Cabinet Office

OPEN IDENTITY EXCHANGE

THE INDUSTRY WORKING GROUP ON ATTRIBUTE EXCHANGE

Progress Report – September 2015

By Rob Laurence

Introduction

Table of Contents

A key principle of the Government Digital Strategy is that a suite of common capabilities will be designed and built as a collaboration between the public and private sectors to deliver key solutions.

GOV.UK Verify is one such capability that will eventually provide citizens with a single digital credential to access several hundred government services.

GOV.UK Verify was developed in collaboration with privacy groups, the Information Commissioner's Office, credit reference agencies, telecoms and digital security companies, and other organisations. A series of principles relating to privacy and the rights of citizens were drawn up. The Open Identity Exchange provided a structure to explore and test concepts, and share experiences and learning with complete openness.

This approach is seen within government as being a catalyst to create an identity assurance ecosystem that will extend to local government, health and eventually the private sector. Central to this is gaining the trust of the citizen, that their identity is safe and that they can transact online safely and securely.

Similarly, attribute exchange has the potential to be another common capability. Being able to exchange information in real time, safely and securely, between organisations has enormous benefits and will underpin the transformation of many public and private sector services.

Definition of attribute exchange

The online, real-time exchange of data specific to the transaction in hand, with the user present and with their full knowledge and permission.

Attribute exchange builds on the approach taken to create GOV.UK Verify with the objective of creating an ecosystem of certified attribute exchange hubs, attribute providers and relying parties. It's very early days. To date, a couple of OIX Alpha projects have been concluded that have tested different approaches to a technical solution.

An Industry Working Group on Attribute Exchange (the IWG) has been established by OIX. Initially its brief was to shadow, review and potentially influence the work of the OIX Warwickshire County Council led Alpha project on attribute exchange, taking the Blue Badge application process as the use case. This was subsequently extended to include the NHS England Citizen Identity Alpha project. Both of these reviews are included in this report.

In this report we also consider what should be done next to advance the cause of attribute exchange ecosystems in both the public and private sectors. Later, questions are posed and an approach outlined to move forward.

The aims of the IWG are:

- To promote the cause of attribute exchange and the benefits it delivers to citizens, service providers and attribute providers, those benefits extending to private sector organisations and their customers in due course
- To shadow, review and comment on OIX Attribute Exchange Discovery and Alpha projects, exchanging ideas, strengthening skills and sharing examples of good practice
- To identify, address and discuss issues of common concern and avoid unnecessary duplication of efforts
- To facilitate access to support and resources that are available in member organisations and elsewhere
- To make recommendations to OIX on issues of common concern and areas pertinent to the creation of an attribute exchange ecosystem or ecosystems; these may relate (but not be constrained) to matters of legal, regulatory, compliance, commercial, functional and technical subject matter.

Participation in the IWG is open to organisations with related fields of expertise and those who would ultimately engage in and benefit from attribute exchange ecosystems. Currently the following companies and public sector organisations are represented.

Axway	Experian	Morpho
PIB-d	Telesign	Tricerion
GDS	NHS England	Warwickshire County Council

The IWG is chaired by Innovate Identity.

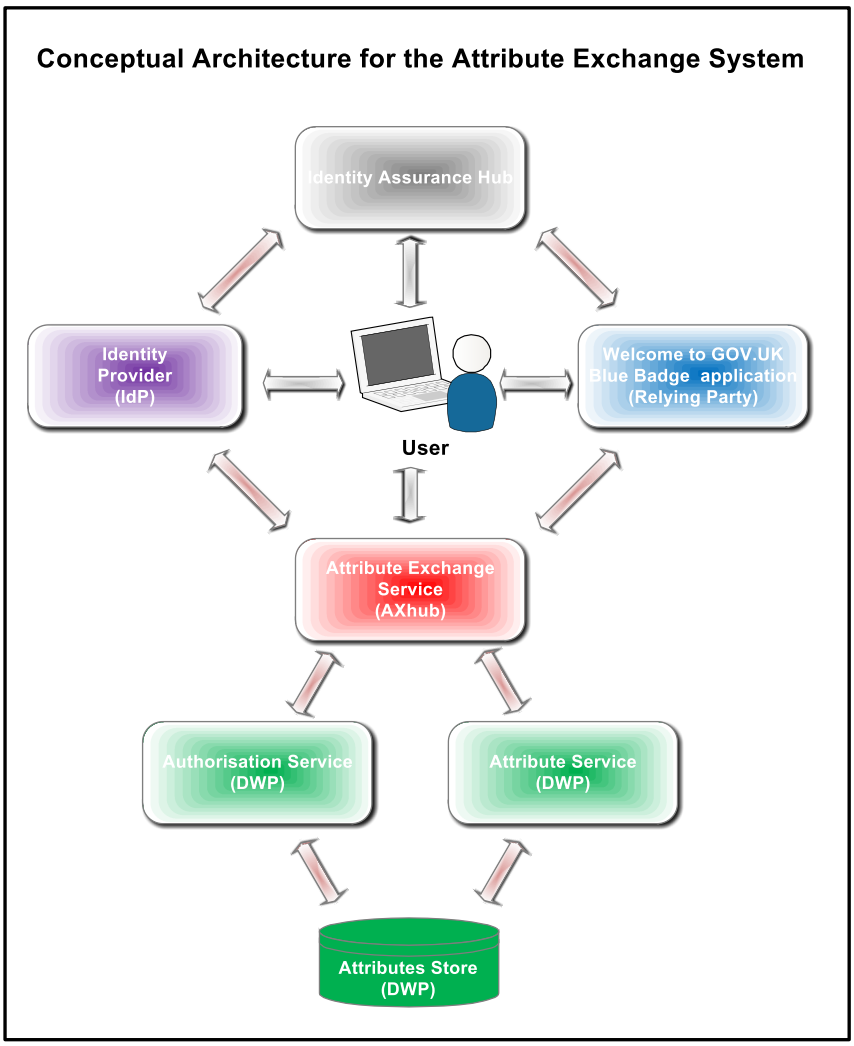
Review of attribute exchange projects

The brief for the IWG was to review and comment on two OIX attribute exchange projects. The first of these was the Warwickshire County Council led project to look at how attribute exchange could transform local government services; the second was an NHS England project looking at a user's access to their medical records. Both of these explored different approaches to a technical architecture and solution.

Project 1: Towards an architecture for a digital Blue Badge service

This was an OIX Alpha project that set out to demonstrate how a typical local government service – applying for a disabled parking badge (a Blue Badge) - could be radically transformed from a process taking several weeks to one taking a few minutes. This was achieved through the design and build of an attribute exchange service.

The resulting technical solution was based on the design architecture as shown here.



The IWG's review of the project was based on

- the underlying business requirements
- technical design principles
- options considered and approach taken to building a technical solution

The IWG fully understood the business requirements and no concerns were raised regarding the technical design principles. It noted that the project team had elected to build a technical solution based on separate identity and attribute exchange hubs and found the reasoning for this sound.

The review raised a number of points for the project team to consider. Most of these related to the clarity of the design and were of a minor nature. No material issues were raised.

The findings of this project have been published as a white paper[1] and technical paper[2].

Future Requirements

Following the review of this project the IWG set out a number of additional requirements that it believes should be considered as part of future attribute exchange discovery and alpha projects, or potentially the work of the IWG.

Ref	Requirement	Description
IWG/001	Transparency	The user should be able to access the attribute exchange hub to find out what attribute value(s) relating to their interaction with the relying party has been sent by the attribute provider to the relying party.
IWG/002	Integrity	Intelligence in the attribute exchange hub to determine what is a permissible request from a relying party for an attribute.
IWG/003	Blindness	Expect use cases where the relying party and attribute provider may wish to remain anonymous from each other but not the user. The attribute exchange hub is responsible for maintaining anonymity (aka blindness).
IWG/004	Dynamic attribute exchange	Decision on where the attribute is sought from is made by the attribute exchange hub.
IWG/005	Enduring permission	There is a need for periodic checks on eligibility for a service to be performed (eg Blue Badge). The user's consent will be obtained. The attribute exchange hub needs to support this for repeat checks where the user is not present.
IWG/006	Categorising relying parties	There is a need for the attribute exchange hub to know the category of the relying party (eg that

[1] See http://oixuk.org/wp-content/uploads/2015/08/WCC-2-alpha-white-paper-final-draft.pdf

[2] See http://oixuk.org/wp-content/uploads/2015/08/WCC-2-alpha-technical-paper-final-draft.pdf

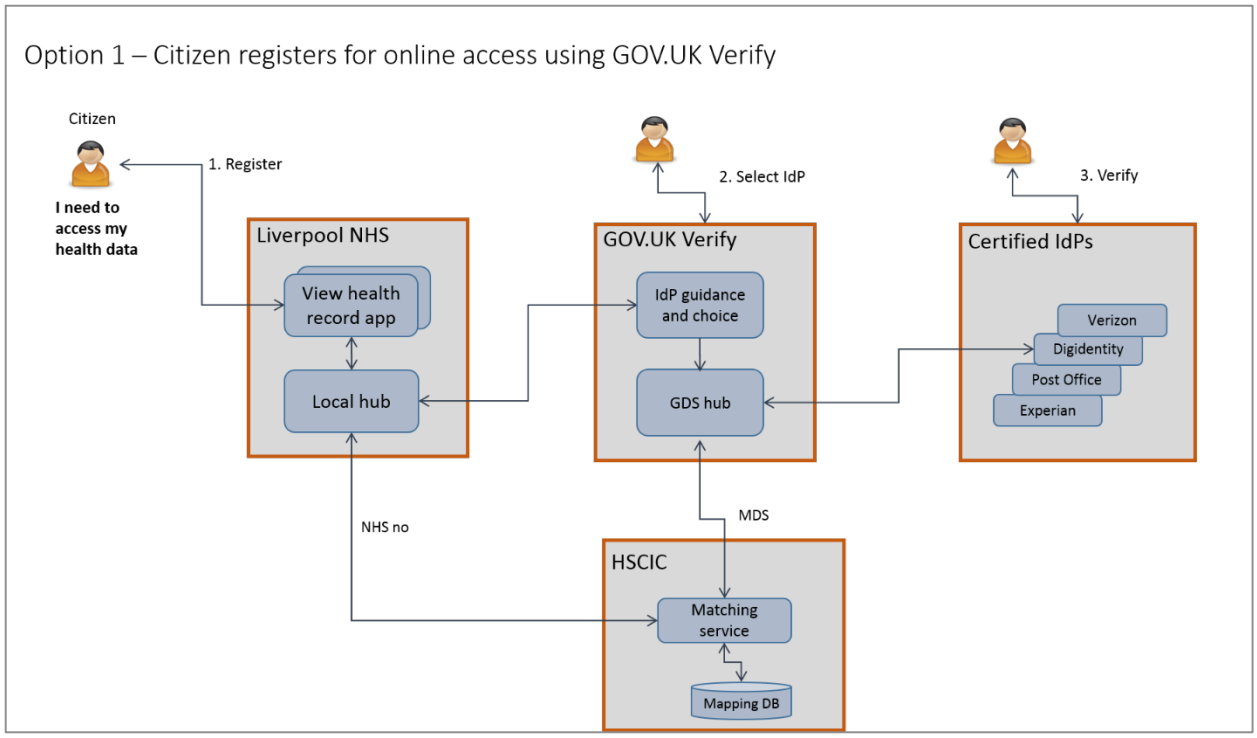
		Warwickshire County Council is a local authority). This would be captured during the onboarding process and provided on each request from the RP for an attribute.
IWG/007	Commercial model	Will a charge be levied on request or on return of an attribute? What if no match is found?
IWG/008	Attribute metrics	There is a need for standards to be developed around attribute naming, level of verification and refresh rate. In addition, other metrics such as coverage and last update will assist relying parties.

Project 2: NHS England Citizen Identity Project

The citizen identity project is about enabling citizens to access their health and care information and to transact with providers. This is an important part of the information strategy of NHS England. The project focussed on the Mi (More Independent) programme, being managed by the Liverpool Clinical Commissioning Group, to test options for identity verification with patients and clinicians at a local level.

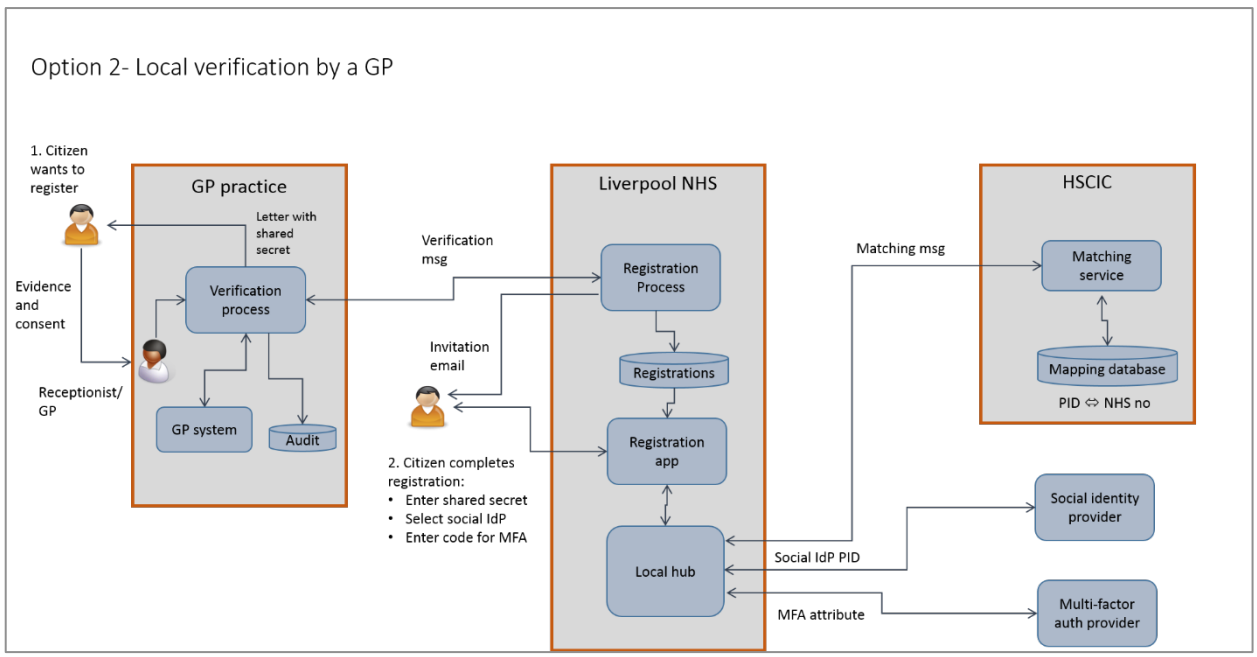
The key objectives of the project were to explore different approaches for citizens to obtain a digital identity in relation to the Mi programme, how trust can be established in that digital identity, and how citizens could use that digital identity to access information across care settings such as GP's, hospitals and social care.

The following diagrams show the two different approaches to identity verification being tested by Liverpool.



In the first option, the GOV.UK Verify solution is used to verify citizens who wish to access their health and care services. Verification is done online through a 3rd party, such as Experian or Post Office. A citizen sets up an account with credentials with a 3rd party of their choice and their identity details are matched to their NHS number by HSCIC. The orchestration of exchanges between the parties is managed by a local hub within the Liverpool domain which interoperates with the GDS hub.

During sign-on a citizen is re-directed to their choice of identity provider. Upon authentication the token issued by the 3rd party identity provider is given to HSCIC which returns a token containing the citizen's NHS number. This token and NHS number can be used by a service provider to grant or deny access to appropriate data and services.

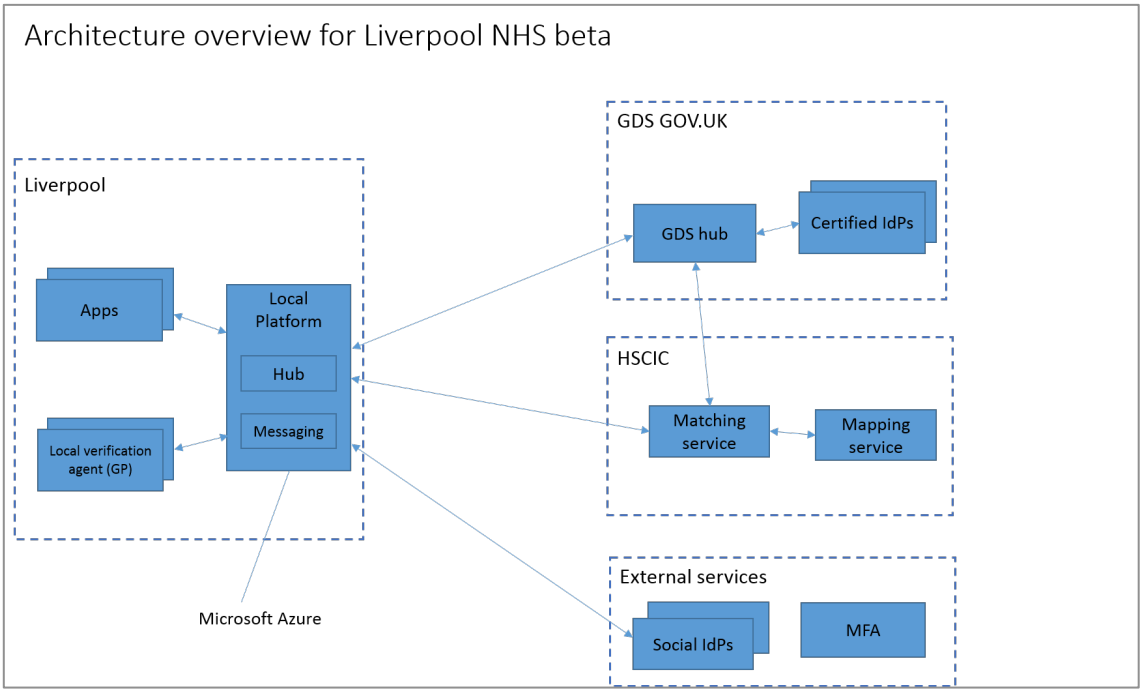


In the second option, a citizen verifies their identity at their local GP practice. This option is needed as there are groups of citizens who will be unable to use Verify, e.g. don't have a passport or driving licence, moved address recently, or thin file with agencies.

A citizen can visit their GP practice for face to face verification by either presenting identity documents or by a professional vouching for the citizen. Local GP practices will be acting on behalf of their local health commissioners so that a citizen can set up an account for online access to multiple providers. A letter and email are issued to a citizen with codes for completing registration. On completion of account set-up the citizen's NHS number is matched to their choice of social identity and method for multi-factor authentication.

Within this Alpha project, both options are brought together to provide alternative ways of establishing a trusted identity. Once established, the resulting digital credentials can then be used to share data in an attribute exchange process. The local hub provides the capability for attribute exchange so that each relying party service can define a policy of required attributes. During sign-on to a relying party service a request is made to the local hub which fulfils the relying party's policy through a process of orchestrating multiple steps of attribute exchange with trusted providers.

The resulting technical solution shared the same fundamental principles as Project 1, but the local hub and platform was based on Microsoft Azure. The federation protocols used by the local hub for the Alpha project for open standards based interoperability between parties were SAML, WS-Federation and WS-Trust. The Beta project will include use of OpenID Connect, REST and SAML.



This project differed from Project 1 in a number of significant ways.

1. Digital identities were accepted from a number of sources, one of which was Verify.
2. LoA1 and LoA2 digital identities were accepted. Trust in a LoA1 low assurance identity was elevated through the use of an additional authentication factor, such as a phone and one time number, and by linking a citizen identity to a verified attribute from a trusted source.
3. A principle of vouching was introduced whereby the GP "vouches" for the identity of the user. This enabled both methods of verification to establish sufficient assurance to match to a NHS Number. However, the method of local verification by GPs is not equivalent to the Verify scheme so the use of locally verified identities is restricted to health and care services.
4. The NHS Number was obtained by attribute exchange between the local hub and the matching service of the Health and Social Care Information Centre (and stubbed for the Alpha project).
5. The technical solution combined an identity assurance hub with an attribute exchange hub, using Microsoft Azure.

Details of the Liverpool identity Alpha project are published here.[3] The Alpha project held a number of workshops with citizens and clinicians to solicit feedback and this feedback along with the project findings are being used to inform the beta project which is also documented on this site as the project progresses.

The aims of the Beta project in Liverpool are to launch a pilot service for a federated identity scheme and to establish a generic approach for the use of trust frameworks to govern federation and attribute exchange so citizens can access services across care settings. The federated scheme will include use of Verify and the option for local verification, and it will enable a citizen with a verified identity to access their GP record as an example of a relying party.

Whilst the IWG observed initial progress with this project, and noted the differences between the two approaches, it was unable to provide informed feedback on the approach taken to attribute exchange.

One question that was raised was with regard to the openness and transparency of the design of the technical solution. Was this a generic design that could be delivered by any such solution provider?

Further use cases of attribute exchange

The IWG also considered a number of scenarios where attribute exchange has the potential to transform the delivery of these services. These are set out in the Appendix.

These scenarios begin to illustrate the extent to which attribute exchange could be adopted by the private sector and, at the same time, shape the realisation that attribute exchange needs to be considered in a wider context with industry and sector-wide engagement.

[3] https://bitbucket.org/Sitekit/liverpool-mi-documentation/wiki/Home

Use cases where the user may not be present

The definition of attribute exchange highlighted in the Introduction, "*The online, real-time exchange of data specific to the transaction in hand, with the user present and with their full knowledge and permission"*, was taken from the Blue Badge Alpha project referenced previously in this report. However, there are numerous situations where the user may not be present but has pre-consented to certain information being shared in the future.

An example could be that the user has consented to allow their bank to check with their mobile operator if the user travels to another country in order to ensure credit card fraud risk is minimised. The mobile operator detects this automatically as soon as the user switches their phone on in a new country and lets the bank know. No other user intervention is required. In this case, the user is not "present" in the transaction flow in that no separate user action is required in the flow between the bank and the operator.

There are numerous other examples as well such as a silent check to see if a mobile phone is listed as lost or stolen to protect the owner from possible account takeover. In this situation, it is not desirable to have the user involved as the thief may be in control of the phone and impersonating the user.

Within the Blue Badge service there is also a case where an applicants' eligibility is not permanent and could be rescinded at a future date within the 3-year validity period of the Blue Badge. In this case, user consent could be sought to periodically check the state of that eligibility with the DWP rather than rely on the user to inform the service when they are no longer eligible.

In the review of the Blue Badge Alpha project, IWG/005, the "enduring permission" requirement, would also back up the view that the user does not need to be present for each attribute exchange, leading to that condition being dropped or amended in the definition.

One issue that has previously been raised in the context of "consent being given for future events" is that the user forgets he/she has given consent. This would need to be addressed going forward to maintain transparency, perhaps in the form of reminders such as with a continuous Direct Debit or Credit Card payment (typically annual service agreements / breakdown cover etc) or confirmation that something has happened. Could and should the user be offered an opt-out?

Question to be considered

Should such examples be considered as attribute exchange or a variant of it, and benefit from the governance, controls and common technology in place in an attribute exchange ecosystem? Or should they be viewed as a completely different form of data sharing?

The need for a common approach to attribute exchange

It is widely acknowledged that attribute exchange has the potential to transform the delivery of digital services within and between the public and private sectors. The project reviews and case studies are illustrative of the scope. What is also acknowledged is that there are different approaches to achieve this. Suppliers in this field will inevitably advocate their own solutions as being the best!

Within OIX the objective is to cut through this and explore through a series of projects the key challenges of creating convenient, secure and privacy-enhancing digital transactions. Projects are undertaken as a collaboration between organisations and the results are published. This approach is fully transparent, doesn't favour one organisation over another, and creates the building blocks for an emerging ecosystem and supporting market. Done properly, it leads to solutions being designed the right way for the right reasons.

The IWG recognises, though, that many attribute ecosystems will coexist in the future. Behind each of these will be operating rules, standards, definitions, protocols, interfaces, legal and commercial arrangements – all enshrined in the trust framework.

In a world of attribute exchange ecosystems, the IWG advocates that wider, more holistic issues need to be addressed from different perspectives.

The user perspective

The evidence gathered from the user research in the Blue Badge project shows that "users were somewhat matter of fact about their experience, happy to say that the attribute exchange driven online Blue badge application was a good idea but, tellingly, unable to articulate their understanding of the overall journey accurately".

Public sector digital services will be accessed on an ad hoc or periodic basis (annually to file a tax return, every 3 years for a Blue Badge, 10 years for a passport or driving licence renewal). Many of the more complex services will require attribute exchange. Services have to be delivered in a consistent, intuitive way so that users become familiar with the approach and process, if not the transaction itself. There are no user manuals for public digital services. Users go to family, friends and Google to get help and support.

Users will need to be confident in using the service, knowing it is genuine, secure and trustworthy. It is their identity and their personal data that is being accessed and shared. A common approach to the digital delivery of services with clear signposting, branding and accreditation will greatly facilitate this.

This implies relying parties need to take a consistent approach to designing digital services that incorporate attribute exchange and to do this they will need a consistent, maybe standardised approach to obtaining attributes – at least to the extent of handling users' permissions and observing users' privacy.

Questions to be considered

1. Is this a fair assessment?
2. If so, how can this be achieved?
3. Does this need to extend beyond the public sector to the private sector, particularly when considering the need for attribute exchange between these sectors?
4. What parallels exist?
5. Can examples from the private sector, such as the consistent approach to designing online shopping carts and online payments, provide guidance for attribute exchange ecosystems?
6. How do we reach industry norm where the key principles of privacy, trust and security are always implemented?

The relying party and attribute provider perspective

The Government Digital Strategy sets out an intent to design and build technical components once and use many times – to create common capabilities. GOV.UK Verify is one such capability. Attribute exchange has the potential to be another for the real-time user-permissioned sharing of data between organisations in a transactional model.

In practice many attribute exchange networks are likely to emerge and each relying party and attribute provider, being the end points in the network, may have to connect to more than one.

For a relying party and attribute provider, this should mean developing one gateway capable of connecting to any attribute exchange network in an identical manner, using open protocols, thus ensuring consistency and standardisation, driving down development costs, increasing quality and reliability and accelerating digital transformation and the take-up of such services.

Questions to be considered

1. Could and should attribute exchange ecosystems develop in such a way that a relying party and an attribute provider could plug into any attribute exchange hub with minimal configuration and no bespoke development?
2. If so, how could we build industry consensus around standards?
3. If so, what barriers would need to be overcome to allow this to happen?

Trust frameworks

In any industry or sector where there is interoperability between organisations to deliver a service that is safe secure and trusted, there needs to be a binding legal framework in place. This framework covers all aspects of operation. It may exist at an international, national or sector level. Examples can be found in the airline industry, rail transport, energy, banking and payments, and credit referencing. These legal frameworks may be regulated and governed by government bodies or be subject to industry self-regulation.

In the digital identity and attribute exchange world, where trust is all-important, we refer to trust frameworks. These combine technology with business, legal and policy considerations, together with assessment and certification functions, to provide top level governance. All organisations interoperating within an identity and attribute exchange network would be required to sign-up to the governing trust framework.

The IWG has reviewed the OIX white paper, *Attribute Exchange Networks: New Infrastructure for Digital Business*[4] that introduces the OIX Attribute Exchange Trust Framework. Its view is that the model for establishing trust frameworks should follow the specification set out.

The specification strongly recommends that communities of interest should establish working groups in the areas of business, legal, technical, privacy and assessment and certification.

The communities of interest are formed from relying parties, attribute providers and identity providers, supported by assessors and auditors, dispute resolution functions and trust framework providers (who oversee the deployment of the attribute exchange network).

However, the IWG has no strong preferences as to how this should be accomplished and would recommend consideration of how models have developed in other industries and sectors to provide guidance.

Questions to be considered

1. How and where should we start?
2. Who should take the lead?
3. Will the market need "seeding" and, if so, how and who?
4. What should be the roles of GDS and OIX?
5. What type of organisations might fulfil the role of trust framework provider?
6. What are the options for commercial models?

Conclusions and recommendations

Attribute exchange is hugely important in the transformation of public and private sector services. The Blue Badge use case has demonstrated what could be achievable within a typical, complex government service as have the private sector use cases referred to.

Attribute exchange enables data sharing across organisations in a way that is transparent, observes user privacy and is inherently less exposed to abuse than other methods.

For the user it means

- They are in control and can give or refuse consent to data being shared

[4] See http://openidentityexchange.org/wp-content/uploads/Lockstep%20AXN%20Whitepaper%20(1.2.1b).pdf

- Less keyboard work is required and they cannot make keying errors
- They get an outcome during the online session

For the business it means

- Large amounts of data do not need to be extracted, transferred and stored, between organisations – just in case they are needed
- "Trusted" attributes do not need to be verified, saving process time and operational costs
- Not having to integrate with multiple sources and maintaining many point-to-point links
- Reducing back office costs
- Providing a better customer experience and service

Although the principles and benefits of attribute exchange are reasonably well understood, we are still only at the beginning of the journey of development, deployment and transformation.

Attribute exchange is the catalyst to create a new commercial market, spawning a new generation of opportunities for attribute providers and technology solutions. Building new digital services, driven by users, to replace costly and inefficient offline processes will deliver massive cost savings to relying parties.

Industry, sectors and organisations need to come together to make a market. How this happens remains open to discussion. One approach might be to follow that being taken to discover the needs for UK identity assurance[5]

To kick start this discussion, share views and ideas, and gauge interest we have set up a discussion forum within LinkedIn and invite you to join in : http://bit.ly/1Nm9HDU.[6]

[5] See http://oixuk.org/wp-content/uploads/2015/09/Discovering-the-Needs-for-UK-Identity-Assurance-V21.pdf
[6] See ????

Appendix A – Use Cases

In this appendix several use case scenarios has been set out that illustrate the potential scope of attribute exchange.

- ABC Insurance Company
- Retail check out and payment
- Opening a bank account
- Opening a utility account

ABC Insurance Company
Introduction to the specification for Data Attribute Exchange: Disabled Driver Insurance Premium Relief

ABC Insurance recently issued an RFI to evaluate the provision of access to GP and DWP records to facilitate the validation of an applicant's health records to determine the validity for certain exemptions from surcharge based on pre-existing medical conditions.

For example, ABC Insurance offers reduced Motor Insurance Premiums (MIP's) to drivers registered disabled and who

a. Are currently registered disabled
b. Eligible for support under the Driver Mobility programmes or qualify for the new Personal Independence Payments awarded by DWP.
c. Have current motor insurance as a disabled driver before (or have held disabled driver cover in the past 18 months)
d. Have completed a Disabled Drivers awareness course approved by DVLA.
e. Have no history of certain medical conditions that would preclude lower risk premiums by the insurance underwriters; for example, blood pressure anomalies, epilepsy etc

The objective for ABC Insurance in this case is the full automation of the validation process at the time of online application by an insured driver.

The flow of attributes required for this example is as illustrated in figure one below.

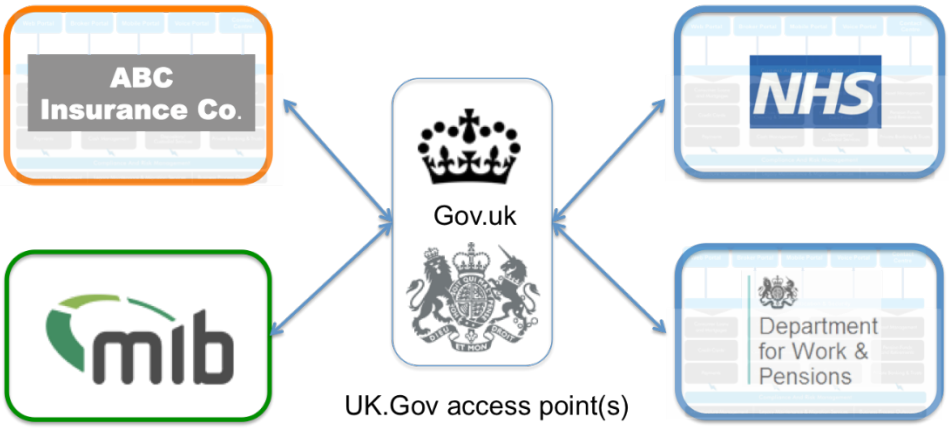


Figure: overview of the data stakeholders in this user case

In this example the decision process is based on data sourced from three "Attribute Providers"

1. Motor Insurers Bureau, (MIB). MIB holds data on previous policy holders and those who are currently insured.
2. NHS/GP records to validate medical condition exclusions
3. DWP for validation of a person's entitlement to disability benefits and/or the new PIP scheme

In each case, ABC Insurance is seeking a simple "Yes-No" validation on given criteria when making an underwriting assessment to apply (or not) a discounted MIP.

In this specific case, the group does not envisage making use of more detailed attributes/data relating to medical conditions or benefits entitlement and the like in the foreseeable future, as the automated underwriting process currently in place would not be able to make distinctions beyond the "yes-no" attribute that currently (manually) validates a person's status as being disabled.

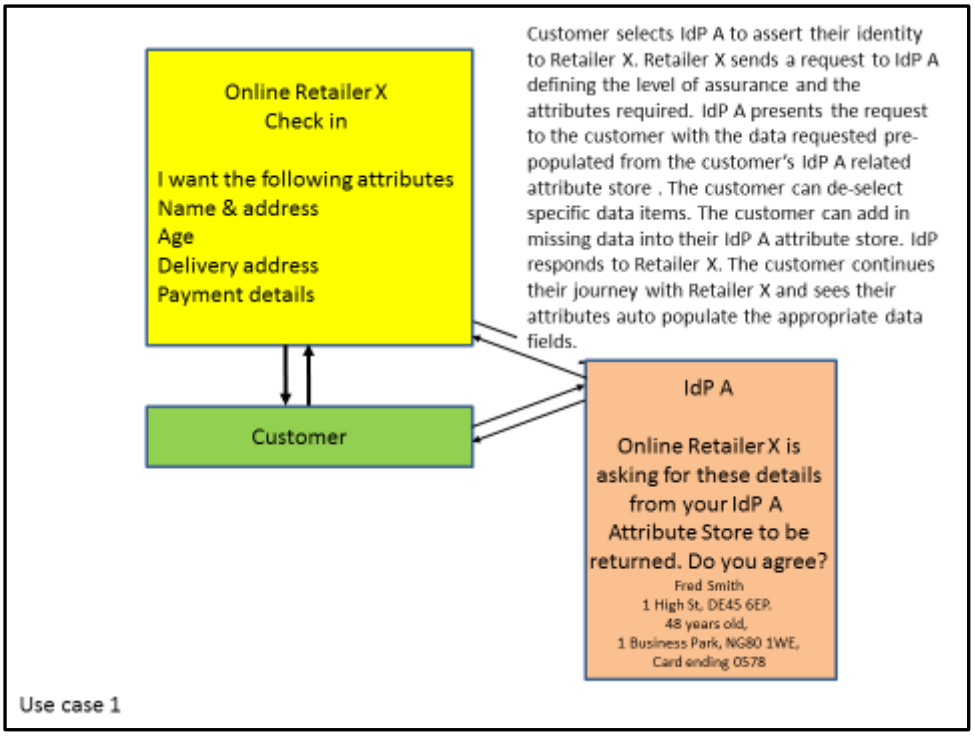
In other cases, such as obtaining specific licence details via DVLA, it is likely that the group would seek where possible multi-layer attribute exchange for validation of insurance conditions.

It is estimated that cost savings in the group would be derived from

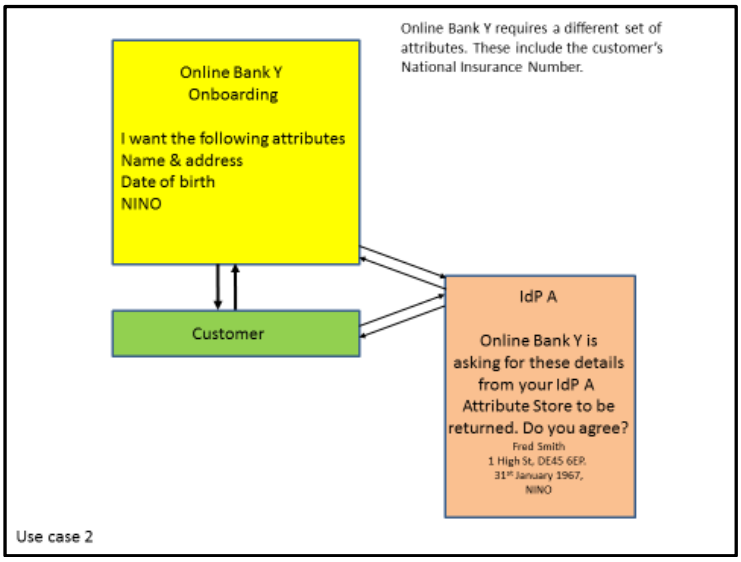
1. Reduction in fraudulent claims
2. Operational overhead in processing applications
3. Reduction in underwriting costs based on verified data affecting risk under individual MIP's

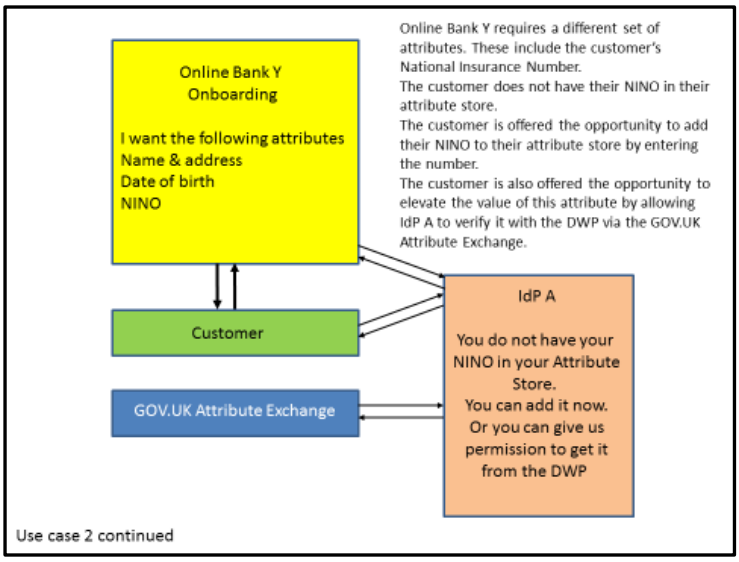
Based on such savings, the group have indicated that they would make a very strong internal business case for participating inside a contribution-based attribute exchange service with the likes of DWP, NHS and DVLA across multiple elements of their business.

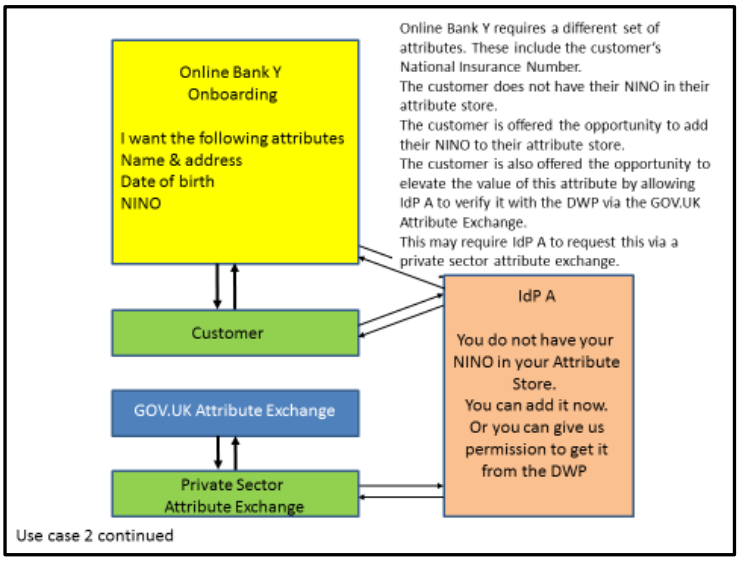
Online retailer – payment details



Opening an ISA with an online bank







Online utility onboarding