mydex

Scottish Government
Riaghaltas na h-Alba
gov.scot

Digital
Scotland
Digital Identity Scotland

Final Report

Attribute Prototype Project

24th April 2020

Mydex CIC Partner

DIGITAL
HEALTH & CARE
INSTITUTE

Table of Contents

Introduction

The aim of the Digital Identity Scotland (DIS) programme is to develop and implement a new way for people in Scotland to prove their identity when they access public services. This would enable individuals to create a digital identity, which then can be used and re-used for secure access to personalised services from public service providers.

The objective of the 10 week project was to build an attribute prototype to test a conceptual architecture for delivery of an attribute led approach to delivering an identity service and wider attribute service across Scotland for the benefit of citizens and public service providers to reduce friction, effort, risk and cost and improve the experience and outcomes from accessing public services.

This is the final report for the project outlining what was delivered, key findings, lessons learned and recommendations for future work that may be undertaken as part of the Digital Identity Scotland programme.

Summary of Report

The goals of this project were to build a prototype to test whether an attribute led approach to service provision can work, and to identify key next steps in implementation, should the Scottish Government decide to pursue this approach further. The outcomes are:

- A working prototype which enables public sector organisations to provide individuals with verified attributes, for individuals to store these attributes in their own Attribute Store, and for these individuals to be able to share these attributes with other public sector service providers as and when needed.
- The prototype is available (through a secure link) for the programme to experience and use, will remain in place post the end of the project and is a potential foundation to build upon in terms of a) operational implementation and b) extension and development of functionalities and capabilities
- Testing of the user journey shows that users quickly and easily understood how they could benefit directly from the introduction of this approach e.g making it easier to apply for and use services.
- At the same time, users did not immediately grasp how using this approach also helps service providers help them e.g. by improving efficiencies, cutting costs and speeding up service provision. This is an important communication challenge and opportunity which needs to be explored further because it provides users with added incentives to contribute

and participate.

- A number of ways of authenticating the identity of participants were tested. Some are already well understood by users, others less so. Also, not every service needs the same levels of assurance. A key finding of this project is the need for a 'horses for courses' approach to authentication where the right user journey is identified for the right service, taking account of both user skills and comfort with different processes and services' needs for different levels of assurance. This is an area needing further, further, more detailed work, which must incorporate the reality of sufficiently securing the citizens's account with two or more factors.
- During the user research, questions were raised about issues relating to data security and user control. These were not substantive questions in the sense that they identified shortfalls in the design of the prototype. Rather, they were communication issues, with users not fully understanding what security and control safeguards were already available. Further work is needed on the communications relating to different user journeys.

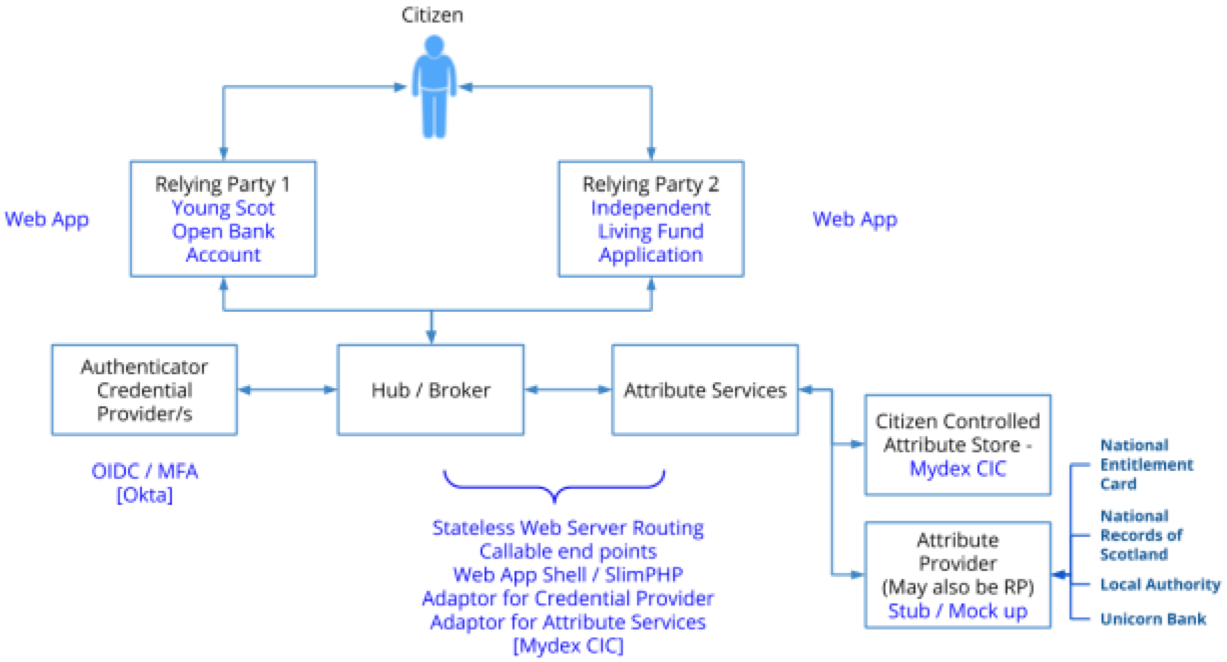
A series of recommendations have been made in this report about potential next steps to take this concept forward with a path towards implementation and ongoing research and testing. These are

- Undertake options appraisal for the creation of an attribute ecosystem across Scotland to initially benefit citizens and public services
- Cross reference and collaborate with outcomes from the Smart Entitlement Strategy project
- Learn from existing projects and programmes already implementing a citizen centred attribute led approach to deliver public services
- Undertake further design, research and testing in key areas covering the positioning and communication of concepts related to the prototype

What was done during Project

Creation of a working prototype

The prototype has built the technical infrastructure that enables individuals to create a set of credentials for accessing government services and their own Attribute Store linked to the credentials in which they can accept verified attributes from public service providers, to store these attributes safely in their Attribute Store, and to forward them to Relying Parties, when asked, for the purposes of service application or provision. The core elements of this prototype and how they relate to each other are shown in the diagram below. The blue text identifies who and what is being delivered against the prototype architecture.



In conjunction with this, initial methodologies for onboarding citizens and taking them through the journey, including giving consent to receiving and onward sharing of verified attributes have been developed and tested, as described below.

The specific use-cases developed for this prototype were a) Using data generated by the Young Scot National Entitlement Card application process to open a bank account, b) Speeding up the application process for the Independent Living Fund. But the capabilities built into the prototype can now be applied widely and generally, with very little extra work, to all other use-cases involving the sharing of verified attributes.

The prototype was built under Mydex CIC ISO27001 certified development and deployment processes.

A dedicated domain name was registered for the project to give the prototype its own identity. All software deployed and configured is protected within online code repositories and released using automated deployment routines.

The prototype utilises the Mydex live Personal Data Store sandbox environment for the provisioning and delivery of the citizen's attribute store.

There is a dedicated stateless hub operating that orchestrates all the activity between the specific web apps and other components in the architecture. Each journey outlined in the scope of the project can be demonstrated. The credential provider service was set up on a trial basis.

The components provided by Mydex CIC are all built on top of open source software and utilising open standards. The credential provider was integrated using open standards.

Data flows between the citizen's attribute store and the relying parties were all encrypted and controlled by dynamic consent decisions made by citizens during journeys.

There is strong emphasis on creating a seamless experience for citizens with a logical progression and intuitive navigation and choices. The architecture enables scalability and extensibility and a high level of resilience through the use of a distributed model for data storage and retrieval coupled with the potential for different providers of each component. At its core is a shared service stateless hub / broker that would be owned and operated by the Scottish Government

Research and discussions on Metadata and Attribute Standards

At the heart of any attribute based service is the metadata about the data being delivered and retrieved. The goal is to ensure maximum reuse and understanding of the data. There are an extensive range of projects and programmes exploring data standards across many different sectors and schemes. The Scottish Government can draw on those projects and programmes where relevant. During the project it was possible to identify a range of options for defining metadata and attribute standards to enable the portability of trust and provenance between attribute providers, citizens attribute stores and relying parties. There are many options which can be agreed as a starting point whilst leaving the approach open to extension and broader interoperability as standards emerge and are widely adopted.

Research into use of Multi-Factor Authentication

Some desktop research was undertaken relating to different forms of authentication mechanisms beyond basic use of a username and password. This additional form of authentication, broadly termed two factor (2FA) or multi-factor authentication (MFA), can enhance security and safety for citizens in accessing services but can also make it more difficult for the citizen to understand and undertake the steps needed to complete the set of this additional layer up and then operate it.

From the research undertaken, a summary of which is in the Appendix C of this document, a range of options were selected for inclusion within the prototype. These included:

- One time codes sent via SMS to the citizens mobile phone
- Authenticator apps installed on mobile devices that could generate one time code in real

time to access a service

- Dynamic push notification to a mobile device running an authenticator app enabling the citizen to confirm it was them logging into a service.
- Use of device dependent fingerprint and facial recognition was also included.

Different people react to different forms of authentication with varying degrees of acceptance and understanding.

The project has identified and demonstrated that not all transactions citizens may wish to undertake require the same level of strong authentication. This has identified a need for configurability and preferences to be expressed from both the service provider (relying party) and citizen's perspective. Consideration should therefore be given to support for different levels and forms of multi-factor authentication based on context of use and preferences of citizens.

Choice of 2FA/MFA is certainly desirable, however the overall service should remain protected at appropriate levels of managed credential if we are to avoid risks of takeover, hijack and breach. If MFA includes dynamic risk assessment based on device and behaviour characteristics, then the user journey may involve fewer second factor re-authentications, but this balance and the attendant monitoring / privacy concerns must be addressed by the DIS programme.

Engagement with potential stakeholders

A range of briefing papers were produced to support engagement with different stakeholder groups along with a range of workshops and virtual meetings held via conference facilities. In addition specific user research was carried out with citizens throughout the prototype to test and learn from their experiences.

Workshops were held with two organisations to explore specific use cases where the provision of trusted verified data could deliver an enhanced and streamlined experience, reducing friction, effort, risk and cost for citizens and service providers alike. These were:

- **Young Scot** - exploring a specific use case around opening a bank account. This use case was chosen to provide a generic scenario for user testing that participants would be able to understand. The central point of the use case was to show how the verified data underpinning their Young Scot Card could be reused to open a bank account reducing the time it took and removing the requirement to supply the information and documents normally required. The net result was the young person holding their own proof of identity. Verified details of their new bank account could then be further reused for other services or application processes where proof was required.
- **Independent Living Fund Scotland** - the specific use case was to explore how the application process for the transition fund could be enhanced and streamlined through the

use of verified attributes. This represents a potential real-life future public sector use case, which user research participants recruited through ILF would have experienced. The person making the application could share these verified attributes from their own Attribute Store. Examples of such proof points were identity based on National Entitlement Card, Bank Account, proof of financial status and disability - all attributes provided to them from service providers already supporting the individual.

Meetings and conversation were held with:

- **The Improvement Service** who are a key service provider to local government and the Scottish Government. They have a clear view of the landscape of systems in use across the public sector and operate a number of services that generate and store verified personal data such as the National Entitlement Card and myaccount service. They also provide a range of data processing services for local authorities which could provide a valuable means of enabling verified attributes to be made available to citizens for reuse.
- **Social Security Scotland** is in the middle of building new systems to administer and manage devolved benefits for the citizens of Scotland. The purpose of the discussions was to share knowledge and experience to ensure that alignment between the Digital Identity Scotland programme and the requirements in the future of Social Security Scotland.

Wireframes to support user research

Initially, working wireframes within the prototype were produced to support user research as part of the core prototype development itself. The pace of change requested however led to the creation of separate ‘interactive wireframes’ that could be more easily adapted as part of the user research process.

The 'interactive wireframes' created were high fidelity prototypes covering the user interface (visual and aesthetic) and also the user experience aspects in terms of interactions, user flow and behaviour. These high fidelity prototypes are interactive and closely resemble real life systems. For the purposes of this document, the high fidelity prototypes are referred to as 'wireframes' for clarity and to distinguish them from the working prototype.

The resulting wireframes were fed back into the prototype build process so that the working prototype reflects the experience created and the lessons learned during user research.

User Research

During the ten-week proof of concept between January and April 2020 we evaluated a series of prototypes to explore young people’s responses to a Scottish Government credential, different approaches to multi-factor authentication and the use of citizen controlled Attribute Store, and decision making during journeys relating to consent for sharing of and storage of personal data.

The participating citizens identified a series of design issues, which fed into the iteration of the prototype system. They also discussed the area more generally. The key findings were:

Citizens understood easily the value to them of an attribute store in reducing the friction and effort in making online applications and the removal of repetitive form filling and provision of evidence in application processes and ongoing service engagement. The concept of capture once and use many times was obvious to them. They had less understanding of the potential value to themselves and to service providers of verified attributes and how this could speed up application processes and reduce cost, risk, effort and friction within the back office processes of service providers. This is an area for future co-design and research as appreciation of the benefits would be a strong motivator for seeking access to and sharing verified attributes.

The term attribute store itself was not considered by those involved in the research to be the most obvious name. Further consideration to terminology should be considered such as Personal Data Store, Personal Data Locker, Personal Wallet, Personal Data Vault.

Security, trust and control are key areas for ongoing investigation. Citizens do care about the security and control of their data and are keen to understand who can view their data and for what purposes they are using it.

Citizens want to know more about how they can control their personal data safely and securely. Some aspects of personal data are considered more sensitive than others in particular because it may affect the services and benefits they receive.

Citizens expressed the desire to be able to store additional information in their attribute store even where it was not verified.

More design and research is needed to better explore how best to convey the benefits and key areas of understanding around security and control. The prototype would benefit from extensions in capability to test different communications and journeys with a wider group of citizens and additional use cases.

A break down of the findings from the user research report is in Appendix B and the UX review report is Appendix D of this document

Creation of specific documents

- **Final Report** - This document
- **Stakeholder analysis and key themes** - looking at the concept of verified attributes from their perspective both as an attribute provider and relying party.

- **Communications collateral** to support briefings for different stakeholders and preparation for workshops along with blog posts as part of the Digital Identity Scotland external communications.
- **Summary Technical Overview** for more technical audiences and stakeholder groups
- **Technical and Security Architecture document**
- **Data Protection Impact Assessment document**
- **Assessment of prototype against NCSC Saas Framework**.
- **User Research Report** - See summary in Appendix B
- **User Experience Report** - See Summary in Appendix D

What was not done during the project

Service Design

We leveraged existing service design experience to feed into the user research and have shared past work that closely matches the scope of the project. Given the timescales involved this appeared to be the best approach.

Mydex CIC and DHI have undertaken to carry out a programme of ongoing service design post the project as part of our ongoing programme. DHI and Mydex CIC have invited Scottish Government to participate in this programme over the next 12 months.

Technical Testing

Opportunities to learn relative to how a production platform may operate were limited given the timescales and deliverables outlined in the scope of the project were that of a prototype. There may have been a disconnect in terms of expectations within the project team centring around the nature of what was being delivered as a prototype and what can be expected in terms of testing of a production platform around API calls, testing content and the API payloads.

Self Sovereign Identity

It was agreed that this element of the conceptual architecture would not be included in the scope of the prototype given that it was simply another source of attributes that is not currently readily available and is simply an alternative technology layer to interface with a store of verified attributes.

Whilst the notion of publishing verified data on some form of ledger may support a number of use cases it would not inform the approach in any significant manner. The core concepts being tested were independent elements of the conceptual architecture working together. At its core was the model of citizen controlled data delivered and collected from a citizen controlled attribute store linked to a standalone set of credentials.

The public sector service providers in this architecture could be performing two roles: a) that of a consumer of verified attributes from a citizen attribute store and b) that of a provider of verified attributes delivered to the citizen's attribute store for reuse by the citizen. The form and format of those attributes could be configured to meet any number of use cases, underpinned by meta data supporting interoperability and transference of trust.

The scope and potential of attributes

The nature of the personal data citizens need in order to apply for and make use of public services is extremely broad and in some cases deep. Verified attributes provided by one organisation as a by-product of their normal service operations can act as a trust anchor for the start of a new relationship between a citizen and another service provider.

Many public services require proof of status on any number of factors e.g. income, disability, housing tenancy, employment, health related matters and all manner of financial and well being information. These need to be able to be combined dynamically to meet the needs of service providers. By equipping citizens to accumulate and share this information in a safe, easy and secure manner it is possible to unlock significant reductions in friction, effort, risk and cost for both citizens themselves and service providers.

A number of core generic user journeys were identified and developed to support any number of different use cases covering

- Registration for a set of credentials
- Creating a Citizen Attribute Store
- Linking the Citizen Attribute Store to the set of Credentials
- Delivery of data to Citizens Attribute Store
- Collecting data from a Citizens Attribute Store

Within these journeys there are a series of **dynamic consent journeys** dealing with the ability for an individual to accept new data being delivered to their attribute store and approve its reuse by one or more service providers acting as relying parties.

In many cases a single organisation may be a consumer of one form of personal data and a generator and provider of another form of data. At a broader systemic level there are significant benefits in enabling citizens to collect and hold certified trusted copies of the data from one organisation and share it with another for different purposes.

Personal Data in the form of Verified Attributes are the building blocks of public services and the transactions that are undertaken. The provision of Attribute Stores by which citizens can receive and share these Verified Attributes changes the architecture of personal data collection and use - moving it from a situation where service providers always gather and store all the information they need, with citizens holding none of this information, to a situation where some of the data service providers need is stored separately from them (in the citizen's Attribute Store) and accessed when needed. The creation of this new, independent layer of data sharing infrastructure is essential to the vision behind this project. It often takes time for participating organisations to understand this shift and begin to see its potential in terms of cost reductions, enhancing citizen access to services and enabling new forms of value. This model may require changes to organisations' systems and processes. The extent to which this is the case will depend on their specific capabilities. By identifying the broad range of benefits to the citizen, individual organisations and wider public sector which drives recognition of the benefit of collective action.

Core to the success of any attribute led approach is the creation of metadata, data about the data which make it possible for different services and systems to understand what data is available, how it was generated and if required by whom, how it is maintained, how current it is and in what format it can be accessed. Metadata can provide the level of confidence or assurance about any specific piece of data and it can be used to find the same data from different sources and do cross comparisons.

It is a taken-for-granted core requirement of this project that everything it does must comply with data protection and other regulations.

Many people assume that the data needed for service provision is highly sector specific: that for health services you need health data, for financial services you need financial data. While it is true that some of this data is highly specific, much of the data needed to provide services (e.g. relating to identity, the basic profile of the individual, basic administration etc) are common to all service provision. Therefore, sector-specific solutions will always be sub-optimal while creating large amounts of duplicated effort. The vision for the Scottish Attribute Provider Service is to equip Citizens to make use of their verified attributes where and when they need in a safe and secure manner beyond their use within the Scottish Scheme e.g. UK Government, Private Sector.

Related Projects

Smart entitlements project

Concurrently with this project there was a Smart Entitlements Strategy project underway that was also being delivered by Mydex CIC and DHI. There was an opportunity to cross fertilise between the two projects and ensure that lessons being learned in one could inform the other. The scope of this project is a strategy paper covering the following areas:

- Stakeholder matrix and sources of attributes
- Review of different operating models
- Review of different economic models
- Attribute matrix looking at sources and value
- Recommendations for an implementation of a Smart Entitlement Strategy

The key areas of relevance were around stakeholder analysis, attribute standards and the wealth of use cases and analysis of the breadth and depth of attributes under the control of the public sector in Scotland.

Social Security Scotland

Whilst Social Security Scotland are not currently considering verified attribute consumption or production there is clearly strategic value that could significantly enhance the citizen experience in downstream use cases where, for example, proof of status will be needed as it can act as a passport to other services and benefits. Like all public service providers, verified attributes can deliver significant reductions in cost, risk and effort in delivering services as well as empowering citizens with access to and reuse of their own data.

Social Security Scotland is delivering a personal data-intensive range of benefits requiring evidence of circumstances and significant levels of information from across a citizens life. Being able to consume verified attributes could significantly reduce the time to apply and process applications for benefits and maintain them. Equally when operational, Social Security Scotland could become a valuable source of verified attributes that could help citizens unlock access to other services they are entitled to. Citizen given consent to the secure sharing of diagnosis or proof of disability or current benefits could significantly improve and streamline access to other services and benefits e.g. concessionary travel.

The main element of engagement during the project was to share knowledge and experience and maintain alignment between the two programmes that are running against their own programme plans and timescales.

Learnings from the project

What worked well

Proving the conceptual architecture technically - the conceptual architecture works and can be scaled relatively easily, the benefit of independent components interacting to deliver outcomes reduces risks and increases the capability to scale and support the widest range of use cases.

Understanding the importance of Meta Data and Attribute Standards - Significant value was gained from the knowledge and expertise relating to meta data and attribute standards which has enabled some clear recommendations to be made about how Scotland can make positive progress to meet its own needs whilst maintaining the potential for interoperability with other schemes.

The insights gained for user research and iterative development of wireframes and language based on citizen testing and their subsequent deployment into the working prototype.

Collaboration between the project team members - Many members of the project were new to the subject and others had a significant depth of experience and knowledge. Effective ways of working were established quickly and knowledge sharing was undertaken at the earliest opportunity. Good use was made of online collaboration tools to share documents and track the project enabling a whole project team view of progress. There was some additional overhead and project members had to feed into their own internal systems as well.

What were the challenges

Clarity about roles and expectations at start of the project - One of the key elements of the project was to secure agreement on key deliverables at the outset. We had to adapt the original project plan to accommodate a different mix and number of project team members and ensure that the scope was understood based on the ITT issued and proposal made. This may have added some delays but as a result, a broader group of people have now engaged in the whole attribute led approach who have been drawn from diverse backgrounds and experience.

Bringing components together - we had a clearly defined set of components as outlined in the conceptual architecture that we intended to build the prototype from all worked well individually. Mydex CIC needed to add new capabilities to support the objectives for dynamic consent steps that could be embedded into relying party journeys. We also had to test a range of paths for integration between the credential provider and the stateless hub to find the most appropriate ones to meet the objectives of the prototype. Ensuring a seamless end to end journey for the citizen also required some innovation to ensure consistency such as being able to embed consent steps and first time connection steps between credentials and Citizen Attribute store into the main use case journey.

Third party credential provider

We selected Okta UK Ltd as an off the shelf cloud based third party service provider that could meet the requirements of the prototype. Their platform was feature rich and had extensive documentation. New features were being added to their platform and this meant that some of the documentation was not completely up to date.

Support was excellent both from the technical and commercial teams. They had a clear understanding from the outset that this project was only a prototype but it could inform future projects.

Some of the requirements were UK specific and required additional information from the credential provider especially in relation to their conformance to a range of UK standards and guidelines.

As stated earlier some important considerations have come out of the research into multi-factor authentication. We explored these issues within the configuration of the credential provider and registration sign up journeys.

- **Context is a key consideration.** Not all transactions need the same levels of authentication. Some do not need multi-factor authentication. We tested SMS, Authenticator Apps and Push Notification, each as different levels of challenge and benefit for citizens. It should be possible for relying parties to specify which approach is required within the scope and parameters of the scheme to protect the security and integrity for the citizen.
- **Giving citizens a range of choices may increase take up and understanding.** The user research identified that there needed to be a better balance between the needs of citizens and the service providers as most requirements were defined in purely organisation terms.

The approach used can be applied to any credential provider wishing to take part in any future attribute led ecosystem thereby affording citizens choice if desired. Equally the Scottish Government may want to support a Scottish Government branded service as well.

Dynamic Consent Journeys

The project placed a strong emphasis on transparency and choice. We tested citizens' understanding of different options for consent relating to accepting delivery of data to their attribute store and approving access to this data. We called this 'dynamic consent’

There is a spectrum of use cases to be considered here and more research needs to be done. In particular we need a better understanding of a) how this form of dynamic consent works during online transactions and b) how it could be augmented by approaches whereby citizens can set broad rules about data acceptance and access in advance. Logically consent management is an integral part of the Attribute Store and available to be integrated into journeys.

Core to data sharing in a citizen-set data sharing policy and preferences is trust and confidence in the relying parties and their specific intentions in using the data. For example is it simply to support an application for something or to operationally deliver something? Or does it include secondary uses of data where it may be used for other purposes or shared with third parties for reasons beyond the scope of the initial service?

Not all collection and use of data necessarily needs consent because there is some form of legislation that mandates its collection, for example where data collection is necessary for the provision of the service requested. Protecting citizens' personal data from misuse and ensuring they have the privacy they are entitled to is a core foundation of an attribute ecosystem. This means citizens need to be able to exercise their rights under transparency obligations placed on organisations including data usage reports delivered on request.

It is worth highlighting that citizens commented that they may wish to have more active control over sharing the same data with the same organisation e.g. if disability changes such that they are entitled to a higher level of benefits, they would be happy for this to be automatically changed, but not so if it was the opposite way round.

There is lots to debate relating to this individual point but regardless, there is an underlying principle to be explored that "data is not neutral" to users and thus a system should not treat it as such i.e. the rules may end up being so complex that they are unwieldy and citizens may not engage in setting rules. Equally if they are too simplistic, citizens may not have trust in the system and/or there are unintended consequences. This is certainly worth exploring further in additional user research and co-design activities.

More discussion is certainly desirable. DIS needs to make decisions on its offer and how it can be explained to citizens and service providers, and the scope of its service.

On the matter of scope, data collection e.g. from private sector service providers is currently out of scope. Data collection mandated for service provision e.g. social security applications means the consent arises from the need to give a citizen a choice - either to use the verified data in their attribute store OR to type the data in again and accept the potential delays for an application to be processed whilst self asserted data is verified in the back office. The law to collect is the same, the consent is for a different reason. Most importantly we need to protect citizen trust in the service offering - without clarity and simplicity Scottish Attribute Provider Service will not reach critical mass, and thus not achieve reuse of value from other Government investment in verification and thus reduction in friction, effort, risk and cost for all parties.

Citizen Attribute Store

The Citizen Attribute Store is initially largely invisible to citizens with exception of the Dynamic Consent management process, but it is an integral element of any journey, providing the ability to save attributes gathered during one transaction and to reuse them for other transactions. This helps remove form filling and make life safer and easier. For the citizens there was no need to do anything technical to get or use their Attribute Store; it was set up and provided automatically for them as part of the process. The goal is safe, simple and secure use of personal data where and when needed.

Some citizens were keen to know more about their Attribute Store and access it directly. This is an area for future research

We used a mature pre-existing personal data store for the prototype that is live and already certified under ISO27001 for information security management under FairData. Citizens are in total control of how and where data is used. The store provider, Mydex CIC, has no access to the data held within it.

We fully expect that any future attribute ecosystem will encourage citizen choice in terms of which attribute store services they use. It is a key consideration for any future Trust Framework or scheme that sets out the standards for involvement of attribute stores and any certifications that may be required.

Recommendations and next steps

Undertake options appraisal for the creation of an attribute ecosystem across Scotland to initially benefit citizens and public services

- Create a shared service using a combination of open source components and existing services available in Scotland today from procurement frameworks
    - Define key deliverables required to implement the conceptual architecture and necessary governance frameworks
- Undertake a live pilot using existing verified attribute sources to populate citizen attribute stores and two or more public services to act as relying parties. Ideally a low volume, low risk starting point that offers high value in terms of learning and relevance
- Define and agree meta data and attribute standards for use within Scottish Government Framework for attribute services

Cross reference and collaborate with outcomes from the Smart Entitlement Strategy project

- Attribute and metadata standards
- Key sources of verified attributes within the public sector in Scotland
- Consideration for the creation of a shared service that would enable a consistent approach to making verified attributes available to citizens as part of any future ecosystem.
- Engage with key stakeholders about the potential and benefits of being a verified attribute provider and/or relying party in terms of reductions in friction, effort, risk and cost and improving equality of access, outcomes and efficiency of public services

Learn from existing projects and programmes already implementing a citizen

centred attribute led approach to deliver public services

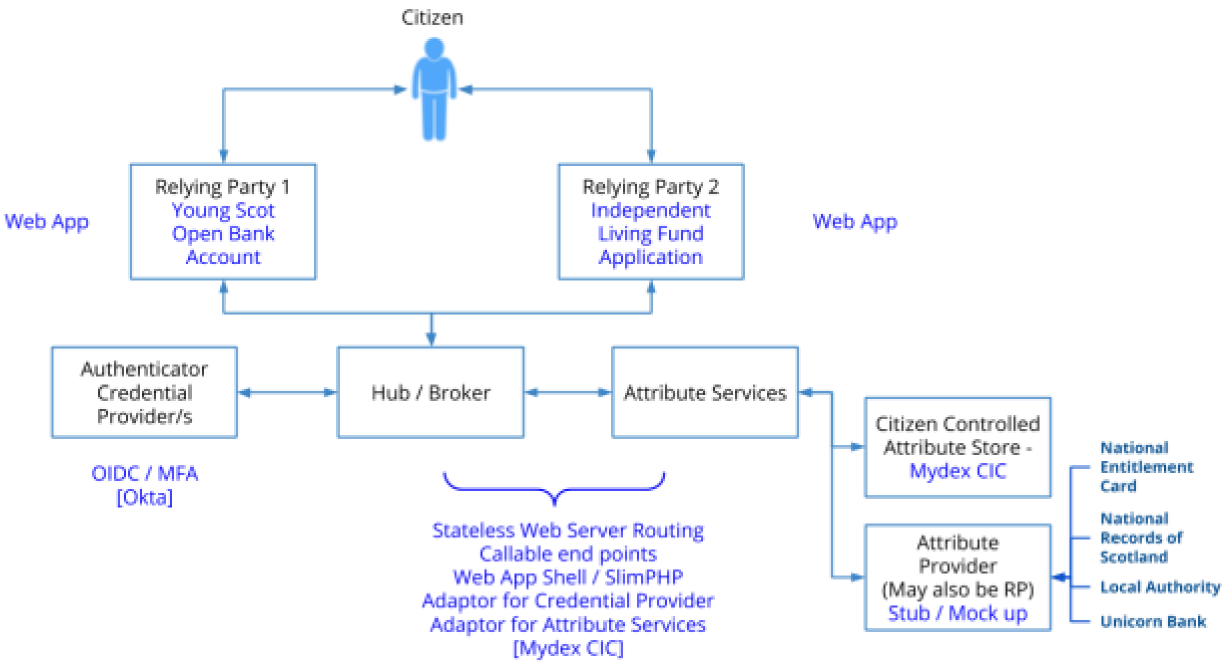
- **Digital Health and Care Institute programme** of innovation across health and social care utilising a personal data store to act as a personal health and care record
- **Macmillan My Data Store Project** to equip people affected by cancer with their own personal data store and simple web apps to manage their cancer journey and how they collect and share personal information with their network of service providers

Undertake further design, research and testing in key areas covering the positioning and communication of concepts related to the prototype

- Security, trust and trustworthiness in the services and actors involved
- The value of 'verified' attributes in removing friction, effort, risk and cost for each stakeholder
- Understanding of the broader potential of a citizen attribute store itself
- Branding of services to ensure understanding and creating a sense of coherence

Appendices

Appendix A: Summary of prototype elements



The following provide summary overview of each element of the prototype

Citizen - A citizen seeking access to one or more services supported by the attribute prototype. This citizen will need some form of digital credential in order to gain access to services. The prototype needs to enable the citizen to approve access to specific attributes in the context of one or more services. Citizens should be able to start a journey without credentials and elect to register for them during the journey.

RP1 and RP2 - These are the Relying Parties who will make use of the attribute services. They are service providers delivering one or more services to citizens which may require a range of verified and self asserted attributes from citizens seeking to access a service. Citizens will need to prove entitlement or facts about themselves to these Relying Parties. The Service Provider/Relying Party will be able to specify what attributes are required in order to access a service. The broker will orchestrate access and delivery of attributes to the service provider.

Broker - An orchestration service that processes requests from RP’s and Citizens and routes them to the correct service element within the model e.g. Registration and Authentication requests routed to the Authenticator and Credential Provider. Attribute Requests sent to the Attribute Services.

Authenticator / Credential Providers - A service that can create and subsequently authenticate a citizen into the service, using a combination of different credentials and authentication mechanisms including issuance of single sign-on tokens and multi-factor authentication. The credential provider has no reason to acquire personal data as it only needs a handle to the citizen (e.g. email) and a means of securely reissuing compromised or lost authenticator credentials. Citizens can become confused if data is being gathered in multiple places as has been shown during user research. If a credential provider stored personal data e.g. name would increase the complexity of the privacy and protection models.

IMO it should not gather details such as names etc. These confuse the user (as UR has now shown) and increase the complexity of the privacy and protection models.

Attribute Services - This is a collection of attribute sources that the broker may connect with, and access attributes from, with the consent of the citizen. This will seek to present to the citizen a uniform consent and approval process for citizens to grant access to relying parties on a one time or persistent basis or for a defined set of use cases. The Attribute Services as the locus of consent was only an artefact of the prototype. This actually belongs in the Attribute Store. The Mydex CIC own consent manager is being developed to support the consent management dashboard requirement as an intrinsic part of their PDS offer.

The objective is to ensure informed consent is given and the specific use cases for access to and provision of attributes are understood and can be reviewed over time and adjusted as required with minimal effort for citizens. Maintenance of an audit trail of such attribute access requests and approval which will be an integral element of the attribute services. Critical to the concept is citizen control over granting access.

Citizen Attribute Store - A secure storage environment and infrastructure under the control of the citizen in which they can store verified attributes provided by service providers and attribute issuers e.g. Scottish Government, Local Authorities, NHS, Third Sector organisations. In addition, the personal data store can keep records of information such as preferences, intentions, profiles and records of interactions and transactions. These attributes remain verified through the use of cryptographic means and persistent or maintained connection to attribute providers. This means any changes to their status could be manually or automatically updated in the personal data store.

Attribute providers (who may also be Relying Parties) - Relying parties acting as service providers to citizens also generate verified attributes as a by-product of their relationship and interaction with citizens. Whilst they consume attributes as part of delivering their services they can also generate attributes as part of their relationship with citizens. These newly created attributes can play an important role in enabling citizens to access and use other services. RPs acting as an attribute provider can offer this service in a number of ways including

- Depositing and maintaining verified attributes with the citizen using a personal data store
- Enabling citizens to generate their own verified attributes and tokens relating to verified attributes originated in a public service or derived from it. Citizens could publish on some form of ledger or deposit within their personal data store
- Enabling access directly from their own systems subject to the citizen giving informed consent from within their own domain and environment using their specific credentials for a given service.

Appendix B: User Research summary

During the ten-week proof of concept between January and April 2020 we evaluated a series of prototypes to explore young people's responses to a Scottish Government credential, and an Attribute Store.

The twelve participants identified a series of design issues, which fed into the iteration of the prototype system. They also discussed the area more generally.

The main outcomes were:

- **Even without any explanation of the Attribute Store from the facilitator, the value is clear to most users**. Recognition of the value is facilitated by short pieces of user-focused text explaining specifics.
- **Security is a central issue,** with some citizens concerned that gathering data into one place will facilitate identity theft, and seeking reassurance that the service is fully secure[1]. Multiple stages of security, a trusted organisation and professional-looking interfaces all contribute towards users' perception of security level. It is important to have security information available upfront so that those who are interested can inform themselves before making a decision about whether or not to establish an Attribute Store.
- **The current prototypes do not make it clear to users who can view data stored in the Attribute Store**, or what level of detail can be viewed. Exploring ways to communicate these issues will increase understanding of the Attribute Store and is likely to increase user trust in the system.
- **The principle of user control of their own store and its data is not yet communicated by the prototypes**; most users equate 'control' of their data with the ability to access the store when it suits them, choose what is in the store and when it is edited.
- **For many of this user group, the concept of "verified" information was not easy or obvious**; this may be an outcome of life stage and inexperience, but in addition, the prototypes

[1] Secure by design, providing reliable, habitually reviewed defensive techniques using real world 24 x 7 risk management - countering threat sources in real time.

did not effectively communicate the idea of information verification. The final prototype more effectively communicated the idea, but who verified the information was still not clear to users.

- **Users may not regard data about themselves as neutral**. Some data, e.g. the change in someone's disability, could either trigger increased benefits payments for a struggling family, or lead to a significant reduction in family income which, if it happens without warning or appropriate time for preparation, could have an extremely detrimental effect. While from a technical perspective, the responsibility in cases like these would be of the relying party, a lack of confidence and control around these issues may lead some users – those who could ultimately benefit most – to reject the service.
- **In terms of the prototypes, more valuable data could have been elicited if the prototypes had been more complete**. Many user comments focused on mis-spellings, unexplained acronyms, inappropriate fields in forms, and confusing content. It is recommended that for future research, time is built in for the review and iteration of prototype screens before they are shared with participants. It is also recommended that, if possible, content design is part of the future design process.

Appendix C: Credential provider desk research summary

During early-mid February, a desk research paper was produced to set out existing research and trends on citizen attitudes towards different credential options. The intention was to provide background information and context for developing and user testing credential options (user authentication for sign-up and sign-in) within the DIS attribute prototype.

DIS requires a credential to meet GPG 44 'medium protection' which requires 2-factor authentication through a combination of two secrets of something the user knows, has or is - passwords, tokens or biometrics rated as low or medium quality. Credentials used in the prototype should therefore also meet this standard, in order to effectively inform future service development. GPG44 lays guidance for secure credentials against multiple criteria, of which 2/multiple factor is only one, e.g. monitoring of credential use. It also requires a standard to be deployed in the context of the deployment to ensure all parties comply with the specific requirements of the ecosystem. The DIS programme will need to address this in the next phase.

Authentication methods for development and user testing in the prototype were reviewed in some detail in this paper and recommendations made:

Passwords (high priority) - despite being insecure and difficult to manage, passwords are still the most common authentication method and are seen as straightforward. Users are very familiar with them, often expecting passwords to be part of security processes

Passwords securely created and stored in password managers (medium priority) are increasing in popularity, though take-up is still reasonably low

PINs (low priority) - similar to passwords

One-time-passcodes issued by SMS (high priority) - widely deployed as a second factor so understood by users. These are also automatically generated by the service so are more secure

One-time passcodes issued by mobile push (high priority) - similar to SMS one time passwords but due to additional reliability and security, this is the direction of travel for the market. However, deployment is currently less common than SMS because users have to download an app (and have access to a smartphone)

Biometrics - fingerprint recognition (high priority) - use has increased exponentially as smartphones' in-built technology have become ubiquitous. Most users are very familiar with this method, particularly for financial services, and they recognise the security benefits. Biometrics are convenient for users and are inextricably linked to an individual.

Biometrics - facial recognition (medium priority) - further development from fingerprint recognition available to users with more recent smartphone models

Some authentication methods were discounted from the prototype work:

Hardware tokens (other than phone-as-a-token) as the issuance of hardware is impractical in the prototype timescales. Their higher cost and their use has been steadily declining so they are highly unlikely to form part of a future solution. Smartcards may be perceived as similar to ID cards, for example.

Bring your own identity (BYOD) in the form of social media or google logins. These approaches generate user concerns that have been raised in previous DIS user research around trust.

Knowledge-based verification (KBV) questions These have a high failure rate as users often do not know the exact answer. They are highly unpopular. They often involve financial information which can raise suspicion with users when the service is not their own bank. The efficacy of this method was severely limited after the extensive 2017 Equifax data breach.

Less mature options such as **decentralised identity solutions, passwordless solutions** and **continuous authentication**.

Appendix D: User experience report summary

A review of the user experience was undertaken along with the creation of a set of interactive wireframes developed within Axure and conforming the the GDS / Scottish Government Guidelines. They fulfilled two purposes one being to enable citizens participating in the user research to be led to the start of the research being undertaken and to test their experience and understanding of the steps in the journey.

A heuristic evaluation was undertaken which involved examining an interface and comparing its compliance against recognised usability principles. A series of recommendations and observations were made to be taken into consideration in any future work. The summary of suggested next steps were:-

- Iterating prototype based on citizen research and testing
- Clarifying what data is essential to be collected from the citizen and reflecting this in the prototype. Any work on this will be to convey the concept to the citizens
- Visually showing what fields are required/not required using (*)
- Include error prevention
- Enabling citizen to review the data they have input before submission
- Content iterations to ensure language used is appropriate for citizens,reliant on relying parties. Any work on this will be to convey the concept to the citizens
- Additional content - clarifying why information is collected and how it is used (ie email address)
- Focus on accessibility and what can be achieved
- Create alternative journey to test different demographic of users (NEC)
- Create an attribute store