,000 residents and pensioners living abroad. Data quality is considered high due to the frequency of access, such as for the receipt of contributions, payment of benefits and pensions, and access to healthcare. NESSIE also holds details of deceased people and those who have moved away and, therefore, could be used as part of a fraud screening process by the identity providers.
Tax	iTax is a comprehensive system covering all business and personal tax matters. It contains around 60,000 active records. 70% of these records are individuals who are paying tax through their employer and using the Income Tax Instalment Scheme (ITIS). There is a high degree of confidence in the accuracy of this data. For the remaining 30%, name and tax reference is thought to be accurate but addresses may not be. It has been traditional in Jersey for the husband (regarded as the head of the household) to be responsible for the payment of tax on behalf of his wife which explains the relatively low number of active records. A large-scale programme is underway to replace the tax system in 2018.
Electoral Roll	The data on the electoral roll is believed to be of high quality. Anecdotally, about 60% of the population eligible to vote, are registered.

Other Government Data Sources	
Populus	This database is populated from NESSIE. It is used to record information pertaining to the Regulation of Undertaking and Developments (Jersey) Law and Housing (Jersey) Law. At this stage, it is not seen as of significance to the digital identity project.
Vehicle Registration	Each of the 12 parishes in Jersey has responsibility for registering vehicles. The Vehicle Registration System (VRS) holds details of 350,000 owners and 125,000 vehicles. Data is not considered to be of high quality.
TrackCare	This is used for hospital administration purposes. It contains 330,000 active records. The population coverage is unknown, although not expected to be high as it primarily covers patients' attendance at hospitals and waiting lists.
Education	The schools Central Management Information System (CMIS) contains details of pupils' performance and attendance. Further investigation is required to determine if it contains a unique identifier and inclusion of parents' data. It could potentially be used to verify the 16 plus age group where other digital footprints would be limited.

Private Sector Data Sources	
Credit Reference Agencies (CRAs)	The three UK-based CRAs, Callcredit, Equifax and Experian, appear to hold credit information on Jersey residents. The extent of coverage is not clear as the CRAs regard this information as commercially sensitive. From investigations and very limited user research, it would appear that coverage is less than mainland UK. If an individual has a credit account with a financial institution that has a presence in the UK, such as one of the high-street banks, it would seem that the institution is sending credit information to the CRAs irrespective of whether the individual is a Jersey resident. If an individual is a customer of a Jersey-based financial institution, it appears that the credit data is not being sent to the CRAs. CRAs have access to the UK Electoral Roll, and this is used for identity verification purposes. Jersey does not currently supply the Electoral Roll to the CRAs. However, in 2016 an agreement was reached between the parishes and the CRAs for the Electoral Roll to be used as a proof of name and address for credit purposes, where the individual gives permission in writing.

Considerations

There are a number of questions that need to be considered when assessing whether a data source could be used within an IPV process. These are set out in the table below.

Considerations	
Is it legal?	Passports and driving licences have been used for many years as proofs of identity, even though their primary purpose is as a proof of entitlement. The responsibility falls on the identity subject as to whether they choose to present these documents. In GOV.UK Verify, the Document Checking Service is used to solely confirm the authenticity of the documents and that they have not been reported lost or stolen, not to disclose further information. Use of other government data sources, such as NESSIE and iTAX, may be subject to current legal constraints that would need to be removed.
Is it a unique source?	Data sources used for identity proofing should be a unique source of information within an IPV process, either as the primary or secondary. So, for example, NESSIE is a primary source of social security related data, accessible by social security numbers, names and addresses. Populus is fed by NESSIE and is, therefore, not an independent data source. One or the other, but not both, could be included within the IPV process.
Is it viable?	Interfacing an IPV system with a data source is an expensive process. An Application Programming Interface (API) has to be built that can be used by the identity providers. It will only be commercially viable if the data source is relevant to a large majority of the population. Alternative approaches may need to be considered for small demographic sectors.
Is it acceptable to the user?	The use of passports and driving licences in an identity verification process is generally accepted as a "way of life". However, people struggle with providing information seen as personal and perhaps not immediately relevant to the process. A typical example of this has been the use of credit records to match a "digital identity footprint", meeting activity history over a period of time and in Knowledge Based Verification (KBV) questions. This case has been accentuated, somewhat, as many users continue to be confused as to why an IPV process for a government-issued digital identity needs access to their financial information. Similarly, how users react to providing information about their social security or tax affairs is unknown. It may be that they see this as doing "business with government" and not have concerns. However, extending this to KBV may raise some unexpected reactions.

In summary, government data sources exist and could be available to the IPV process that are at lease comparable with UK government data sources. These would enable government-issued documents and evidence to be verified against the government-held data source and for holders of such documents, this shouldn't present a problem. This identity evidence generally falls within with the Citizen and Living elements. The percentage of the population with government-issued identity evidence is high.

The situation regarding identity evidence falling within the Money element is less clear. In the UK, the identity providers have generally relied on access to credit reference data (held by the credit reference agencies). This data has also been used to underpin KBV checks. Some 80% of UK adults have a credit reference. However, this doesn't appear to be the case in Jersey where the breadth and depth of credit reference data appears to be somewhat less. This means an alternative approach to the Money category evidence needs to be considered.

One such approach might be to use tax records. Around 70% of Jersey residents pay income tax monthly through their employer. This would be indicative of earnings and deductions via payroll rather than spend as with credit reference data but still demonstrates they are financially active. The use of tax records could also be applied to KBV.

Conclusions

The project set out to establish whether the GOV.UK Verify model could be used as an economic and viable basis for the States of Jersey digital identity scheme.

Three aspects of the model were explored:

1. User acceptability
2. Technical capability to build an identity assurance hub
3. Data availability, sufficient to enable a significant majority of citizens and residents (90% plus) to complete identity verification and obtain a digital identity to LoA2.

The findings were then used to consider the likely impact on costs and, therefore, economic viability of implementing such as scheme in Jersey.

User acceptability

Generally, the users' awareness and acceptance of the need for a digital identity, as part of a States of Jersey digital service, was influenced by two factors. First, the benefit obtained in exchange for the effort expended. Second, the degree of security expected with the service and whether the effort in obtaining a digital identity was believed proportionate to the risk associated with the service transaction.

Users struggled to comprehend the digital identity journey, particularly with regard to the identity proofing and verification process and the amount and variety of personal information being requested. Users were uncomfortable with this.

The role of certified identity providers created a general misconception with few users able to understand and explain why they were involved. On a more positive note, most users trusted the government and believed checks and balances would prevent such a service from causing harm.

These findings should be considered in context. For the users, this was the first exposure to a federated digital identity model. With familiarity, the benefits this brings to the user would be expected to counter any negative impressions gained at the outset. States of Jersey may need to consider whether the requirement for multiple certified and independent identity providers is the right approach, given the size of the population, trust in government services, and potential impact on costs.

Technical capability to build

Many significant challenges were encountered during the build and test of the prototype hub service, equivalent to GOV.UK Verify.

These challenges were not atypical for a project of this general nature and may have been attributable to one or more factors.

- The GOV.UK Verify hub was designed to meet a very specific set of identity assurance principles. It is essentially a bespoke design that made use of an open-standard data format for exchanging authentication and authorisation data between the identity provider and the relying party.
- Trying to replicate this design closely with a multi-purpose, cloud-based platform with proprietary service applications was always likely to introduce constraints and compromises, resulting in "work-arounds" (for example, due to the early stage of Azure AD B2C there was a need to use CSS to manipulate HTML elements to behave as differently e.g. radio button vs checkbox).
- The B2C platform at the time of this project was in "preview" state in Europe and, as such, was effectively being tested by the development team.

Following an extended testing period, however, a working prototype of the hub was successfully completed.

Data availability for identity proofing and verification

The analysis of data sources in Jersey with those used by the identity providers in the UK, shows areas where Jersey may be stronger but also areas of apparent deficiency.

Beyond the usual government-issued document checks (passport and driving licence), the data that sits behind the social security (NESSIE) and tax (iTax) systems in the States of Jersey are considered to be of high quality. Access to these data sources would require an API to be developed, and the cost-effectiveness of this would need to be considered in terms of use generated.

Credit reference agency databases are extensively used, at present, in the UK. Anecdotally, some 80% of the UK population have a credit record with one or more of the three credit reference agencies. In Jersey, it appears that a lower percentage of the population has a credit record or that the record contains less data. (Commercial sensitivities mean that an accurate percentage cannot be obtained).

The use of credit data is unpopular with citizens in an identity proofing context and identity providers are exploring other approaches. It is the responsibility of the identity provider to ensure that their proofing and verification process meets the published guidance and can be certified.

The conclusion drawn is that sufficient data sources could be available but further detailed investigation would be required to establish exactly how these data sources could be used to satisfy the proofing process. The emphasis, though, appears to be on government data sources and less so on private-sector data.

Appendix A. Principal requirements of a digital identity scheme

The table below sets out the principal requirements established in 2016 by the States of Jersey for a digital identity scheme. (These have been superseded by a more comprehensive set of requirements in a tender issued in August 2017)

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	This has been implemented within Verify. Certified identity providers have to provide all levels of assurance.

	require higher 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.