OPEN IDENTITY EXCHANGE

CAN ATTRIBUTE PROVISION, TOGETHER WITH IDENTITY ASSURANCE, TRANSFORM LOCAL GOVERNMENT SERVICES?

By Ian Litton and Rob Laurence

August 2014

Contributors

OIX UK is the UK arm of a global organisation and works closely with the Cabinet Office on the Identity Assurance Programme. Its goal is to enable the expansion of online identity services and adoption of new online identity products. It works as a broker between industries designing, testing and developing pilot projects to test real use cases.

Executive Summary

Identity assurance is frequently portrayed as the key to unlock the potential of the Internet.

In the UK the Cabinet Office's Identity Assurance Programme team and Open Identity Exchange (OIX) are leading the way to unlock this potential as part of the UK Government's digital by default strategy for central government services. Local government, too, recognises that digital by default is the way forward. Many local authorities are, themselves, starting to adopt this approach for the delivery of their services.

Identity assurance is key if we are to enable the digital by default strategy. It provides a means of common access to services across central and local government. But the bigger opportunity arises when we can access and use data. We call this "attribute provision". This is when it becomes possible to transform services.

"Attribute Provision" can be differentiated from traditional data sharing initiatives. It is a user-controlled activity under which the user sees the data and can vouch for its accuracy and pertinence to the transaction. This avoids inaccurate or out-dated information being used without the user's knowledge or consent. Attribute provision grants permission for a point-in-time disclosure of information from a trusted source to a service provider, for a specific purpose. It does not grant perpetual access to the data source.

Transformation of service means delivering a better customer experience. Processing and waiting times are slashed, queries and progress chasing reduced. For local authorities it means better customer engagement, greater efficiencies and significant cost savings.

In this white paper we report on the learnings of the Warwickshire County Council Discovery Project that considered how attribute provision can be enabled through the identity assurance infrastructure. This is a practical way to achieve what has long been talked about, a digital infrastructure that enables data to flow freely, cheaply, securely and with the permission of the service user, to underpin the delivery of services online.

Local authorities are responsible for the delivery of some 1,500 services, ranging from the publication of information to meeting complex social needs. An initial analysis of these suggest that approximately 200 require confirmation of the user's identity and somewhere between 50 and 100 require additional personal information. Identity assurance and attribute provision pave the way for these to be delivered as a digital service. Rough estimates would suggest cost reductions in local government alone running to hundreds of millions of pounds.

During the course of this project we built prototypes of the Blue Badge and Residential Parking Bay services and tested these with citizens. The prototypes demonstrated real-time processing of user applications. Online access to assured identities and user attributes enabled these applications to be processed within minutes. The ease and speed of these journeys was a source of surprise and delight for users..

One of the 'unknowns' at the outset of the project was the user reaction to their data being obtained from other organisations such as government departments. Considerable time was taken during the design of the prototypes

looking at the issue of information privacy and consent, and how this should be addressed. This is covered in some detail later in this white paper. It's fair to say that all the users who tested the prototype were comfortable with the approach taken and raised no concerns. They raised no concerns about government departments holding their data securely or fairly, although this trust did not extend fully to the private sector.

The project enabled us to develop a set of business requirements and consider approaches to the technical design. It is planned to take these forward into an Alpha project to build and test a technical solution.

The overwhelming conclusion that can be drawn from the project is that identity assurance and attribute provision are essential if many of the more complex local authority services are to be provided online.

Following the approach taken by the Cabinet Office with the Identity Assurance Programme, a similar open and collaborative approach to attribute provision would speed up the delivery of such an infrastructure, protect investment and accelerate the transformation of service delivery.

The potential scale of the savings is significant. At a DCLG co-design event in July 2014* it was estimated that £100m could be saved each year by local authorities if they had access to Driver and Vehicle Licensing Agency (DVLA) data to deliver a range of services online, such as concessionary bus travel, taxi licences and parking permits.

If the 324 local planning authorities in England had access to Land Registry property data a saving of £97m could be made each year through fraud reduction and efficiency gains.

Figures are not available for the savings that could accrue from Local Authority access to data in two of the particularly data rich government departments – The Department for Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC) – but these would significantly exceed the benefits identified above from sharing DVLA and Land Registry data with local authorities. The transformative potential of access to DWP and HMRC data has already been proven by the Connect Digitally Free School Meals project.

*see Reference[i]

Table of Contents

1. Background and context

In 2013, Warwickshire County Council (WCC) and the Cabinet Office's Identity Assurance Programme team collaborated on an OIX Alpha project to demonstrate that local authority and central government identity assurance schemes could interoperate. Interoperability was achieved and the results were written up in an OIX White Paper, "*Interoperability between central and local government identity assurance schemes*"[ii].

Although technically successful, the Alpha project recommended further areas of investigation to improve the user experience and to build on the value delivered by identity assurance.

These areas were as follows:

- To introduce attribute enrichment to avoid users having to enter the same personal details on multiple screens. Attribute enrichment would allow a service provider (SP) to set up a local account for the user, based on the Matching Data Set (MDS) provided by the identity provider (IdP), and to use this to pre-populate online forms
- To address the complexity of data matching, which is a key risk area for service providers matching an assured identity to back-office records[iii]
- To streamline the identity assurance registration process[iv]
- To investigate attribute exchange as a way of users proving eligibility for services in online transactions. This has the potential to be transformative both for users and service providers.

This white paper discusses the case for attribute exchange in local and central government and is based on the findings of the recent Attribute Exchange Discovery project that involved WCC, Government Digital Service (GDS) and two IdPs, Mydex and Verizon. The discovery project picked up on several of the key findings from the first WCC Alpha project, and had the following aims:

- to evaluate the requirements for attribute enrichment;
- to evaluate the requirements for attribute exchange;
- to recommend a high level architecture capable of delivering attribute exchange;
- to carry out user experience testing to establish user acceptance of attribute enrichment and attribute exchange
- to investigate the potential role of personal data stores in delivering attribute exchange

Since the publication of the Interoperability White Paper, OIX has also published a white paper on The Economics of Identity*. This identifies the potential for UK companies to reduce their identity assurance costs over the next decade from £1.65bn to £150m based on "make once, use many times" electronic processes. But more significantly it claims that "models of identity assurance enable significant markets for verified attributes that have long-term potential for service innovation and economic growth" (p.3). The potential market for verified attributes is valued at £16.5bn.

*see Reference[v]

2. The case for attribute provision within Government

a) Supporting "Digital by Default"

Central and local Government have long recognised that moving services online – making them digital by default – has the potential to significantly reduce cost and improve service delivery[vi]. Moving more complex eligibility-based services fully online is only possible, however, with the introduction of electronic attribute exchange.

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 cost of face to face services to deliver the more complex transactions that would benefit from attribute provision is considerably higher.

In the Discovery project we considered the application process for Blue Badges (a.k.a. disabled parking badges) as a typical example, to demonstrate the benefits that might be gained. Although there is a national Blue Badge application system, hosted on GOV.UK[vii], it relies on paper proof of identity and paper proof of eligibility to complete the application. Some councils quote up to 10 weeks to process a Blue Badge application when the application is submitted on paper. With identity assurance and attribute exchange in place the whole process could be automated for the 40% of applicants whose eligibility is based on the primary criteria (i.e. they are in receipt of one or more of the six qualifying benefits). Rather than taking 10 weeks, the application could be processed in 10 minutes. This would simplify the application process for over 350,000 people each year, and dramatically reduce the time and cost for local authorities to process their applications. The applicants are, by definition, more vulnerable people for whom the burden of delivering paper proof of identity and eligibility can be somewhat onerous.

Basing online service delivery on a robust online identity assurance process and electronic attribute exchange also reduces the likelihood of fraudulent applications. Blue Badges are valuable items, as evidenced by the rise in prosecutions for fraudulent use.

b) Cost reduction

The Blue Badge example shows that attribute exchange could dramatically speed up and improve customer service. There are significant cost savings to be made as well. Using processing times measured in WCC and the number of Blue Badge applications annually, we estimate that the adoption of attribute exchange for this one service would lead to national savings of between £1.5m and £2m per annum[viii]. But how widely can this be applied and how large are the potential savings?

There are around 200 local government services that require assured online identities to ensure safe and secure online delivery. Of these, at least 50 could be streamlined by attribute exchange, removing the need for paper proof of eligibility.

In addition to the potential savings to service providers from introducing attribute exchange. There is, of course, a potential saving to attribute providers as well. The provision of immediate, automated responses to attribute requests reduces the need for applicants to contact government departments and agencies (attribute providers in this context) for written proofs of eligibility.

c) Fraud prevention

Attribute exchange, based on assured online identities, also has the potential to prevent fraud by establishing eligibility for services *before* they are delivered to applicants. This is far more efficient than detecting fraud after the event, using inter-organisational data sharing, and ensures that services are only delivered to citizens with genuine needs.

3. Investigating the use of attributes

The aims of the Discovery project are set out in the section 'Background and context'. In order to meet these aims we performed the following tasks:

- researched the area of data privacy and consent, in the context of data sharing, to understand how online processes should be designed to comply with data protection legislation and best practice guidance
- set out a series of high-level business requirements for the provision and use of attributes
- designed and developed online prototypes of two existing local government services, incorporating identity assurance, attribute enrichment and attribute exchange
- tested the prototype with a number of test users in one-to-one sessions
- considered different approaches to a high-level technical solution.

The findings are set out in the following sub-sections.

a) Statutory obligations and guiding principles relating to data sharing

Attribute enrichment and attribute exchange are forms of data sharing and, in the context of delivering public sector services to an individual, will involve personal data. The Data Protection Act 1998 (DPA) is the legislation that governs obtaining, sharing and using this data.

The Information Commissioner's Office (ICO) has produced a Data Sharing Code of Practice[ix] and a Subject Access Code of Practice[x]. 'Data sharing' is defined as the disclosure of data from one or more organisations to a third party organisation or organisations.

The Privacy and Consumer Advisory Group (PCAG) has produced a set of Identity and Privacy Principles[xi] to support the Identity Assurance Service, designed around the needs of the individual and not the needs of the state body or commercial organisations. These are based in part on the fundamental principles of data protection that are set out in the DPA.

Data sharing is core to attribute exchange. Within the scope of this project we only concerned ourselves with the sharing of data between the IdP, a central government department, and a local authority in support of digital by default. However, we recognise the scope may go much further in the future and embrace the private and third sectors.

When considering how the prototype should be designed we discussed in depth the topics of fairness and transparency, privacy policies and consent. Much of the guidance on privacy policies is particularly relevant in data sharing contexts because of the need to ensure that people know which organisations are sharing their data and what it is being used for. Consent from the individual may or may not be required depending on the nature of the data sharing agreement. In a policy, the wording tends to be generic and timeless.

Attribute enrichment uses the Matching Data Set (MDS) provided by the IdP. The MDS is used by the Service Provider to set up a user account (name, address, date of birth and gender). Attribute enrichment is deemed to be part of the Identity Assurance Service. In the prototype used in the Discovery project, the Identity Assurance Principles of user control and transparency were designed into the process.

Attribute exchange is based around the sharing of data necessary to deliver a service in a digital world. The Identity and Privacy Principles are directed towards the Identity Assurance Programme so, although relevant, Attribute Exchange is notionally out of their scope. The prototype aimed to follow the ICO Data Sharing Code of Practise where appropriate, in the first instance.

For example, here is an extract from the DWP personal Information Charter:

"We may share information with certain other organisations such as:

- *other government departments*
- *local authorities*
- *private-sector bodies, such as banks and organisations that may lend you money"*

This considers data sharing from the perspective of the organisation collecting and providing information to a third party. In the context of the Discovery project and attribute enrichment and exchange we needed to consider data sharing from the perspective of the third party, in this case WCC and the service user.

In attribute exchange we know specifically what information is required to be shared and who holds it. Taking into consideration the principles of user control and transparency, we looked at how the principles of subject access (within the Data Sharing Code of Practice) could be applied, and examples of where it had been used by individuals in conjunction with third parties (eg financial services, solicitors).

The Subject Access Request (SAR) approach has some elegant and positive features that would benefit attribute enrichment and exchange:

- it can be used in a very specific way with a clear purpose at a point in time
- it's driven by the individual (user centric) and, thus, completely transparent
- it's legal, has a comprehensive set of guidelines and is an accepted and proven model
- it may take precedence over other areas of legislation that restrict data sharing in the public sector

Using the SAR approach enables the user to drive the service transaction in an interactive way, "pulling" through the attributes required by the transaction at the point they were required, cutting out applications forms, processing times and delays.

The conclusion is that the main principles of the SAR approach worked very well in the case of the prototype developed, both from the service provider and service user perspectives.

However, we also recognised it may not satisfy all types of attribute exchange and there may be legal matters to resolve.

There are two areas that should be considered for future investigation. Firstly, the user has a right to see the data returned during the exchange process, and may wish to retain this. Secondly, there may be beneficial reasons for the user to receive and keep an electronic 'copy' or token of the resulting entitlement from the application, in this case a Blue Badge.

The features and benefits of personal data stores perhaps lend themselves to this type of solution in the longer term.

b) Warwickshire County Council's requirements

At the outset of the prototype design, WCC set out a series of business requirements for attribute provision.

The key requirement in terms of attribute enrichment was to provide WCC with the data needed to create a local directory entry for users and pre-fill online forms with the user's key personal details.

The key requirement in terms of attribute exchange was for online, real-time exchange of attributes in order to determine a user's eligibility for a service.

It was also crucial that the prototype adhered to good practice around privacy, confidentiality and consent and that the user felt comfortable with this. Consequently the following requirements were put in place:

- all requests for attributes should be transparent to the customer, both in terms of the attributes being requested and the identity of the attribute provider;
- the customer should give explicit permission for attributes to be shared;
- at the same time, the user journey should be as simple as possible and not interrupted with frequent requests for permission; all required consents should be grouped together at or near the outset of a transaction;
- user transactions involving attribute provision should be based on assured identities provided by an IdP to be certain that it is in fact the user authorising the exchange of data;
- attributes from more than one attribute provider could be requested in the same user session

It is our belief that these requirements are likely to be generic to most service providers engaging in attribute provision.

The requirements set out by WCC are limited and specific to the delivery of services digitally within the context of the Discovery and subsequent Alpha projects.

The project team believes that to deliver attribute provision on an industry-wide scale there will need to be a collaboration of organisations to create an ecosystem. This ecosystem will need to operate under a governance mechanism in accordance with an agreed industry set of scheme rules. These rules will cover areas such as the legal and commercial framework; money flow, billing and settlement; technical standards and interoperability; accreditation and auditing; and, most importantly, privacy, protection and reparation for the individual.

c) Determining customer needs and expectations through user research

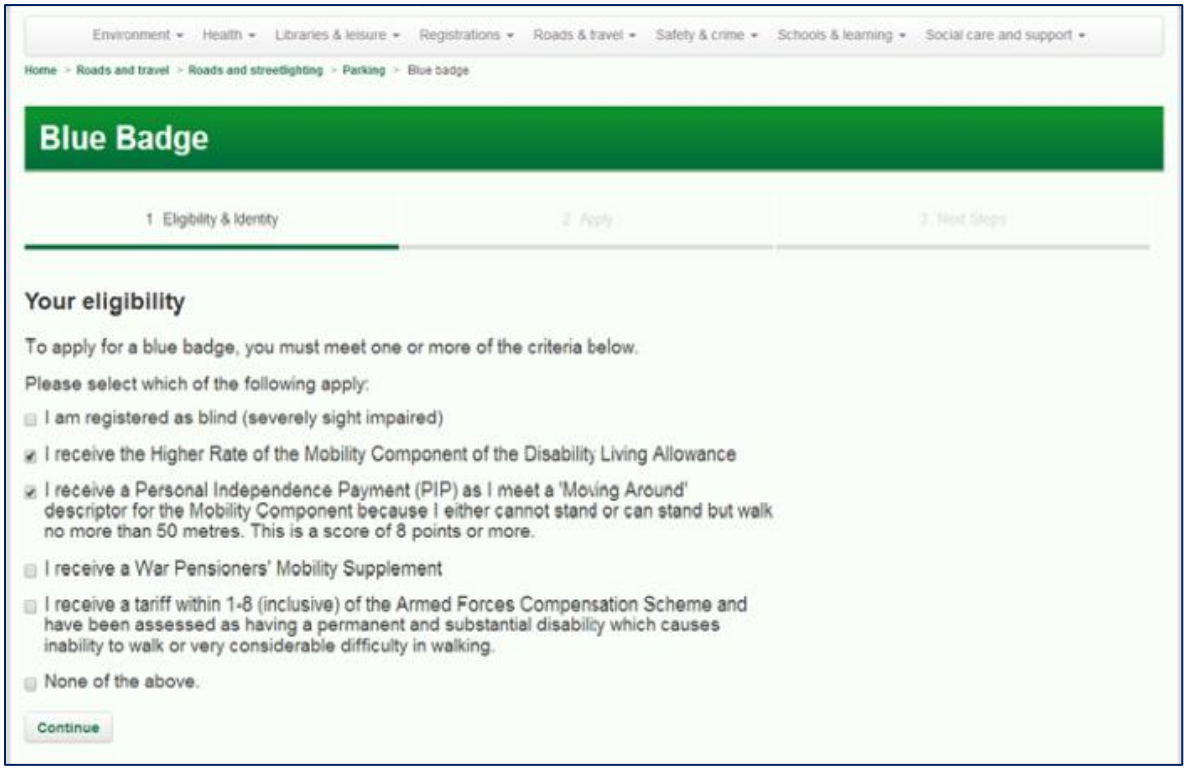
Savings and service improvements are only achieved if users take up online services, and that depends on those services meeting their needs and expectations. As part of the Discovery Project we ran two rounds of user experience testing to test user reaction to, and readiness for, electronic attribute exchange. At the same time we took the opportunity to test attribute enrichment in order to address one of the outstanding usability issues from our first Alpha project.

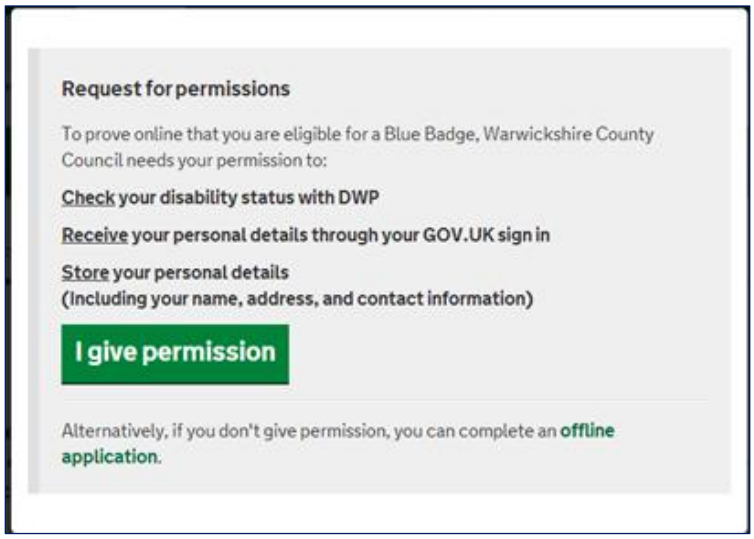
A prototype was built for the Blue Badge and Disabled Parking Bay applications that took account of the business requirements and legal considerations considered above. A GOV.UK sign-in was required to access the services. The respondent profile was predominantly older people: 11 of the 13 respondents were aged 60+ (oldest: age 86).

Attribute exchange as presented in these prototypes was unproblematic for respondents. It did not trigger concerns about privacy, intrusiveness, 'big brother' or any of the common themes encountered when exploring other aspects of identity assurance with users.

Instead, attribute exchange was seen as sensible, reasonable and necessary in order to complete the transactions in hand. Several respondents thought it would be strange if communications and exchange between WCC and other parties did not take place in the context of an online Blue Badge application.

It was recognised by some respondents that attribute exchange would be a good way to reduce fraud. More than one felt that if one had nothing to hide then there would be no difficulty in giving WCC permission to request attributes from (in this example) the Department for Work and Pensions (DWP). Or as one respondent put it: "I'm quite happy if it stops the naughty people!"

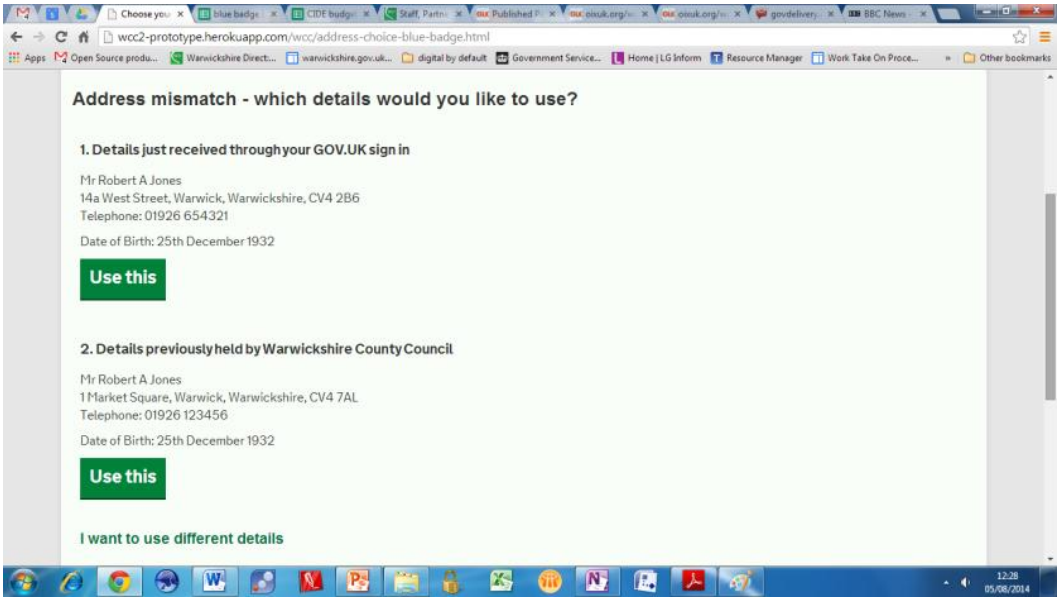




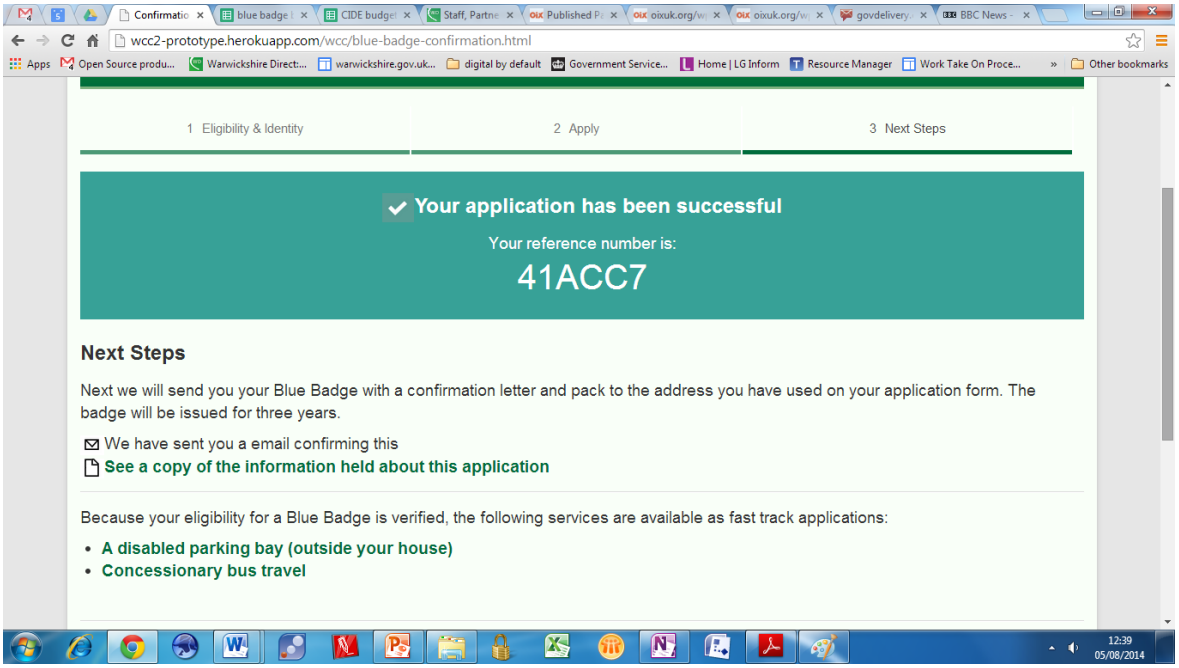
The prototype made the grounds for eligibility and the request for permissions very explicit. Permission was asked to check the applicant's disability status with the DWP and to receive their personal details from the GOV.UK sign-in and store them locally. The applicant had the option not to give permission, and to proceed with a paper application. All respondents were comfortable giving permission.

The permissions message was reinforced later in the transaction by giving the applicant a visual indication of the data being exchanged and for what purpose. This screen also gave a graphic indication of the rapidity with which the application could progress using these digital approaches.

Respondents had no concerns about WCC receiving and storing their personal details "through your GOV.UK sign-in", which confirmed the assumptions from the first WCC Alpha project about the benefits of attribute enrichment. In fact, when shown an address mis-match in the details held by the IdP and those held by WCC, some respondents thought there should be automatic updates; so if WCC had more up-to-date personal details these should be automatically updated at the IdP and vice versa. Automatic updates are not part of the current design brief. If this were considered it would need to be transparent and with the permission of users.



The ease and speed were further emphasised when the user was taken through a 'fast track' application for a disabled parking bay outside their house. Identity and eligibility had already been established through the Blue Badge application, further reducing the time taken to carry out the disabled parking bay transaction.



Perhaps the most significant finding, though, was the user reaction to the ease and speed of the online application process which attribute exchange allowed. This was often surprising to respondents and was strongly liked. Indeed, there was an element of 'wow factor' in terms of

respondent reaction, which is rarely encountered with online government transactions. Attribute exchange was accepted as a perfectly reasonable way to achieve this surprising ease of outcome. One of the respondents who, in the past, had given up on the "pages and pages" of the paper Blue Badge application form was especially impressed – "I think it's brilliant!"

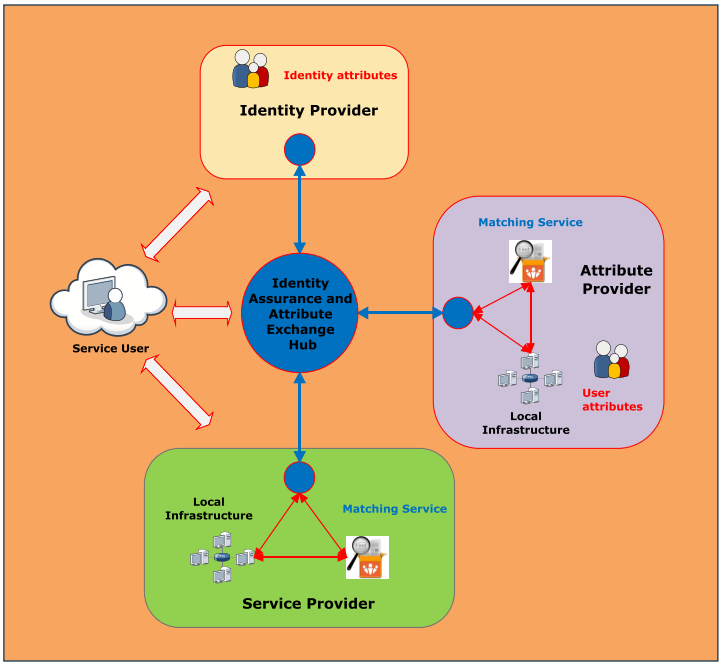
The entirely positive user reactions to attribute exchange were, perhaps, even more remarkable given the age profile of the respondents.

d) Architecture and technical design

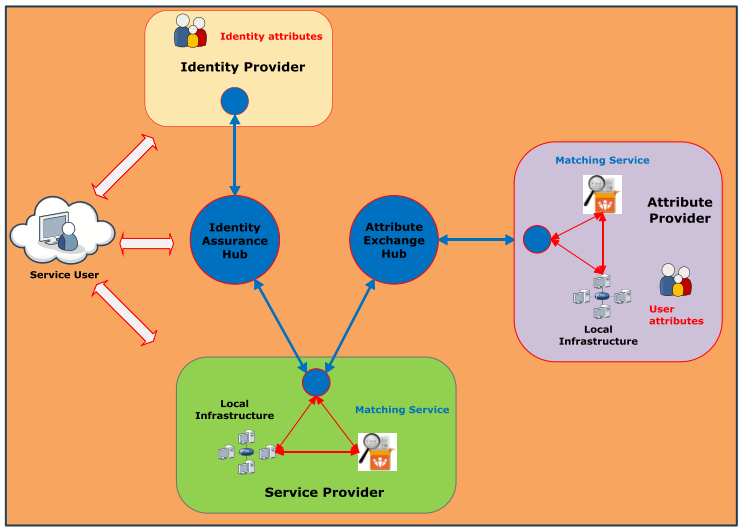
The Discovery project has delivered some high level technical design principles for attribute exchange, capable of meeting the business requirements (see Appendix). These need to be refined in the Alpha phase of the project, in which a working attribute exchange prototype will be built.

A key design principle yet to be decided is the link between identity assurance and attribute exchange. Three different models have been considered to date.

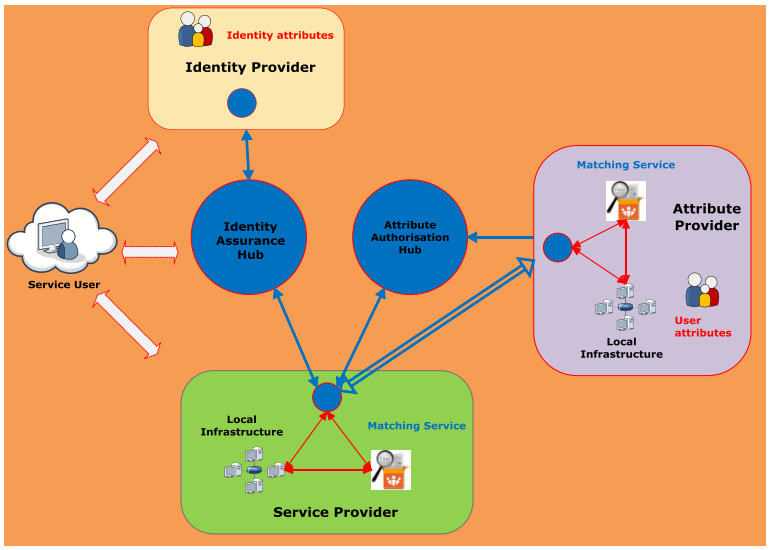
The first of these combines the identity assurance and attribute enrichment function with attribute exchange into one, all-encompassing hub, as shown in the diagram here.



The second approach splits the function of attribute exchange from identity assurance and attribute enrichment. One key benefit of this approach is that the Attribute Exchange Hub doesn't have to replicate the identity assurance functionality.



The third option is a variant of the second. Here the concept of an Attribute Authorisation Hub is introduced that sets up a secure connection between the service provider and attribute provider. The attribute can then be sent directly between the two and not via the hub (as shown by the double-lined arrow). This has the advantage that the hub doesn't handle the attribute.



The Discovery project team has identified a set of basic principles for the design of the technical solution that are set out in the Appendix – technical design principles.

4. Conclusions

The Discovery project tested the concept of identity assurance enabled attribute enrichment and exchange in the context of a specific local government service. The findings indicated strong user support.

Test users commented that they "love it", "think it's brilliant" and wonder: "Why on earth wouldn't you do it this way". They feel secure, in control and like the idea "it keeps the naughty boys out".

For local authorities it is a way of achieving channel shift and digital by default, and at the same time realising tremendous cost savings.

For attribute providers it is a way of driving out costs and improving performance. Many attribute providers are also service providers and could benefit in both ways.

Across central and local government and beyond, attribute exchange along with identity assurance have the potential to be a game changer.

In the Economics of Identity White Paper that considered the size and potential of the UK market for identity assurance, Ctrl-Shift wrote:

"Identity assurance is just a small sub-set of a much bigger market for verified attributes. Identity assurance, along with its associated market for verified attributes, is a multiplier of wealth creation."

The findings of this project offer support to this assertion.

All of this helps grow the evidence supporting a new market opportunity for the information technology sector. A market of hub providers and identity providers; of services to attribute providers and local authorities, to central government, the public sector at large and beyond.

In today's world of information technology projects, this is not about a large hub infrastructure commissioned by government, connecting public sector attribute providers and service providers. This is about an ecosystem of private-sector hubs and identity providers meeting the needs of public and private sector service providers and attribute providers, with choice and competition driving innovation and progress. This is an opportunity open equally to new and agile businesses as well as the established giants of the information technology industry.

Industry, Government and other stakeholders need to work together to make the market, to turn this opportunity into reality.

For Warwickshire County Council, this has been an important journey of discovery as they look to develop a digital by default service strategy. It sets the foundations for an Alpha project in the coming months, working with industry participants and GDS to address some of the design principles and technical challenges in implementing the business requirements and use cases.

5. Appendix – technical design principles

Set out below are a series of design principles that the project team believes should be incorporated within the technical solution.

- Attribute exchange works seamlessly with IDA
- A service provider may use more than one authorisation (for attribute exchange) hub
- Information on transactions undertaken should be captured, in a way that is compatible with privacy principles, so that audit, billing, and reconciliation can be undertaken
- A standard naming convention should be agreed for attributes within the alpha project. As part of this project the team review available standards and apply learnings from IDA to date in order to come up with recommendations around achieving interoperability across schemes
- It should be possible to determine the quality of data being provided. Quality in terms of accuracy, source, timeliness and relationship to the identity involved in the transaction
- Where obfuscation of the source of data or proof of claim is required it must still be possible to trust the data as valid.
- The core SAML-based identity hub remains unchanged, and will continue to embody the Identity and Privacy Principles established by the Privacy and Consumer Advisory Group
- The user is central to the attribute exchange process and gives explicit permission for attributes to be shared
- The user should be able to 'opt out' of the attribute exchange process and revert to traditional methods of accessing a service
- The user should have the ability to capture a record of their consent and the context
- Attribute exchange will be built using open standards. OpenIDConnect has been selected for attribute exchange for its flexibility and ease of implementation, and there will be a single agreed profile for the Alpha
- Authorisation hubs will facilitate the retrieval of authority tokens that can be used for direct transactions between service providers and attribute providers
- It should be straightforward for service providers and attribute providers to move between different authorisation hub providers without the need to re-engineer their services
- It should be possible for multiplicity of supply and use
    - attribute providers to use more than one authorisation hub at the same time
    - service providers to use more than one authorisation hub provider at the same time
- Attribute providers may source their attributes from any source of verified data
- Each component will be described as logically distinct elements but it is possible for an organisation to provide one or more of the elements

- A market for authorisation hubs and attribute providers should be supported and encouraged
- There will need to be an on-boarding process for attribute providers and service providers before they can provide or consume the attribute services

6. Glossary

assured identity	An identity that has been verified to the required level of assurance by an identity provider
attributes	The personal information provided by a principal that's to be authenticated by the identity provider Data linked or about an Identity that support and/or indicate such things as entitlement, authority, right to work
attribute enrichment	The onward use of attributes delivered as part of the identity assurance process. The service provider will either use them in a user journey they are accessing or use it to populate a user record within the service provider records.
attribute exchange	The request for, authorisation and sending of an attribute, or attributes, originating from a relying party to an attribute provider.
attribute provider	An entity that can assert attribute values in line with the policies set by the scheme it is being used within. It responds to a request from a trusted relying party.
attribute provision	A generic term to cover both attribute enrichment and attribute exchange.
data matching	The process of finding a local identifier through matching that is useful to the relying party when completing a transaction. For example, confirming a National Insurance number so the principal can amend their tax records
Data Protection Act 1998 (DPA)	A piece of UK legislation covering the processing, transporting and storing of personal data
digital identity	The digital representation of an entity that's authenticated through the use of a credential
Government Digital Service (GDS)	The organisation within the Cabinet Office with the responsibility for transforming government and Identity Assurance
hub (identity assurance hub)	The website that manages communications between users, relying parties and identity providers for the purpose of authentication to a service operating in a federated identity system. It provides a clear divide between the identity providers and service providers, avoiding complex many-many integration between identity and service providers. It also ensures privacy and security during authentication transactions.
identity	The attributes of a person that make them unique from other people; who a person is In the case of identity assurance, this is the description of being who or what an entity is, defined by a collection of attributes

identity assurance	The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity . Proving you are who you say you are to a certain level of 'trust'
identity provider (IDP)	Private sector organisations paid by the government to verify a user is who they say they are and assert verified data that uniquely identifies them to the relying party The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority). Also called a certified company Holder of the source of authority database to which a credential is bound and managed
matching service (MS)	The service that matches data from the identity provider to the transaction's local data store in order to tie the principal's identity to their transaction account
matching data set (MDS)	The minimum data set of name, address, date of birth and gender sent by the identity provider to the relying party matching service for the purpose of matching
Open Identity Exchange	A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon)
personal data	Data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
personal details	A combination of personal name and at least 1 of date of birth or address. Not to be confused with personal data as defined by the Data Protection Act
principal	The person whose identity is being assured
Privacy and Consumer Advisory Group	Established to help the government develop an approach to identity assurance and come up with the Identity Assurance Principles
privacy principles	A set of principles set by the Privacy and Consumer Advisory Group that aim to protect an individual's privacy when using identity assurance
relying party (RP)	A government service, such as HMRC or DVLA, that needs proof of a person's identity to complete a transaction. In SAML specifications, a relying party is a system entity that depends on receiving assertions from an asserting party (a SAML authority) about a subject, eg an assertion of identity from an identity provider

SAML (Security Assertion Markup Language)	An Extensible Markup Language (XML) open standard for the exchange of authentication and authorisation data between parties such as identity providers and relying parties., The SAML standards are governed by OASIS. A SAML Profile derived from core SAML standards is used for the purposes of signing in to government services under identity assurance. Created by OASIS
service provider (SP)	Provide government services to users. Service providers are referred to as 'relying parties' to avoid confusion between those providing the government service to the user and those providing the identity service to the user
sign in	The name for the process of using identity assurance to access digital transactions on GOV.UK
single sign-on	A user's single authentication ticket, or token, is trusted across multiple IT systems or even organisations
standards	The quality levels that need to be met by the identity providers and specifications that they should be compliant with
subject access request (SAR)	Defined in the Data Protection Act 98, it gives individuals the right of access to personal information that is held about them by organisations
transaction	The thing the user wants to do or get from a government service. An individual online service that a government service offers, eg renew a passport
user journey	The steps a user takes to complete a task within the hub
user	The person accessing the government or local government service. Not necessarily the same as the principal, eg could be a carer filling in a form on behalf of the person that they care for

7. References

[i] http://www.ukauthority.com/LocalDigital/tabid/226/Default.aspx?id=4865
[ii] The white paper is available on the OIX website and at the following link http://oixuk.org/wp-content/uploads/2014/05/Warwickshire-County-Council-Project-2.pdf
[iii] Data matching is the subject of a separate OIX white paper currently being written.
[iv] This is beinginvestigated by the IDA Programme team within GDS.
[v] The Economics of Identity white paper is available on the OIX UK website and at the following link http://oixuk.org/wp-content/uploads/2014/05/Economics-of-Identity-White-Paper.pdf
[vi] See the Government Digital Strategy https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy
[vii] https://www.gov.uk/apply-blue-badge
[viii] Figures based on 2012 national statistics
[ix] See https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
[x] See https://ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
[xi] See https://gds.blog.gov.uk/2012/04/24/identityand-privacy-principles/