

INTEROPERABILITY BETWEEN CENTRAL AND LOCAL GOVERNMENT IDENTITY ASSURANCE SCHEMES

Can they coexist? Is it compelling?

White Paper

IDENTITY STEERING GROUP

By Rob Laurence and Ian Litton

What is the IDSG?

The Identity Steering Group (IDSG) has been formed by OIX, the UK Government's Identity Assurance Programme (IDAP) and the Identity Providers it has contracted: Digidentity, Experian, Mydex, Post Office and Verizon. The purpose of the IDSG is to direct collaborative projects that reduce costs and mitigate risks in developing the UK's new identity services. At the time of the project, PayPal was also a member of the IDSG.

The Warwickshire project was a small scale test of Identity Providers' services in the context of the county council. It helped all parties work together to address key challenges to realising IDAP goals of convenient and secure access to digital public services.

Key Findings

- Technical interoperability is relatively straightforward to achieve
- User registration processes require further investigation and trials
- Users are adverse to using social media
 IDs on government sites
- Data matching across parties is an area of risk and needs further investigation
- Projects of this nature would benefit from a 'discovery' phase at the outset

Executive Summary

The 433 local authorities in the UK are responsible for delivering the majority of services that citizens access. These services are diverse in nature: from collecting rubbish, managing parkland and recreational facilities, to delivering benefit payments, providing education, social care and health support.

Since 2000, local authorities have been moving these services online. Today, the goal is 'digital by default': that is, all services should be provided online as the default position. Only with a reliable and effective digital identity assurance solution will this goal be fully realisable.

Over the past few years a diverse range of solutions to identity assurance have been implemented by local authorities. The purpose of this project is to examine how one such local authority's identity assurance scheme could coexist and interoperate with the UK Government's Identity Assurance (IDA) Scheme for central government services, potentially leading to a single, standards-based approach to citizen identity assurance across all public services to the citizen.

This project is the first instantiation of a service in development. It focuses principally on two areas: bridging the technical challenges faced and testing the user's understanding and acceptance of the journey. It was conceived by Warwickshire County Council, a medium-sized local authority, and involved the participation of the Government Digital Service (GDS), a team within the UK Government's Cabinet Office tasked with transforming government digital services, and three Identity Providers – Mydex, PayPal and Verizon.

1. Central and Local Government Identity Assurance Schemes

Government Digital Service (GDS), part of the UK Government's Cabinet Office, has been leading the way to develop a framework Identity Assurance (IDA) Scheme as part of the policy of "transforming government services to make them more efficient and effective for users". The intention is for this IDA Scheme to be adopted across central government service providers such as DWP and HMRC. The Cabinet Office is also keen to promote the use of the Scheme in other areas such as further education, health, transport and local government, thereby reducing development costs and risks to these bodies and providing citizens with a digital identity that can be used widely to access many public services.

Local government services in the UK are delivered by 433 local authorities. Although there is a degree of collaboration at regional and national levels, essentially each authority operates autonomously. As a consequence, each has developed its own systems to deliver services online and, where required, identity assurance solutions.

For the most part, the early wave of online services only required low levels of identity assurance, sufficient to enable basic name, address and contact details to be captured. These have typically been used to facilitate page personalisation and form filling, or to provide a minimum level of deterrent where there is a low financial risk (eg bogus fly-tipping reports). Some solutions require the citizen to provide "known facts" to access specific services and a few local authorities are looking to use third parties to provide identity assurance services.

Warwickshire County Council currently uses a proprietary solution for low level identity assurance.

Table of Contents

- Central and Local Government Identity
 Assurance Schemes
- 2. The Case for Interoperability between Schemes
- 3. Building a Business Case within a Local Authority
- 4. The Project
 - Description
 - Participants
 - Architecture
 - User Experience Testing

5. Conclusions

- Findings
- Recommendations

Postscript

¹ For example the London Borough of Enfield.

Local Authority Funding

Local authorities are facing an unprecedented crisis in funding. In the period 2010 to 2013 a combination of inflation, demographic pressures and reductions in central government grants led to local authority funding shortfalls of between 20% and 30%. In the period 2014 to 2018 local authorities are likely to face further shortfalls on the same scale. The increase in the elderly population, in particular, is putting a mounting burden on local authorities. Against this backdrop, local authorities will only invest in Identity Assurance programmes if they can be shown to improve efficiency and reduce costs. It becomes a virtuous circle if, in addition, online identity assurance also improves customer satisfaction.

Limitations of existing schemes within Local Authorities

- The typical approach taken has been to shift low risk transactions online that require a minimal level of identity assurance. As such, low cost solutions have been adopted for identity assurance and citizen registration
- Citizens often face the need to register separately for each service they access, as the underlying systems may originate from different providers with different approaches to identity assurance in the absence of an approved, standardised
- The existing situation will become significantly more complex if local authorities have to develop solutions that provide a higher level of identity assurance to support the online delivery of higher risk transactions and services

As more services are enabled online, typically with higher-levels of financial or reputational risk, higher levels of identity assurance are required. The decision for Warwickshire County Council rests between developing its own scheme, adopting a standards-based national approach, or to embrace the benefits both bring to allow the two to coexist and interoperate.

2. The Case for Interoperability between Schemes

The case for interoperability between schemes is driven by

- (1) the need for all local authorities to introduce higher levels of identity assurance as higher risk transactions are shifted online
- (2) the cost and service quality benefits of a standard approach to identity across all public services delivered at central and local levels
- (3) the protection of investments made in schemes to date
- (3) the user's ability to grasp the concept, and
- (4) ultimately, cost and affordability.

Interoperability will facilitate the use of the existing with the new, remove the need to rip and replace, and give local authorities confidence to develop local schemes in the knowledge they will be compatible with the central government offering.

Interoperability will allow citizens to "step-up" from providing an identity with a low-level of assurance to one at a higher level in line with the greater risk and security required.

As the IDA Scheme is intended to support a range of low to high levels of identity assurance one may well ask the questions: "Why the need for interoperability? Why not replace the existing scheme with the IDA Scheme?"

The answers may be assumed to include: "The existing scheme for low level services is very quick for the citizen." "The citizen is becoming increasingly familiar with the use of social media ID as a means of establishing their "social" identity." "It's a low cost solution."

This project is intended to explore whether these assumptions are valid.

3. Building a Business Case within a Local Authority

The need for an assured identity is related to risk and the importance of knowing that the person you are transacting with online really is who they say they are. High risk transactions will typically fall into 3 categories:

- Financial transactions where there is potential for fraud and financial loss
- Confidential transactions where there is potential for data protection breaches and fines from the Information Commissioner's Office²
- Regulatory situations where there is a need for a robust audit trail

The IDA Scheme will eventually support the four recognized levels of identity assurance (as set out in GPG45³). In most cases in local government, online services will require a Level of Assurance 1 or 2 (LoA1, LoA2). Currently within Warwickshire County Council, LoA1 is established through its existing scheme based on its proprietary solution. LoA2 could be delivered through the IDA Scheme. LoA2 is significant in that it is a level of assurance that would be expected to stand up in a Civil Court of Law in England and Wales, but not in a Criminal Court.

Each council will need to make its own assessment of the transactions they are moving online, the degree of risk they pose, and the level of risk

The Business Case for Moving to Online Delivery

In 2012 SOCITM, the professional association for public sector ICT management, released figures that indicated that the typical cost of a face to face transaction was £8.62; for a telephone transaction £2.83; and for an online transaction £0.15.

The business case for moving to digital delivery is clear. In turn the business case for electronic identity assurance is based on the extent to which it facilitates this channel shift.

² The ICO is empowered to issue fines up to £500,000. The highest fine so far issued is £325,000

³ The Government's Good Practice Guide to Identity Proofing and Verification of an Individual.

mitigation necessary⁴. Many council transactions can be carried out without any form of identity assurance at all. Others may be deemed to rely on simple "known facts" (Council Tax number, National Insurance number and so on). It is the remainder requiring higher levels of identity assurance that are key to the business case for LoA2 identities.

Clearly each local authority has the choice to build its own identity assurance infrastructure rather than using the IDA Scheme. This decision will be based on technical capacity and cost, but must factor in ongoing support and maintenance, resilience and availability.

However, there are additional benefits to be derived from participating in the IDA Scheme:

- The infrastructure is built to meet the <u>privacy principles</u> developed by the Identity Assurance Programme's Privacy and Consumer Advisory Group, and will ensure a greater degree of privacy than is likely through a locally developed solution⁵
- There are citizen service benefits that stem from a citizen having one properly assured digital identity that can be used to access both central and local government services.
- The GDS infrastructure will be significantly enhanced in future with the addition of Attribute Exchange alongside Identity Assurance. Attribute Exchange (the citizen being able to prove online that they are, for example, registered disabled or in receipt of specific benefits) will drive much more sophisticated online transactions by establishing trust frameworks between Service Providers and Attribute Providers that will effectively eliminate paper proofs from complex transactions.

Business Case Factors

In summary, the business case will be based on:

- The number of transactions that require an identity at LoA2
- An assessment of the percentage of those transactions that can be driven online
- The savings that can be delivered as a result
- The cost of providing an IDA solution, whether that is through the IDA Scheme* or a local development procurement
- Other non-financial improvements to customer service that can be delivered through identity assurance

^{*} At the time of this project the commercial model for the IDA Scheme was under review.

⁴ As set out in points 3 and 4 of the Government's <u>Digital by Default Service Standards</u>

⁵ Particularly in relation to principles 3 (Multiplicity) and 7 (Governance and Certification)

Warwickshire, England

Participants

Warwickshire County Council

(Service Provider)

GDS (Hub)

Mydex (Identity Provider)

PayPal (Identity Provider)

Verizon (Identity Provider)

GDS Business Information Unit

(UX Workshop Facilitation)

OIX (Project Co-ordination)

4. The Project

Description

Warwickshire County Council (WCC) is a two tier local authority where services are split between county and borough/district levels. It serves a population of 547,000. Some 75,000 citizens have login profiles with WCC for low trust transactions. Examples of these transactions include alerts for school closures and public consultations. During the next 12 months Lotus Notes, the system that sits behind these logins, is being replaced. As part of this, the plan is to migrate the 75,000 existing users to a standards-based log-in (Open ID, SAML, oAuth), compatible with social media log-ins.

WCC is also involved in higher assurance level transactions (e.g. social care, community health provision) and intends to deliver these online. The wider business case is to ensure the replacement identity assurance scheme that will be adopted for low trust transactions is capable of coexisting with the IDA Scheme for high levels of trust.

Architecture

The project utilised two Service Providers. The first was a mocked-up central government agency, the Driver and Vehicle Licensing Agency (DVLA) and the second a mocked-up WCC site. A DVLA service had been developed to allow drivers to check their driving licence details and motoring convictions. This required a user identity at LoA2 to access. The WCC site provided two services. The first, to report a pothole, required a user identity at LoA1 (eg a social media ID); the second, to request a disabled parking bay close to the user's place of residence, required a user identity LoA2.

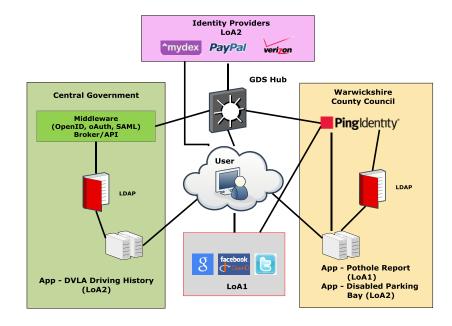
The Service Providers and the three IdPs were connected to the Hub developed by GDS. The Hub provided user pages that explained the IDA Scheme and details of "approved" IdPs. It also provided a routing service to the chosen IdP for registration and log-in at LoA2.

The schema of the project architecture is set out here.

Utility Software

PING Identity: A Federation Server, used to provide the SAML interface between the WCC applications and the Hub, WCC applications and social media IdPs, and WCC applications and their internal LDAP server.

Matching Service Adapter: The MSA has been developed by GDS for the use of all government Service Providers. The MSA passes the Matching Data Set (as sent by the IdP) to the Service Provider, and provides a simplified JSON interface to allow the Service Provider to communicate the results of their matching process back to the Hub.



User Experience Testing

A key objective of the project was to understand the level of users' understanding and acceptance of the forms of and approach to identity assurance.

Specifically, the principle areas of investigations were

- Users' acceptance of social media IDs as a means of obtaining personal information for transactions requiring low levels of trust
- Users' understanding of the IDA Scheme concept and the potential privacy and security benefits it offers, together with a single log-in credential to access central and local government services
- Users' understanding of the need to "step-up" from a social media ID to the IDA Scheme to provide a higher level of trust, privacy and security.

The findings are set out in the next section.

SAML: SAML stands for "Security Assertion Markup Language" and is an XML-based standard for communicating identity information between organisations. The primary function of SAML is to provide Internet Single Sign-On (SSO) for organisations looking to securely connect to Internet applications that exist both inside and outside the safety of an organisation's firewall.

Source: Ping Identity

Federation Server: The project identified several necessary components of a federation server:

- the ability to handle multiple certificates;
- capability to interact with multiple IDPs;
- translation of attribute names to provide a single interface to internal applications from different IDPs;
- creation of user accounts:
- ability to integrate with internal directories

Data Matching: Data matching is a key source of risk. A false "positive" match could lead to incorrect attribution of identity and the incorrect disclosure of personal and sensitive information. Data matching is often based on complex algorithms and confidence levels in order to cope with quite legitimate variations in data records.

5. Conclusions

Findings

The key findings and areas of learning gained from the project are set out below. These have been categorised within three areas: technical, business process and user experience.

Technical

The project brought together the technical components of the IDA Scheme for the first time. WCC and the three IdPs developed connections to the GDS-built Hub service according to the SAML 2.0 specification. The inclusion of PING Identity within the WCC development enabled third-party collaboration in the project. Interestingly, and perhaps unsurprisingly, it brought together two interpretations of the SAML specification. The Matching Service Adapter was implemented for the first time as part of the project.

One consequence has been the evolution of the SAML specification implemented by GDS to align with current industry practice. It has also prompted GDS to write a technical guidance paper aimed at the different parties who will be connecting with the Hub service.

The project highlighted the issue of accurate data matching, specifically the matching of names and addresses originating from different sources. In the project there were 3 sources: the user's name and address as keyed, the user's social media ID as returned by Google and the user's LoA2 identity as returned by the IdP in the Matching Service Adapter. In a live situation a fourth source is also possible: the existence of a record in the Service Provider's local directory. The issue is further compounded by the process rules implemented by the IDA Scheme.

A further assessment of the impact of this is set out in the Business Process section below.

Key Objective Achieved

One of the key objectives of the project was to look at the question of interoperability of the two schemes. From the development of a technical infrastructure perspective, WCC has successfully built a platform to deliver this around an LDAP server and a federation server.

The complexity of data matching may present a significant barrier to implementation by Service Providers. This would seem to be an area where "develop once and reuse many times" would make real sense, and warrants further analysis.

The full details of the technical experiences are set out in an associated document, entitled IDSG Project Technical Findings. Warwickshire County Council - using a Federated UK Government ID in Trusted Local Authority Transactions.

Business Process

The project has highlighted shortcomings in the user journey arising from the technical implementation of the IDA Scheme.

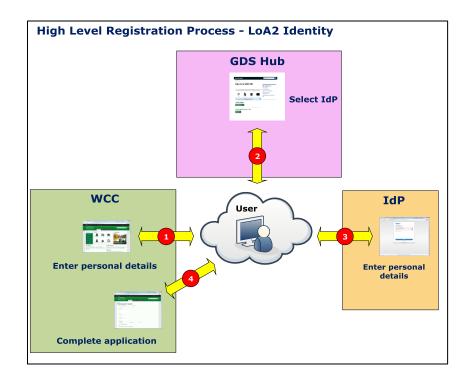
At the outset it was recognised that functional gaps existed. In part, these were a product of trying to bring two schemes together and, in part, these were subject to future, planned Scheme developments (Attribute Exchange, for example). The experience gained during the project enabled the significance of these to be better understood.

LoA Step-up. One of the aims of the project was to test the step-up from a social media ID (LoA1) to an identity assured by an IdP (LoA2). As there was no realistic way of linking the two automatically, the project highlighted the importance of designing a process that would take the user through a clear, understandable journey. The project tested this journey and from a technical perspective it worked well. From a user perspective, much was learnt from the user experience testing (see later) to suggest that considerably more thought needs to be applied in this area if it is to become a viable proposition going forward.

Creating User Accounts. The relationship between a citizen and a local authority is usually ongoing and covers a number of services. Many of the higher level trust transactions require online forms to be completed with name, address and contact information, and potentially

other proofs of service eligibility. It would be desirable for the common identification data items to be obtained from the IdP in the first instance and from a local "user account" thereafter to pre-populate these online forms. However, at the time of this project, the functionality required to deliver user data directly within the IDA Scheme had yet to be developed. The IdP was able to return the data to the Hub where a Matching Data Set was created comprising name and address. The Hub returned this to the Service Provider to match with an *existing* local directory entry. The Matching Data Set could not be used to create a local directory entry for the first time service user.

The consequence is that the user is faced with a convoluted process when using the IDA Scheme for the first time. It involves entering name, address and contact details on the Service Provider's site to create a new directory entry and user account, navigating the way through Hub pages to an IdP, to be asked to enter the same information again to register and create a new user account with the IdP.



User Tasks

Scenario 1: The user was asked to report a pothole using the online service provided by WCC. This required the user to use a social media ID as a means of identification. For the purposes of the test, a fictitious Google Mail account was created, although other social media (Facebook and Twitter) were introduced into the discussion.

Scenario 2: The user was asked to access the DVLA application to check their driving licence details. The application required a LoA2 identity. The user was taken to the Hub and presented with a choice of IdPs to use. The user was guided through the selection process and to the IdP registration pages before being passed back to the Hub and DVLA with a successful LoA2 identity.

Scenario 3: The user was asked to apply for a disabled parking bay outside their residence. This service provided by WCC required the user to register with an IdP to obtain LoA2 identification. The user was directed to the Hub and asked to select the IdP they had previously registered with, then complete the log-in process before being handed back to the Hub and WCC application.

The ideal scenario would be for the user to give permission to the Service Provider to automatically populate its local directory with the registered information held by the IdP. This would avoid the need for the user to re-key the same details. Future planned development of the Scheme will support this.

User Experience

User experience testing was performed in a laboratory environment and involved 5 users on a one-to-one basis with an experienced research facilitator provided by GDS. Each user had extensive experience of online services including internet banking, government services and social media such as Facebook and Twitter.

The users were presented with the mocked up local and central government services. PayPal and Verizon were the selected IdPs. Each user participated in registration and log-in processes using social media IDs (Google) and one of the two IdPs.

The feedback from the small sample of users was generally fairly consistent.

Use of a Social Media ID. Most users would be very reluctant to use their social media accounts with a government site, the prevailing view being that their social life is distinctly separate to doing "business" with government. The issue of privacy and the feeling that government would be able to "see my social life", or that government transactions would appear in their social media profiles, was of concern. That said, some users saw the benefit in forms being pre-filled with details held within their social media account.

The Hub. The Hub service was being used as the only source of information to the user on the IDA Scheme. Users were unfamiliar with the model of using a third party for identity assurance and expected to see a standard registration form. As a result, users often struggled as they sought to understand how this method of signing in to government

IdP Experience

The user experience testing provided the IdPs with a good opportunity to refine their registration and logon processes.

Areas addressed included:

- how to indicate password strength requirements in an easy to understand way
- adoption of more user-friendly terminology on forms
- refinement of error messages
- design of screen layouts
- improved process flows

services worked. The Hub service provided the user with a link to a video clip that described the scheme and its purpose. The users' initial reactions were to avoid this and continue with the selection process. Once they were shown the video the general comment was "it makes sense".

Selection of an IdP. The initial choice of IdP was left to the user and it was clear that the choice was based on "brand" awareness alone. Users were not clear why private sector companies were being used to carry out identity assurance on behalf of government. There was an expectation that government itself would be more capable of identifying them rather than a third party with whom they had had no previous relationship.

The Registration Process. The users were split across the two IdPs involved in the user experience testing. Views were mixed on the process itself, with some favouring very simple registration processes due to their speed, balanced with other views recognising the "feeling" of a safer and more secure service in a more complex and time-consuming process. Some aspects of the registration processes proved annoying to the users but could easily be addressed by the IdPs.

The IDA Scheme. Upon reflection users felt comfortable with what the Scheme is trying to achieve and the approach taken.

Recommendations

In summary, the project demonstrated that the technical components of the IDA Scheme that were addressed, ie the IdPs, Service Providers and Hub, could successfully be integrated by the five parties to a common standard (SAML 2.0).

However, fundamental concerns over the enforced business process and resulting user experience were identified. As a consequence, the

User Quotes

"Well you go on the WCC website and register with them. These companies will prove who you are and they are safe. It appears to be 99.9% safe, and it's pretty straight forward" Paul, talking about the Scheme

"This feels safer with the verification and more details needed. Yes, normally I would probably use something someone else has used or researched or if it's better known" Elizabeth, talking about the choice of IdP

"Actually sounds good, new way of accessing services online. Could be good" Elizabeth, talking about the Scheme

"You have to sign up twice essentially haven't you? I mean if you have to go out to sign up for an Identity Provider I may as well have done it through the website in the first place - right?"

Dan, talking about entering personal details at two points in the process

following recommendations are put forward for further consideration by the appropriate bodies.

Warwickshire County Council. The case for the technical implementation and coexistence of a low-cost identity scheme based on social media with the higher-assured, potentially higher cost IDA Scheme has been proven. However, the user experience, based on using a social media ID is generally negative, and when asserting two types of identity, appears confusing. In part, this may be due to the design of the user interface. Future design iteration would establish the impact of this. Further investigation, therefore, is required to determine if this is indeed an appropriate and realistic approach. The true business costs of each will also need to be established.

The Hub. The user journey through the Hub to select an IdP for first-time registration was not straightforward and involved navigation through a number of pages. The mix of user education and establishing awareness, together with the process to select an IdP, will need considerably more examination and testing to understand better how to approach this in a "live" environment.

The IdP Registration Process. The IdPs in the project have developed registration processes in different ways. Further work will be required to streamline these. There is also a need to establish a common "vocabulary" across the three entities in the registration process (the Service Provider, Hub and IdP) that users engage with.

The IDA Scheme. The limitations imposed by the Scheme rules on the return and use of names, addresses and other related data elements to the Service Provider, cause a significant business process issue. Attribute Exchange is designed to overcome this. This technical capability needs to be proven and built into the Hub in order to provide a more seamless and compelling user experience. It will be key to adoption by Service Providers.









GDS





Further information about the project can be found at www.oix.mvine.com.

Postscript

The objectives of the project have been delivered. It has proven to be a rich source of learning for the direct participants and, hopefully, for the members and observers of the OIX/IDAP initiative.

From a technology perspective, the project has been relatively straight forward and all parties have been able to deliver technically proven components that have enabled end-to-end processing to be completed for "happy" journeys.

In terms of business processes and usability, much has been learnt. It would be fair to say that there is much more work to be done going forward to streamline processes and facilitate a better user experience.

The IdPs have gained a clearer understanding of the nuances surrounding user verification in the UK and effective user messaging and communications.

GDS has gained useful insight into design of the Hub pages and how to communicate the purpose of the IDA Scheme with first-time users.

For Warwickshire County Council, this is a stepping stone towards a robust identity assurance process. Further work is planned to embrace Attribute Provision in its various guises to support more efficient methods of user registration and underpin complex service transactions.

Much has also been learnt about how a project of this type should be structured and executed. At the outset, there is general agreement that there should be a period of "discovery" that results in a clear definition of the purpose of the project and intended outcomes backed up with a very good understanding across all parties involved as to how the project will be executed.