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

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.

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

Table of Contents

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[1].

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

---

[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 scheme
- 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 Office[2]
- 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 GPG45[3]). 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 necessary[4]. 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 privacy principles 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 solution[5]
- 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 Digital by Default Service Standards

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

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.

Participants

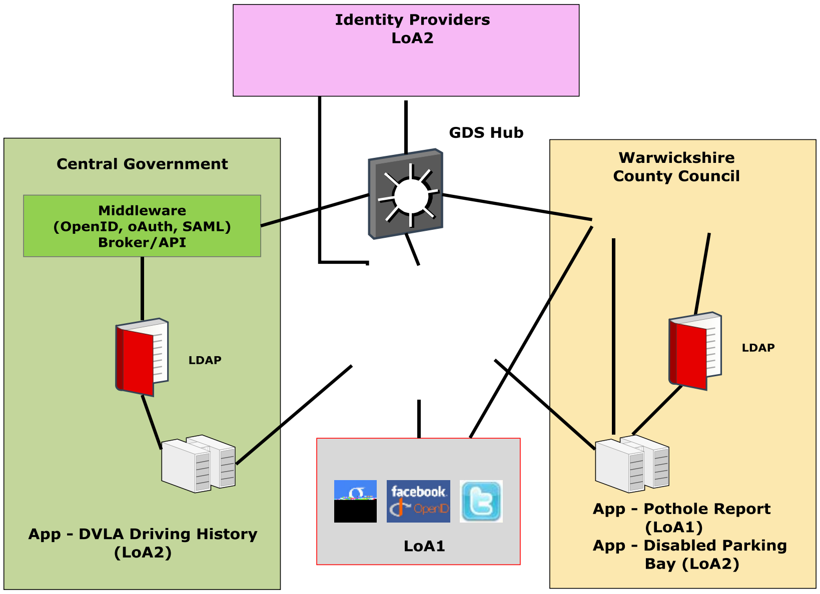
Warwickshire County Council	(Service Provider)
GDS	(Hub)
Mydex	(Identity Provider)
PayPal	(Identity Provider)
Verizon	(Identity Provider)
GDS Business Information Unit	(UX Workshop Facilitation)
OIX	(Project Co-ordination)

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.

The schema of the project architecture is set out here.



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.