Smart Entitlements: Recommendations and Report for the Scottish Government

July 2020

Mydex CIC Partner

DIGITAL HEALTH & CARE INSTITUTE

A research report commissioned by the Scottish Government

Table of Contents

Executive summary

In a nutshell

1) Scotland has the opportunity to radically reduce the costs of providing public services while improving their quality and citizens' experience of accessing and using them, in a way which directly promotes Scottish Government goals of an innovative inclusive wellbeing economy
2) It can do this by better uses of personal data outlined below. There are no substantial technical, operational or legal obstacles stopping Scottish Government from being able to implement these proposals with immediate effect, and it can do it using its own existing resources and capabilities without large scale disruption or risk
3) This report makes a series of recommendations relating to a Smart Entitlement Strategy for Scotland and explains how they can be achieved

Findings

The ways public and third sectors are currently delivered are highly wasteful for both service providers and users, in terms of time, money and energy. *Examples are: ongoing reliance on paper based processes that could be digitised; on manual processes that could be automated, and widespread and unnecessary duplication and re-working of these processes.* This is not the fault of anyone in particular, especially not front line workers whose dedication in the face of often extremely difficult circumstances delivers minor miracles daily. It is because advances in digital technologies mean that, in terms of structure and process, current approaches are no longer fit for purpose.

The 'Smart Entitlement Strategy' proposed in this report identifies a simple way forward that can improve service quality while radically reducing friction, effort, risk and cost for both service providers and citizens.

It does this by creating systems for known, checked information about citizens ('verified attributes) to be shared, used and re-used by public and third sector users, under the citizen's control and in ways that protect citizens' data and privacy, to eliminate duplication of effort, reduce errors and fraud and minimise delays. In doing so it makes accessing public and third sector services much easier for citizens and much cheaper for service providers, to bring on new citizens to a service, and manage the ongoing

service delivery.

The proposed Strategy is doable now in Scotland at very low cost, using systems and assets that have already been built, in ways that do not require large scale and risky changes for existing systems. A Road Map to achieving these goals, using existing technologies and current capabilities, has been identified and is detailed in the Recommendations.

If implemented, in a post-Covid world the Strategy would:

- quickly reduce pressure on the public purse
- target those most in need of support, e.g. the heaviest users of public services
- practically promote the goals of the National Performance Framework and Scottish Government's inclusive growth and wellbeing agenda
- build robust digital capabilities and infrastructure whose resilience and adaptability will help Scottish Government deal with future crises
- provide a practical means of maintaining the momentum for improvement triggered by the pandemic and enable faster economic recovery, to move Scotland forward in a better and more effective manner.
- provide a platform for ongoing digital innovation that will underpin future inclusive economic growth. As explained below and in Appendix G, the infrastructure and processes proposed in this report could have significance for Scotland's digital economy as far-reaching as those that the introduction of the mass production moving assembly had for the industrial age.

The following are the key points of the report.

The current state

For the reasons outlined above, current ways of delivering public and third sector services are extremely cumbersome, costly and inefficient, often resulting in poor experiences for service users including delayed access to the services they need. Again, this is not the fault of the people working in these organisations, who often go to the ends of the earth to provide the best service they can. The underlying reasons are structural and process related.

- **Structural** Current ways of collecting and using the data needed for service provision rely on a large number of separate organisations and systems, each

working in isolation. Across the system as a whole this creates endemic duplication of effort, as each different organisation undertakes its own, separate data collection, checking, storage, and curation processes.

- **Process** Because there are no comprehensive, standardised systems in place to verify the veracity of data that citizens present about themselves when applying for services, many processes are still paper-based, requiring the physical presentation and checking of paper documents for example. If they are not paper-based they are still usually manual. Citizens have to fill in forms manually and the data they enter has to be checked manually.

As a result:

- a high proportion of service providers' costs are effectively wasted in manual checking and data processing activities
- citizens experience ongoing frustration as they find themselves having to present the same information many times over to different (or sometimes the same) service providers in ways that are time-consuming and often costly (in terms of both time and travel)
- Accessing public services and support needed can take much longer than it needs to.

The Smart Entitlements Concept

The 'Smart Entitlement' Concept tackles these structural and processes issues at source. Under the proposed system service providers a) mint secure electronic tokens [1] that verify facts about citizens (such as proofs of address, age, disability or educational qualification), b) provide these tokens to citizens to be held safely in the citizen's own attribute/personal data store, so that c) citizens can share these tokens with other service providers, under their control, as and when they are needed.

Our key finding is that this is doable, at low cost and risk, ***now***, by Scottish Government, using what already exists, without having to ask permission from or being

[1] 'Mint' refers to the act of generating a cryptographically protected electronic token that contains a verified attributed and associated metadata about its provenance and structure in such form as to carry its trust and trustworthiness with it. Smart Entitlements are a form of verified attributes

dependent on anyone else.

Already established initiatives such as the National Entitlement Card (NEC) are already verifying key attributes about target citizens. It is easy and cheap for them to mint secure electronic tokens verifying attributes without interfering with any of their core operations. The necessary infrastructure for safe citizen attribute stores already exists (created by a Scottish Community Interest Company, Mydex), and a Scottish Government prototype-building exercise has already demonstrated the technical feasibility of safe, efficient attribute sharing.

Scottish Government can require a small number of attribute providers such as NEC to supply the attributes they already use. These attributes will cover a high proportion of the data points that citizens need to apply for services, and that services need to process applications, assess entitlements and deliver services. Once made available (and kept up-to-date and accurate via persistent secure delivery links using APIs [2]) these attributes would remain 'on tap' ready to be used again and again, as necessary, at virtually zero incremental cost, thereby eliminating swathes of duplicated effort and cost from the system for both service providers and citizens.

Once the Scottish Attribute Provider Services is pump-primed with access to the core attributes from core attribute providers, it can be incrementally extended (again, at low cost and low risk) to cover all public services, expanding the range of service provision it supports. The number and range of citizen attribute stores, and the services they provide, can also be extended incrementally.

Benefits

The Report identifies many potential benefits of the new system for citizens, service providers and Scottish Government. They main benefits are:

Citizens would benefit from such a system by the ability to reduce the time, effort and money they currently have to spend finding the information they need to access services, filling in forms and proving bits of information about themselves (often physically and manually, in person).

[2] API - Refers to application programme interfaces that can enable secure communication and exchange between different systems across the internet.

These benefits would have an emotional as well as a practical dimension. Many citizens find current processes frustrating, stressful and humiliating, often breeding a sense of helplessness. Having the information they need at their fingertips and being able to use this information without having to jump through multiple hoops will provide them with a sense of agency and empowerment, building personal confidence and wellbeing while reassuring them that their needs are being understood and met, thus increasing their satisfaction with public services.

The proposed Smart Entitlement Strategy also helps ensure that those most needing access to public services get it without unnecessary barriers, thus promoting inclusivity and reducing the 'poverty premium'. In this way, it is one practical means of implementing many of the goals of the National Performance Framework and of an inclusive wellbeing economy.

Finally, the proposed Smart Entitlement Strategy can improve citizen resilience: providing citizens with the resources and capabilities they need to address new and different needs as they arise, whether they are completely new challenges (such as Covid 19) or the inevitable multiple changes in their circumstances that will unfold as they go through their lives. From a social/economic point of view this last user need is perhaps one of the most important. It is also perhaps the most overlooked, because it is an absence - a 'dog that is not barking' - rather than a present, felt, irritation.

Service providers would benefit from being able to collect the information they need quickly and at low cost, without having to devote large amounts of staff time and effort to checking claims that are being made and manually processing information. The resulting reduced operating costs can be used to serve more citizens using the same resources and to focus available resources on other priorities. Fraud rates would be reduced along with cyber-security and regulatory compliance risks.

Scottish Government would benefit from a reduction of pressure on the public purse plus the establishment of digital infrastructure that is highly configurable at low cost, enabling it to introduce and implement new services and programmes quickly, cheaply and easily (including the addition of new verified attributes such as 'tested for Covid 19'). Over time, as each citizen collects their own, unique store of verified attributes, the system would create rich new data assets for Scotland plus a safe, trusted, secure and efficient data sharing infrastructure - creating a platform for ongoing innovation and inclusive growth (with potential to extend its operation to private sector service

providers).

One additional byproduct of this system would be to help public sector service providers with identity assurance, because many of the most commonly used verified attributes contribute towards confirming an individual's identity. The more such verified attributes are collected and shared, the more confident service providers can be of the individual's identity. Helping to crack the problem of identity assurance is one positive *byproduct* of the proposed Smart Entitlement Strategy - delivered at close to zero incremental cost and thereby reducing dependency on third party commercial services with all the attending cost, and constraints on reuse of proofs provided.

More detailed findings

Landscape review

To inform our recommendations we reviewed initiatives that are already under way in Scotland, the UK and the rest of the world including Canada, Estonia, India, Korea, New Zealand, Sierra Leone, Spain and the United States. Key findings from this review are that the need for improved trustworthy, privacy protecting data sharing is now widely recognised across the world. There are a wide range of initiatives focusing on particular issues such as identity assurance, on particular industry sectors such as financial services, and based on particular technologies such as blockchain.

Much can be learned from these experiences, but they also demonstrate some deficiencies and risks. For example, addressing the problem of identity assurance in isolation leaves broader issues relating to data sharing for the purposes of service access and delivery untouched. Industry specific solutions risk creating new silos resulting in additional duplication of cost and effort and usability constraints. Specific technology-focused solutions risk creating new dependencies and limitations. We have taken both identified opportunities and risks into account in crafting our recommendations.

Specific implementation requirements

Any Smart Entitlement system introduced by Scottish Government should be:

- Open source, based on open standards where available or open specification if not. The core design requirement is the development and deployment of

reusable building blocks
- Technology agnostic
- Designed for interoperability
- Minimise the need for internal systems changes to focus on the development of new layers of infrastructure and 'plug-in' tools and capabilities
- An agreed definition/structure for the portability of verified attributes, metadata formats, data directories, and basis of provision of citizen attribute stores

Risks and barriers

The biggest potential barrier to the success of this programme is potential reluctance of organisations who hold attributes of importance to improving public services making the verified attributes available. This is a collective action problem: it may not be in the (perceived) interests of each individual public service organisation to incur costs providing information that helps other public service organisations reduce their costs, improve efficiency and equality of access, but if *all* organisations did it *all* of them could gain benefits, along with the citizens they serve.

This potential logjam needs to be broken by decisive Scottish Government leadership and actions as discussed in the report.

There are multiple technical/operational risks in implementation including:

- Poor service design making citizen journeys difficult
- Poor communications failing to explain why the programme is being implemented or what its benefits are
- Cumbersome/poorly explained consent processes which raise question marks about compliance with GDPR
- Lack of resources / poor implementation of metadata standards and data directories
- Poor implementation of APIs links and other technical processes to ensure security and efficiency

All of these risks can be avoided by a) adequate investment in expertise and resources and b) ongoing disciplined focus on operational excellence.

Broader strategic considerations emerging from the project

It is recommended that Scottish Government view the proposed Smart Entitlement

Strategy at three levels.

1. Potential to provide an immediate solution to an immediate problem, creating infrastructure and processes that address the costs and frustrations experienced by both citizens and public/third sector service providers in providing/obtaining the information needed for service provision
2. Leveraging this infrastructure and processes to ensure ongoing incremental extension and enrichment (e.g. the provision of more verified attributes) that simultaneously delivers increasing benefits and builds further capabilities and momentum
3. Using the resulting infrastructure and processes - the creation of rich new citizen data assets and safe, low-cost information sharing capabilities - as the foundation for further, far-reaching economic transformation: to spread order-of-magnitude reductions in the costs of service provision, to place the benefits of fruits of the digital revolution into the hands of Scotland's citizens, to ensure universal inclusive access to services and to act as a platform for ongoing digital service innovation

Definitions and Scope

In this section we identify and define the key terms in this report.

What is a 'smart entitlement'?

A citizen's ability to electronically present verified attributes about themselves to service providers needing to verify these attributes, in a way that is reliable, safe, easy and efficient for both parties. [Working definition to be refined.]

Design principles implied by this formulation are:

- That the citizen is 'self-sovereign' in the transaction. The citizen is the party holding and presenting the verified attributes, which in turn implies that these verified attributes have already been shared with the citizen.
- That it is privacy protecting: the minimum amount of information is shared at all times (e.g. proof of age does not require date of birth), and relying parties using this information are not building up new, centralised banks of data about this individual

- Smart entitlements are not the same as 'self sovereign identity' because it is bigger and broader than identity. Identity is just one of the ways that these verified attributes can be used; it is just one use case of smart entitlements.
- It is thus focused on enabling and supporting multiple, different types of process (applications, entitlements, identity assurance)

Citizen 'control'

While most people agree that citizens should be able to control their own data, much confusion is generated by different assumptions/understandings about what this means and looks like. Here are some of the different meanings of control. Control means:

- Citizens should have to tick a consent box before a service provider can use their data
- Citizens should understand what data is being collected about them and how it is being used before consenting to such collection and use
- Citizens should have greater degrees of granularity in controlling what data controllers do with their data. For example, they should be able to pick and choose between different uses of their data and to withdraw consent for the use of their data
- Citizens should be able to specify general rules which they expect all data controllers to abide with, without having to read, inwardly digest, understanding and signal 'consent' to specific terms and conditions provided to them by a variety of different data controllers
- Citizens should be provided with the means to assert the above definitions of control from one central place (e.g. a consent management dashboard) rather than having to log in to and navigate the systems of each different data controller
- Citizens should be able to ask that data held by one data controller be transferred to another data controller
- Citizens should be able to hold data about themselves independently of any and all data controllers, and be able to use this data for their own purposes. This includes choosing who they share their data with, and being able to assert their rights under GDPR.

The first five variants of 'control' relate to citizens having a degree of control over what data controllers do with their data. The last variant of data control is qualitatively different: it relates to citizens directly 'doing stuff' with their data independently of any

particular data controller.

Consent

The definition of consent in legal terms as defined by General Data Protection Regulations in Article 4(11) as:

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

There is a lot of confusion about consent, the nature and approach to achieving it or even if it is required at all.

In many service situations today, consent has become a cognitive and administrative burden on both service users and service providers (see Appendix E). Context is an important consideration in how consent is sought and how citizens can exercise control in a safe and secure manner that empowers them.

We have identified three broad approaches to consent:

- **Dynamic consent** - The means to integrate consent authorisation into any online process at any stage required to approve access, collection or storage of personal data for one or more defined purposes.
- **Static consent** - The ability to join some form of scheme or service that involves the collection of and distribution of personal data to multiple service providers responsible for delivery of a service to a citizen. There is a well defined data sharing agreement with defined limits on scope of use.
- **Citizen preference driven consent** - The ability of a citizen to set a range of preferences or policies about how and where their personal data can be used for what purpose in order to streamline and automate processes. These could be broad categories e.g. to keep me safe and well, to get financial advice, to secure access to state benefits and it could also expressly exclude things like secondary use or onward data sharing and place limits on time data can be used for or retained. It can also offer the ability for data to be used for societal benefits such as research of one form or another against topics and subjects that the citizen may care about.

For the purposes of this Smart Entitlement Strategy, when we talk about consent we mean a Scottish Government policy goal, not a specific mechanism.

The purpose of consent in the proposed Strategy is to make it as quick, easy, safe and simple as possible for citizens to exercise genuine control (as defined above) over how their data is to be used.

This is as much of a design challenge as it is a legal or compliance challenge and may require process innovation. Consent could take many forms, consent applied at every step in a transaction (dynamic consent), once in a transaction or once in the context of a service provision (static consent). It could be something that is given when first joining a scheme or it could be driven by some form of citizen controlled policy and preference.

For example, might it be possible to establish mechanisms by which citizens can establish their own 'consent policy' which establishes general criteria by which they will automatically consent to access of their data? In essence, such a policy might say 'You can access my data if I have requested a service, and the service accesses only the data it needs to provide this service, will not use this data for any other purposes or share it with any other parties'. Services that agree to such a policy could signal formal agreement to this, gaining access to the data they need without having to go through a separate consenting process. Bespoke consent processes could then be used for other, more detailed or exceptional cases, becoming the exception rather than the rule. For more information on GDPR and Verified Attributes please see Appendix D. For more discussion of issues related to consent please see Appendix E.

Verified Attribute

A verified attribute is any piece of information about a person or performance that has been generated or checked by a responsible trustworthy body and made available to another party in such a manner as to be trustable as a specific attribute.

Metadata

Metadata is data about a piece of data (e.g. verified attribute), describing what that data contains how it was collected, created, protected, maintained and updated and what its status is (e.g. the degree to which other parties can trust this data to be accurate and up to date).

To be useful in an ecosystem based on the sharing of verified attributes, such metadata needs to be standardised as far as possible using easy-to-understand definitions that are unambiguous and precisely targeted to the context of the transactions they are used in. Such metadata must be machine readable.

Directories

In the context of this project a directory is a list of types of attributes (e.g. driving licence, proof of entitlement, proof of address) that are available and where they are available from - their sources. Directories do not hold the data points themselves. They hold metadata about the data - information relating to the nature and type of data that is available - plus routing information that makes it easy for those wanting to access verified attributes to find and access them.

A directory is not an inventory of personal data about a citizen. An inventory is a personal list made available to the citizen when authenticated, advising them about what data they hold about them. Inventories will also support GDPR implementation in relation to transparency and data portability. Data inventories are important for the future but are not required for this project.

A directory of the personal data held by Scottish Government and where this data is held could be used as a signpost for citizens and service providers wanting to access this data to complete specific applications and other processes.

A personal data store itself can provide an inventory of what it holds subject to giving the relying party consent to interrogate it. This could be used by relying parties to find and access (with the citizen's permission) the information they need to streamline an application process and organise service provision.

Attribute Provider

An attribute provider is an organisation that has generated or verified attributes about individuals and is making this information available to other parties, including the citizens the attributes relate to.

Relying Party

A relying party is an organisation that wishes to access and use a verified attribute e.g. to

reduce the friction, effort, risk and cost of making an application for benefits or services.

Attribute Store

An attribute or personal data store is a citizen-controlled database holding verified attributes, or links to these attributes. The key functions of an attribute store are to help citizens easily and safely access verified attributes from attribute providers, to hold these attributes safely and securely under their own control, and to enable citizens to easily and safely share these attributes with relying parties (or allow relying parties access to them).

In this paper we assume that Attribute Stores display a number of key characteristics including:

- They enable citizens to become the point of integration where data about themselves is aggregated and accumulated under their control independently to any organisation that has collected data about them. Attribute stores 'untether' personal data from data controllers who traditionally collect and use data about persons.
- They operate on a zero-knowledge basis, designed so that the attribute store provider is unable to 'see', 'look into' or control what citizens do with their data.
- They operate to the highest possible levels of security, encrypting all data both at rest and in movement, with independent certification of their security processes within their information security management system to one or more recognised independent standards e.g. ISO27001, FairData, tScheme.
- They provide citizens with the tools they need to easily and safely manage their data, including accessing data from attribute providers, sharing/allowing data access to relying parties, managing consents and permissions, and asserting their rights under GDPR.
- The attribute store provider's business model is so designed that they have no financial or other incentives to invade citizens' privacy or seek to monetise or otherwise abuse citizens' data.
- Their core services are provided free to citizens, in perpetuity.

A Scottish Attribute Provider Service

A Scottish Attribute Provider Service (SAPS) would enable a Scottish Government service

provided for citizens that provides them with the digital tools they need to easily access and use verified attributes held about them by Scottish Public Services. The aim of a Scottish Attribute Provider Service would be two-fold:

- To use and reuse of their verified data, including their identity, when consent is given, and to help citizens reduce the friction, effort, risk and consent they experience when seeking to access and use public services
- To enable Scottish Public Sector services to decrease their cost and risk in digitally delivering public services by reducing error and reducing reverification of data.

Policy Goal

As set out in the ITT the core vision of a Smart Entitlements Strategy is that citizens should be able to quickly, easily and safely demonstrate enhanced or otherwise differentiated entitlements to a service based on multiple verified attributes they can provide at point of use or elsewhere. Public sector organisations should be able to use the attributes citizens provide to create new or integrated products and services and to ensure their delivery by public sector, third sector or private sector service providers, either alone or in cooperation with each other.

The underlying goal of this Strategy is to reduce friction, effort, risk and cost experienced by *both* citizens in applying for and service providers assessing a citizen's specific entitlements and delivering the resulting service. In doing so the Strategy should help reduce the poverty premium, make it as easy as possible for citizens to apply for and get the services they are entitled to, and avoid potential sources of stress and anxiety along the way.

It should accomplish these goals in ways that empower citizens with the use of their own data, building in privacy and data protection as the default setting.

In doing this, the Strategy should directly contribute to the achievement of the National Performance Framework and the Scottish Government goal of creating a more inclusive wellbeing economy.

By reducing the administrative costs of service provision the Strategy should also help reduce pressures on the public purse and free up resources to increase current capacity

and or more fruitful investment elsewhere.

Current state review

There are already a number of initiatives underway that come under the broad heading of 'smart entitlements' in Scotland, the UK and elsewhere around the world. In this section we will undertake a cross-cutting analysis of this 'current state'. By 'cross-cutting' we mean viewing these initiatives from different angles such as types of data used, degree of citizen control over their data, intended benefits, technologies used, processes relied upon, stakeholders involved.

Summary

The idea that individuals should be able to share verified information about themselves under their own control is gaining momentum. This general trend embraces a number of emerging themes including:

- **The benefits of data portability.** There is increasing recognition around the world that data originally collected and stored by a single data controller may have other uses/benefits that cannot be realised as long as that data remains within the firewalls of that particular data controller.

  Currently, most initiatives in this area (in finance and health particularly) focus on data sharing between organisations, not data sharing between organisations and individual's for subsequent onward use with other organisations. Examples include the UK's Open Banking initiative and the Indian Government's 'Account Aggregator' scheme.

- **Solution focus** e.g. digital identity. There is growing recognition of the value of verified attributes in creating and assuring digital identities. For example, the long-standing Open Identity Exchange is now presenting its workstreams under the banner headline of Identity and Attribute Exchange aligning with current UK Government programme of the same name. There is a proliferating array of initiatives focused on the use of attributes for digital identity purposes, but not recognising broader potential uses of verified attributes.

- **Technology solution**. Many of these proposed ways forward are based on the

use of a particular technology such as distributed ledgers.

As such, these initiatives may not address all the needs of a Smart Entitlements Strategy in Scotland, but they may illustrate aspects of what such a Strategy needs to address.

We analysed initiatives in Scotland, the UK and globally which are already using verified attributes to a significant degree and whose approach and experience highlights opportunities for further development.

Business and operating models

The key insight from our research is that 'market' assumptions do not apply and are not helpful to the development of an efficient, effective Smart Entitlement Strategy. This Strategy is not about creating discrete 'products' that profit-seeking actors seek to sell at the highest possible margin, including finding ways to 'monetise' citizen data. It is about creating a state and mission-led mutually beneficial data-sharing ecosystem that generates powerful economic and social win-wins. Scotland can do this by stripping costs out of the workings of the system as a whole, by developing common processes and infrastructure that build capabilities and possibilities across public services as a whole (and, potentially, beyond) and thereby reducing dependency on commercial services that increase costs to public services.

The specific business models that apply need to be tried and tested but are likely to differ according to actor/role.

The core of the Strategy assumes Scottish Government funding of the necessary initiatives (e.g. developing metadata standards, data directories, and the Scottish Attribute Provider Service itself and critically a shared service broker/hub), but this funding is paid for quickly by the resulting cost reductions in public service provision. A policy decision to use only open source components avoids risks of dependency on proprietary technologies which are not needed in this instance.

Cost impacts for attribute providers will vary. While some may incur some extra costs, most already incur expenses providing citizens with copies of information via manual and paper based processes. Digitising these processes will actually be a cost saving for them and provide a more efficient mechanism for meeting GDPR obligations under data portability, transparency and subject matter access requests..

The biggest beneficiaries are relying parties and citizens who can now access reliable information at much lower cost.

Citizen Attribute Stores' costs need to be covered and their business models may vary within limits (see 'Criteria for recognition/inclusion of attribute stores' below). Some, like Mydex CIC, will operate on the basis of subscription fees charged to service providers per citizen. Others may want to charge fees per transaction.

Credential providers (entities providing registration and authentication services) that could be compliant with any Scottish Government Attribute Provider scheme ((as distinct from the public sector attribute providers) offer a range of commercial models including, per transaction, per user over different time periods and specific negotiated models.

Given the conceptual architecture of the Scottish Attribute Provider Service is it not envisaged the public sector relying parties or attribute providers would be charged for use of the scheme on a collective action and benefit basis.

Overview of existing examples

The role verified attributes can play in helping service providers deliver better services more efficiently and effectively is being widely recognised internationally.

The examples identified illustrate the potential of systems designed to share verified attributes safely and efficiently at scale. For such systems to deliver their potential they must provide reliable, trustworthy information about identified individuals that can be accessed quickly, cheaply, securely in ways that protect individuals' privacy and comply with data protection regulations.

The benefits of such systems would be experienced by both service providers and individuals using these services. Service providers mainly experience reduced costs and reduced risk. Individuals experience improved convenience: accessing and using the service involves less effort and stress and the end result is faster, more efficient and effective outcomes

Common features of these initiatives (mostly) include a recognition that:

- Data - verified attributes (sometimes referred to as tokens or credentials) - currently held 'under lock and key' by the organisations that collected/generated

this data has value if used for other purposes by other parties
- Individuals should be able to control the sharing of this data
- There are multiple potential benefits including improved efficiencies, risk reduction, privacy protection and service/business model innovation
- Primary focus is on reducing costs and risks of existing processes

They also differ in many ways, by:

- Target use cases (e.g. identity assurance, access to information needed to decide entitlements/service configuration)
- Target industries (currently, the biggest focus is on financial services), closed systems
- Target users ('all citizens', the unbanked)
- Technologies used
- Primary actor (government/private sector)
- Sector (private/public)
- Method of data sharing (see below)
- Lack of meta data or portability of trust with data
- General lack of citizen involvement beyond consent, no agency to collect, store, and reuse verified attributes under their own control

For the purposes of a Smart Entitlement Strategy we have given careful consideration of the options illustrated, to focus on those which provide the greatest opportunities at least risk for public service providers in Scotland.

Pros and cons of current state

In formulating our proposals we have been encouraged by the growing interest in and momentum towards both increased data portability and increased citizen control over their data. But we have also identified a number of risks, pitfalls and shortcomings which our proposals are designed to avoid.

The main identified potential drawbacks are as follows:

- Most initiatives so far are 'point solutions':
    - they focus on solving only one particular problem and do not concern themselves with opportunities or issues that may arise beyond this

problem. For example many of them on focus on 'identity' while ignoring potential uses of the same data for other purposes
    - they are bespoke: arranged between particular parties using particular mechanisms/arrangements and are not designed to be generalised.
- Most are focused on enabling data sharing between organisations, leaving individuals out of the loop except for the provision of consent. Very few focus on directly empowering individuals with their own data.
- Most operate bilaterally e.g. Organisation A sharing some of the information it has collected with Organisation B (e.g. Open Banking, Data Transfer Project). While these approaches can work for bespoke point solutions, they risk creating complexity catastrophes where costs spiral upwards as they scale.
- Most are industry specific e.g. 'financial services', 'health', or 'social media' and are not designed for cross-sector service provision.
- As yet, many do not have clear business models that would ensure their sustainability. Very few have a clear operational or benefits focus. Rather their focus is often on more on abstract policy goals.
- Many rely on the deployment of a particular technology such as blockchain and, as a result, are constrained by what these particular technologies can and cannot do.
- Many create consent management issues which can become barriers to take up and use, are open to systemic gaming, and are costly to implement for both service providers and users.

Types of attribute currently in use

A successful Smart Entitlement Strategy will need to have robust means of identifying and handling different types of attributes. For example, some attributes like blood type or DNA sequence are permanent and unchanging. Other attributes, such as home address, marital, or employment status may change relatively infrequently, while others such as the balances in an individual's bank accounts might be changing on an hourly or daily basis.

The utility of a piece of data depends on the purposes for which it is being used. Date of birth is an unchanging data point. Current age is always changing. The fact that an individual who was under 18 yesterday is now 18 is a potentially significant *state change* that may be critical to the completion of a transaction or open up rights to new services or indeed close off entitlements. Likewise, the fact that yesterday an individual had a

valid driving license but it is no longer valid today is an important change that could change services and entitlements.

For this reason, a key requirement of any new infrastructure/systems is a) the ability to time and date stamp the attribute in question and b) the ability to regularly or instantly and automatically update its status (depending on the attribute in question) or show that the status is not maintained and provide the last date at which it was updated. Without this form of meta data risk cannot be assessed and decisions cannot readily be made (without external verification taking us back to the central issue of manually completed forms and processes).

Clarity over exactly what the nature of the data that is required is also essential, especially as it relates to level of detail.

Take the example of a bank account. Bank accounts generate huge volumes of detailed operational data such as the current bank balance at any particular point in time, and data relating to each transaction such as how much was spent, where (which retailer, retail identification number etc), on what, at what time, using what payment method, via which payment system, what the transaction approval number is etc.

A wide range of analytical data points may be derived from this data, for example, the pattern of bank balances over the course of a month, average bank balance over a particular time period, whether the person ever goes overdrawn and if so how often and by how much, average monthly spend, average monthly spend on different categories e.g food, travel, mortgage payments, savings etc. Critically it can also speak to evidence of an individual's economic activity in person and online, demonstrating physical existence at a location or venue. These types of proofs can be important in demonstrating specific facts to support activities such as proof of identity as well as proof of income and expenditure. They are important in debt advice services, financial advice and planning, and assessment for benefits and entitlements

The bank account will also have a tranche of administrative data connected to it, including bank account details (name of account holder, bank name and address details, account number, sort code, IBAN number, SWIFT code) etc.

All of these different categories and types of data require robust, detailed metadata that captures complete and accurate descriptions of what the data is, what formats/software used, what its provenance is, etc.

For the Scottish Government Attribute Service and Smart Entitlement Strategy, identifying the core / anchor verified attributes under Scottish Government and Scottish Public Service control that are of the most value in the short term to pump prime the service is an important consideration. The scheme can be extended overtime with more attributes.

Initiatives in Scotland

A range of initiatives in Scotland are already processing and sharing verified attributes to a certain degree.

The National Entitlement Card

is a national smart card based scheme designed to make it convenient for citizens to access a range of different public services and facilities. Using only one card citizens can access free/discounted/concessionary travel on public transport, access to libraries and leisure centres, to prove age and therefore entitlements to discounts (e.g Young Scot), to get discounts on entry to cultural events, access health reward initiatives (e.g. for giving up smoking), as a cashless payment method for some some services, and for other purposes such as acting as a staff identity card or to control access to buildings.

To support this scheme, which is administered separately in each locality by different Local Authorities, a certain set of core attributes is already being collected:

- proof of person: birth certificate, current passport, photo driving licence, PASS hologrammed card
- proof of residence: Home Utility Bill (e.g. Gas, Electricity, Landline Telephone), Council Tax Bill (current financial year), Council / Housing Association Rent Book / Statement / Letter, Bank or Mortgage Statement, Credit Card Statement, Television Licence, HMRC Letter, DWP Letter / Disability Entitlement Letter, Occupational Pension Letter, Letter from Care or Residential Home, Letter from Local Authority confirming that you are resident within the council area
- proof of photograph: current passport, photo driving licence, PASS hologrammed card

While the NEC is currently smart card based, work is underway to extend it to smart phones.

Our Assessment of the NEC is that it provides a powerful proof point of many of the potential benefits and advances of a Smart Entitlement strategy, particularly in the potential of 'make once, use many ways portable attributes'. The NEC:

- embraces the principle of using the same core sets of data for multiple purposes
- embraces the principle of local authorities providing information pre-verified by them so that this information can be used for other purposes (e.g. the data file application extracts personal details from an existing Local authority system)
- means that Local Authorities have already collected a wide range of additional information about citizens, some or all of which could be re-used as part of a national Smart Entitlements strategy (or where the process of acquiring this data could be used for both NEC and for Smart Entitlements strategy purposes, to avoid doubling up of effort)

Much of the data already generated by the NEC could become powerful contributors to the core data sets required by a Smart Entitlement strategy. The NEC could benefit in turn from the creation of a Smart Entitlement strategy, drawing on verified attributes created by other schemes and bodies to streamline its own operations e.g. data from Transport for Scotland to run concessionary fare schemes.

What the NEC also shows is that it is not necessary or desirable to trap attributes within the requirements or boundaries of separate schemes (that creating an underlying Scotland wide systemic data sharing infrastructure is much more powerful and efficient), and that duplication of effort in the minting and use of attributes needs to be reduced as far as possible.

The Scottish Government's myaccount

The myaccount service is designed to enable citizens to use the same username and passwords to access multiple different services. Currently 31 services and 984,001 citizens (at the time of writing) are using the service. A number of local authorities have adopted this service and relying parties by using the myaccount to manage registration and authentication of citizens to their services.

The myaccount services can have up to 24 data points stored in the underlying profile. Relying parties (e.g. local government services) select which of these data points are to be used in their services.

Our assessment of the myaccount service is that:

- it is possible to link a myaccount to other records and data such as Council Tax records to start augmenting a myaccount related profile and its currently limited set of 24 data points used to establish the username and password service
- For example, myaccount data could be cross-referenced to NEC data
- There is clear potential to build on myaccount as a supporting element of a Smart Entitlements Strategy - so long as related privacy and data protection issues are addressed (see analysis and recommendations below)

The Improvement Service has set up a data hub to act as an online data matching and cleansing tool for local authorities.

Seen in the context of a Smart Entitlements Strategy, this data hub could take on a new role in minting attributes. The data hub could also be used as a means to populate citizens' personal data stores.

The Scottish Qualifications Authority

Offers to provide exam candidates with replacement certificates of exams they have passed. It also offers an authentication service for companies and educational organisations who wish to confirm that candidates have gained their qualifications and that the grades and years provided are correct.

The SQA is already providing individuals with verified attributes (copies of their exam certificates), and verifying claims made by individuals about their educational attainments. Currently however, all these processes are manual and paper based. There is clear potential for the SQA to digitise these processes by minting secure electronic tokens that contain the same information. If these tokens were provided to individuals, the administrative burden of the current authentication service could be greatly reduced, if not eliminated.

The SQA could therefore act as an important attribute provider within a Smart Entitlement strategy.

Transport for Scotland

TfS aggregates smart card related data from ticket machines to analyse traffic patterns and monitor demands being placed on the transport system, and to reconcile claims, especially those relating to concessionary fares and has been used to support searches for missing persons and resolving crime investigations.

A new system has been commissioned called TABO and is currently being built. There is reference to data interfaces in scope which could be very useful in the context of smart entitlements and any Scottish Attribute provider service.

Some of the data generated by Transport for Scotland could be re-used for other purposes such as creating evidence that a person is alive and active (which is sometimes needed for ID assurance processes), and to help in the search for missing persons. In a Smart Entitlements ecosystem, Transport for Scotland could have a double role of relying party for verified attributes (e.g. for management of concessionary fare schemes) and as an attribute provider.

Social Security Scotland

Social Security Scotland would be an important source of verified attributes because they are approving citizens' entitlement to benefits both financial and services. They would also benefit greatly from the establishment of a system for the sharing of verified attributes as it would significantly reduce the friction, effort risk and cost of taking citizens through the application process and service providers undertake their own checks and assessments of the information provided.

Social Security Scotland already have access to data held elsewhere using API's but this is a back office process as opposed to anything directly involve the citizen

However, at their current state of development attribute provision is not a key priority, but it could become so in the future. When this happens it will become an important source. Work is underway to envisage how this could work and it would make sense for there to be alignment between this work and any national approach that may arise from the implementation of a Scottish Attribute Provider Service, and the adoption of a consistent approach to defining verified attributes that underpin delivery of smart entitlements.

Passported benefits have existed for nearly a decade in both England and Scotland. 'Passporting' is based on a recognition that if an individual is recognised as being

entitled to a certain benefit, they may also automatically be entitled to other services or benefits. For example, people getting approval for Universal Credit may also be passported to the Healthy Start scheme for pregnant women, free school meals, the help to save scheme and some health costs. Other income related benefits may include legal aid, court exemption fees, free school lunches, free NHS dental treatment, NHS patient travel costs, NHS optical vouchers, individual learning accounts and education maintenance allowance.

Passporting saves citizens the time and effort needed to make themselves aware of what additional benefits they may be able to apply for and going through the process of making these applications. As GDS notes, this makes obtaining their entitlements much easier and "takes away the worry of understanding the different eligibility criteria and the need to provide evidence".

The provision of passported benefits requires the sharing (or checking) of data between DWP and other government departments such as the NHS, Department for Education and HMRC and Social Security Scotland and by Scottish Local Authorities who can make use of online access to DWP Customer Information System via the EAS-R scheme. The Government Digital Service is currently working on a project to streamline and automate the passporting of some benefits in the UK via the creation of APIs linking data from different departments.

The Scottish Government controls a number of disability related and income based passported benefits which people can qualify for if they receive one or more UK welfare benefits. The income related benefits are Legal Aid, Court exemption fees, Free school lunches, Free NHS dental treatment, NHS patient travel costs, NHS optical vouchers, Individual Learning Accounts and Education Maintenance Allowance. The disability related benefits are the Blue Badge scheme, Concessionary bus travel (for working age), Student Loans for Higher Education - exemption from payment.

All of these would benefit from accessing verified attributes including proof of current benefits and entitlements and in turn once granted would themselves also become verified attributes able to presented as smart entitlements

In assessing these systems and approaches we note that currently, all such data sharing/checking happens via intra-government interactions between departments 'without citizen involvement, knowledge or awareness. Reliance on inter-departmental

information flows also creates potential barriers to scaling and diversifying on the principles established by passporting. Service providers are reluctant to provide high degrees of direct access to their systems for reasons of security and performance and because they are nervous about risks and issues relating to consent and liabilities.

The legal basis for data sharing is not consistent, some rely on non-GDPR legislation that gives the government department the right to share. For others it is simply that of a requirement to provide a service. Others may require specific consent during an application process. This can be confusing for service providers and citizens alike. Regardless of the basis on which data is shared it is inconsistent in its approach and still has the obligations of Transparency under GDPR unless a specific defined exemption.

If Government departments provided individuals with secure tokens (verified attributes) verifying information relating to entitlements, many of these privacy and security issues could be avoided and individuals would have data assets that they could use more broadly than is currently possible under current passporting administrative arrangements.

Practically speaking, sharing of tokens with individuals could start small (i.e. focused on a few key pieces of information such as “has approval for Universal Credit”, but the amount and nature of the data thus provided could be extended and augmented over time.

The Electoral Registers in Scotland

There are 15 Electoral registers in Scotland. Whilst the only proof citizens need to vote is an entry on the electoral register there is proof needed to get on the register itself: citizens need to prove that they live at a specific address and you have the right to live in Scotland. To complete this verification process manually is expensive and involves significant evidence in document form as well as home visits and other checks. 10% of citizens cannot complete the process online. The cost to deal with manual registration is significant and presents a significant opportunity to make use of smart entitlements and verified attributes to deliver the proof needed safely and securely online.

It should be noted that these registers are depended on by a range of commercial service providers such as credit reference agencies who in turn sell back to the public sector assessments of people's identity or address. This is done using online API’s that

are paid for on a transaction or subscription basis. Such services could be delivered via a Scottish Attribute Provider Service that would assist in reducing public services' costs in accessing this information.

Another area of opportunity is to manage movement between the registers. Currently there is a simple and secure way for a citizen to move home inside one region or move between regions. Citizens need to start the process of registering to vote all over again, with the attending proofs. There is some significant interest in and opportunities for overcoming this hurdle for the 10% and making it easy for people with disabilities to get on the register and vote, safely and securely.

What also came out loud and clear from citizens consulted, as part of the project looking at how equality of access to vote for people with visual impairment, is that they are frustrated with the endless duplication of effort and in particular the form filling needed to get anything done.

The opportunity for Smart Entitlements would be to reduce the friction, effort, risk and cost of helping citizens get on the register itself which would benefit them by removing friction and effort, the electoral registration offices by removing cost, risk and effort in verifying people applying and for Scotland as a whole by increasing the total size of the electorate able to vote.

Scottish Local Authorities

Local Authorities across Scotland have a long history of collaboration in trying to address collective challenges. They have worked with organisations like the Improvement Service and other funded programmes to share the costs of developing back office applications, standardise on specific applications and make use of shared services such as Scottish Government myaccount and National Entitlement Card.

There is an ongoing integration challenge within and across local authorities in how data they already hold about citizens can be deduplicated and better integrated to create a single view of the citizen in the context of the services they provide to the citizen. Local Authorities are involved in any number of local programmes and initiatives covering health, social care, housing, poverty, debt management, employability, addiction and urban and economic renewal and regeneration.

The need to share data across the local clusters of organisations and between their own

departments and functional areas is a matter of some complexity due to data protection, information governance and a lack of interoperability between systems. Even the same application software is often implemented differently or operating on different release levels.

Local Authorities are intimately involved in citizens' lives. They receive money from them, pay money to them and provide a wide range of services through a citizen's life and across different life stages and events. They are also the gateway for a number of Scottish Government managed benefits and programmes and are able to access citizen information held by DWP relating to their benefits.

Local authorities need a safe and secure way to access verified attributes and proof points about the citizens they serve and they also need to be able to create and share verified attributes internally and externally.

Because of their natural approach to collaboration and shared services they could become a verified attribute provider issuing smart entitlements for citizens with little change to their own back end systems and could very quickly consume verified attributes to help reduce the friction effort, risk and cost in delivering services.

Projects are already underway to demonstrate how this can work using a personal data store to enable citizens to be an active participant in the collection and delivery of verified attributes. These include the Improving Cancer Journey in Glasgow and West Dunbartonshire, the Inclued Platform being delivered to Glasgow City Council as part of the CivTech Challenge programme and a broad spectrum of work by the Digital Health and Care Institute working across the the NHS in Scotland, GP's, Local Government, Third Sector and private sector.

National Records of Scotland

The National Records of Scotland (NRS) holds a valuable range of registers of canonical information about citizens. It runs the Scottish national archive and a range of public registers relating to births, deaths, marriages, divorice, civil partnerships and adoption. They also operate a multi million pound commercial operation that sells services to citizens and partners to gain access to and use of some elements of the registers. Services range from production of copies of certificates, online access to registers and API based services for third parties. The secure APIs are already in place to allow searching and access to the registers.

What NRS do not have in place today is any mechanism to bind a record within a register or census to a real world person via a digital channel. The registers are themselves of a public nature in most parts. Anyone can request a copy of a birth or marriage certificate for example, and many external services such as ancestry services have access online to the registers.

In order for these critical proofs to become verified attributes (of things like birth, marriage, civil partnerships, divorce and adoption) NRS would need to support a trust binding process between a citizen and their own records. This process could be part of any future smart entitlement and Scottish Attribute Provider Service. It would enable a citizen to bind their NRS records on specific registers to their own personal data store (citizens attribute store). In the future this would logically be best done at the earliest opportunity e.g. at birth or as part of an onboarding process for something else like the National Entitlement Card.

Consideration must be given for the current business model in place at NRS which generates significant revenue to offset operating costs. The type of use cases that could be supported as part of Scottish Attribute Provider Service do not appear to conflict with the core revenue streams of NRS.

Rest of the UK

As one would expect there a wide range of local initiatives underway to try and address the need for data sharing between service providers across health and social care and public services. There are also national programmes within NHS England around patient Apps and access, GP systems that offer citizens an app or view of their health records. They are all predicated on organisational held and controlled personal data and do not provide citizens with the independence and portability of the trust and confidence that would enable citizens to re-use these verified attributes independently.

Intra-governmental data sharing - There is data sharing between government departments and agencies and some online services in which third parties can gain access to government held data e.g. driving licence information for insurance companies. Other new initiatives are underway in different stages of procurement or design such as data sharing between the NHS and DWP and Identity verification hubs for DWP. Currently in the UK we have not found any sustained recognition of the need for collective action to overcome the friction effort, risk and cost in public services and

the need for portable reusable verified attributes under citizen control.

Private sector schemes - There are significant private sector initiatives to create schemes within sectors to reduce administrative costs for organisations. For example, within financial services there are initiatives to streamline the movement of pensions related data between providers and to create a financial passport to reduce the cost of onboarding new customers through shared credentials and outputs from KYC and AML checking processes.

Numerous data aggregators such as credit reference agencies are seeking to monetise access to personal data and proof points about citizens so that organisations can subscribe to their services.

Open Banking and midata Energy - There have been a number of regulator and competition and market authority interventions to mandate data sharing in sectors such as Banking and Energy, in which organisations are required to present a range of APIs that allow third parties to access data held by a citizen's bank or energy company and transfer this data into another service. These have consent steps involved but at no point do citizens themselves obtain a certified copy of the data that they can use independently. These transfers of data are only available for a defined period of time before they must be approved again by the citizen. Each scheme is different and at different stages of development. Even where they use common protocols and standards they are implemented differently. The consent journeys between schemes create inconsistent experiences for citizens who have no personal record of all the consent they have given and the data sharing resulting from it that they can review and adjust which makes understanding where and how personal data is being used hard and difficult to change.

Digital Identity - There have been a number attempts at implementing Digital Identity schemes in England and Wales and across sectors. All have been based on creating a market in which fees have to be paid to use a service or identity. Many of these schemes require different forms of proof in different formats and rely on external verification and assurance processes which create significant friction, effort, risk and cost for both citizens and relying parties. These schemes have been largely organisation or sector centric in their approach. Citizens are not empowered to reuse the proof identity or the set of credentials in other settings themselves: identity and the verified attributes that underpin are not made portable or put under the citizen's

control.

None of the schemes undertaken move beyond the identity assurance step. They are focused on identity assurance for the purpose of allowing a citizen through the front door of a service. Once they are through this door, processes remain unchanged, e.g. traditional online form filling and the provision of proofs in the form of documents (either uploaded scanned documents or posted). Some public and private sector services may use online data aggregator services to validate the information entered onto those forms. Many have to undertake manual checks. This fixation on getting citizens through the front door has, in reality, held many services back in terms of service improvement.

Many public service journeys were originally designed in ways that forced citizens to prove their identities before they could even start an application. The resulting delays and dropout rates meant many citizens were left unable to access services they were entitled to, causing severe hardship in some cases. A classic case in point is Universal Credits.

Summarised below are some examples of how verified attributes may be used in the future and some insight into some current approaches for third parties to access verified attributes held by one organisation and used by another.

UK Government Identity and Attribute Exchange (IAX) Scheme

The UK Government has confirmed that the current GOV.UK Verify Identity Assurance scheme will be replaced in the future with a scheme of broader intent in so much as it will not just focus on identity assurance but also include the concept of attribute exchange. This is a significant change and a step forward.

The UK government digital identity and attribute scheme is currently called the Identity and Attributes Exchange (IAX). This programme is being run by the Government Digital Service and the Department for Digital, Culture, Media and Sport within their combined Digital Identity Unit.

This scheme is designed to allow public sector organisations to easily use identity and attributes in their services. Private sector organisations may also take part in this scheme.

Members of the IAX scheme will be certified against a set of government-approved

scheme rules that follow trust framework standards that are currently being formulated.

The outline of the proposed scheme is currently being shared for consultation and feedback from public, private and third sector organisations. The consultation includes relying parties who may want to use the new scheme, organisations who may become attribute providers, a range of vendors who may seek to provide attribute exchange hubs and services, verification services or be credential providers.

There will be a government commercial framework for buying digital identities from the IAX, which will sit outside of both the trust framework and the scheme. The government commercial framework is still being developed.

The scheme will require certification of participants and will have a defined set of protocols that must be used. It is predicated yet again on a market model as opposed to a model in which the object is reduced friction, effort, risk and cost (FERC) in delivering public services and ensuring equality of and ease of access.

IAX-certified organisations can fulfil any of four defined roles:

- **Buyer** – such as a government department that wants to allow approved digital identities to log in to its services.
- **Identity provider** – companies that create verified digital identities for users, which can then be used to log in to online services.
- **Attribute provider** – organisations that collect information about users that can be used to verify their identity. The Passport Office or DVLA are examples, which could offer access to passport or driving licence data.
- **Broker** -a company that connects users, digital identity providers and attribute providers. Brokers will allow a buyer to access multiple identity or attribute providers.

DWP Dynamic Trust Hub

In common with other areas of government DWP are actively seeking to improve their own digital offerings to citizens and are intending to build a common platform around Identity and trust. They began market engagement in March 2019 and stated that the platform will consist of a number of continuously evolving solutions that support the core capabilities that the DWP feels it needs. This is not envisaged as a single solution,

but rather a collection of interoperable services that are linked by common concepts, standards and purpose.

This will be known as the Dynamic Trust Hub (DTH) It is anticipated that the DTH will consist of the following capabilities:

- Credentials and Authorisation;
- Identity Verification;
- Transaction Monitoring and Behavioural Risking;
- Fraud and Error Prevention

The Dynamic Trust Hub is not a live service and is still in development. It is not clear what the relationship between this and the Government Digital Service IAX is or is intended to be. The scheme does not appear to support the concept of citizens being able to provide or reused verified attributes beyond their dealings with the DWP.

There is no information about how citizens will interact with the DTH or if it is visible to them.

DWP / NHS England Data Sharing

DWP and the NHS in England have been undertaking discovery and technical proof of concept work relating to improving the accuracy and efficiency of administering applications to DWP Health-related benefits. This involves building a digital service to gather information from citizens and present it to DWP processing agents.

The emphasis is on addressing the time and cost of gathering the information needed to make a decision about the right support for someone with a health condition or disability. Three perspectives are being considered:

- Citizens applying for a health-related benefit need decisions about the support they are entitled to as quickly and accurately as possible.
- The DWP agent processing applications to health-related benefits needs quick access to verified medical information, so that it can accurately and effectively determine the right level of support for the citizen.
- Medical professionals need the process of providing medical information to DWP to be as frictionless as possible, so that they can focus on helping their patients.

In reality this is largely a vouching system that enables medical professionals to vouch

for or confirm diagnosis, or provide narrative supporting an application for health related benefits. There are parallels with the challenges faced by Social Security Scotland.

There may be direct NHS to DWP data sharing of information held in clinical data repositories, but this is not yet clear. Whether there is any data sharing back to the NHS is also not clear at this time. There appears to be no scope currently for the citizen to be an active participant in terms of delivering verified attributes covering diagnosis or being able to keep their own copy of any decision about benefits in a digital tokenised form.

International initiatives

There are multiple initiatives across the world that, in one way or another, demonstrate recognition of the importance of the sharing of verified attributes. They also illustrate how diverse and varied current ways forward are. The following list in alphabetical order provides an summary of these initiatives and programmes

Alberta Credentials Ecosystem

The Alberta Credentials Ecosystem (ACE) is a collaboration to create a decentralized, multi-sector digital credential ecosystem working in a local cluster in Alberta Canada. Credential in this context is being used to describe verified attributes that can underpin a range of transactions.

The scheme has a mixture of financial services, telecommunications, post-secondary, government, insurance providers. The goal is to create new value for citizens and organizations of every size and shape across the province. Citizens are able to control access to the verified attributes within the ecosystem. Each scheme member is both an attribute provider and relying party.

eIDAS

eIDAS seeks to enhance trust in electronic transactions in the EU's internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities across-borders. The goal is to increase the effectiveness of public and private online services, electronic business and electronic commerce in the Union. eIDAS will bring a new layer to Digital Signature Regulation and

aims to:

- Make cross-border electronic transactions more secure and trustworthy.
- Allow for transparency and standardization in the market.
- Ensure accountability.
- Allow citizens moving to new member states to reduce paperwork through online administration.
- Decrease red tape for businesses, meaning overheads can be reduced and profits increased.
- Increase flexibility and convenience of government services.

eIDAS is a scheme with standards and protocols and external certification requirements that work across the EU. How it is implemented is left up to each country.

The adoption rate has been much lower than expected in part due to low awareness and lack of use cases to drive up adoption. eIDAS does not address the broader issue of portable personal data to remove friction from online application processes and does not support verified attributes and their exchange beyond the narrow scope of the scheme.

eIDAS is exploring future options for the scheme including the notion of enabling citizens to control their own identity through the adoption of support for Distributed Identifiers, based on the W3C standard.

Estonian Government

Estonia has developed a national ID-card system that links into its digital services. It is considered to be much more than a legal photo ID. The card is the mandatory national card and also provides digital access to all of Estonia's secure e-services. The ID-card is linked to a digital identity and along with it a Mobile-ID or Smart-ID, so they can safely identify themselves and use e-services.

The ID-card is used as a legal travel ID for Estonian citizens travelling within the EU, as a national health insurance card as well as proof of identification when logging into bank accounts. It is also used to deliver digital signatures, i-Voting, to check medical records, submit tax claims, and to use e-Prescriptions. 99% of state services are online and some 67% of the population use the National ID Card regularly.

A part of the Estonian strategy is to remove the need for citizens to have to provide

information to the state more than once and enable it to be shared with third parties connected to the state via what they describe as X-Road.

X-Road® software based solution X-tee is the backbone of e-Estonia. Invisible to citizens, it allows the nation's various public and private sector e-service information systems to link up and function in harmony.

Estonia's e-solution environment includes a full range of services for the general public, and since each service has its own information system they all use X-tee. To ensure secure transfers, all outgoing data is digitally signed and encrypted, and all incoming data is authenticated and logged. It connects different information systems that may include a variety of services. It has developed into a tool that can also write to multiple information systems, transmit large data sets and perform searches across several information systems simultaneously.

All citizens are dependent wholly on the state National ID Card to function effectively. They do not have independence or portability of their personal data or identity outside of the state run scheme.

There is little sense of how citizens prove entitlement or status for a broader range of transactions e.g. income, state benefits or how they themselves can control their the data the state holds about them.

GDPR compliance and how data portability and transparency is being addressed is not extensively explained. What can be noted is that the appointment of Data Protection Officers (DPOs) also raised many questions, as the position of a DPO was largely alien for Estonian data controllers and processors (with the exception of those controllers who processed delicate personal data under the former regime, for whom the appointment of a DPO, although in a less regulated manner, was optional) before GDPR.

It also seems that a lot of emphasis is being put on explaining what the possible and correct legal bases for processing personal data are. Estonian data controllers either have not always properly defined the legal basis for processing personal data or historically have relied extensively (and often incorrectly) on consent. The latter most probably derives from the wording of the previous Estonian Data Protection Act, which favoured consent as the legal basis for processing personal data.

Indian Government Aadhaar and Digilocker

These are two schemes by the Indian Government. They are both operating at significant scale and are both owned and operated by the state via large central databases, not distributed systems.

Both have come up against concerns around data protection and have faced adoption issues. Many service providers and citizens have resisted adoption because of issues related to trust, privacy and security. The two schemes have often been conflated, but have drawn a lot of attention over the last five years from those seeking to address the challenges around identity. The two schemes are:

Aadhaar is essentially a unique 12-digit random number relating to a verified citizen. It is issued by the UIDAI ("Authority") to the residents of India after satisfying the verification process laid down by the Authority. Recently the Indian Government has mandated that mobile phone numbers must be linked to a citizen's Aadhaar number.

Any individual, irrespective of age and gender, who is a resident of India, may voluntarily enrol to obtain Aadhaar number. The person willing to enrol has to provide minimal demographic and biometric information during the enrolment process which is free.

An individual needs to enrol for Aadhaar only once and after deduplication only one Aadhaar is generated - the uniqueness being achieved through the process of demographic and biometric de-duplication.

Demographic information	Name, Date of Birth (verified) or Age (declared), Gender, Address, Mobile Number (optional) and Email ID (optional), in case of Introducer-based enrolment- Introducer name and Introducer's Aadhaar number, in case of Head of Family based enrolmen- Name of Head of Family, Relationship and Head of Family's Aadhaar number; in case of enrolment of child- Enrolment ID or Aadhaar number of any one parent, Proof of Relationship (PoR) document
Biometric information	Ten Fingerprints, Two Iris Scans, and Facial Photograph

DigiLocker is an initiative of Ministry of Electronics & IT (MeitY) under Digital India

programme. DigiLocker aims at 'Digital Empowerment' of citizens by providing access to authentic digital documents to citizen's digital document wallet.

It has benefited from state leadership with some 156 issuer organisations (attribute provider) organisations pushing documents to the citizen's DigiLocker and some 45 requestor organisations (relying party). It currently has 38.6m registered citizens and over 3.7 billion authentic digital documents covering in excess of 300 distinct document types. Digilocker was launched as a beta in 2015 and has seen steady growth during this time. Critically citizens must possess an Aadhaar number to get a DigiLocker.

The DigiLocker platform is owned and operated by the Indian Government and has created a large database of citizen personal data and documents. It can only be used inside the scheme of supporting agencies. It cannot be used by citizens outside of the scheme. The data is not independently under the citizens control or portable.

The issued documents in DigiLocker system are deemed to be at par with original physical documents. The benefits of DigiLocker are described as:-

"Benefits to Citizens

- Important Documents Anytime, Anywhere!
- Authentic Documents, Legally at Par with Originals.
- Digital Document Exchange with the consent of the citizen.
- Faster service Delivery- Government Benefits, Employment, Financial Inclusion, Education, Health.

"Benefits to Agencies

- Reduced Administrative Overhead: Aimed at the concept of paperless governance. It reduces the administrative overhead by minimizing the use of paper and curtailing the verification process.
- Digital Transformation: Provides trusted issued documents. Issued Documents available via DigiLocker are fetched in real-time directly from the issuing agency.
- Secure Document Gateway: Acts as a secure document exchange platform like payment gateway between trusted issuer and trusted Requester/Verifier with the consent of the citizen.
- Real Time Verification: Provides a verification module enabling government agencies to verify data directly from issuers after obtaining user consent.

Indian Government: Licensed Account Aggregators

The Indian Government is establishing an ecosystem of 'Account Aggregators' that, with the individual's consent, act as a conduit of holders of financial information about them (banks, insurance companies, mutual funds, the tax system) to users of this information (providers of credit, personal financial management services, wealth management services). The system, which is similar to the UK's Open Banking system, was due to launch in May 2020. Account aggregators are responsible for transferring, but not storing, the individual's financial information.

Korean Government MyData Programme

K-Data (Korean Data) is part of the Korean Government's Department of Science and ICT that is responsible for developing Korea's strategies around data - Big Data, AI and Internet of Things data as well as personal data. It has established a separate programme for personal data that it calls MyData *(not be confused with the MyData Global membership organisation)*, whose core principles revolve around citizens being empowered with their own data.

The Korean Government is investing significant resources and effort into this initiative. Actions include:

- introducing legislation to enforce data portability in the credit referencing industry
- launching 8 different pilot projects to test MyData solutions: four in health, one in finance, one in energy, one in small business, and one for researchers (basically, a tool for them to gather information about their research around themselves for academic and grant getting purposes). The Government has invested US$10 million in these projects, all of which involve consortiums of companies. They are due to announce their first results soon.
    - They are planning an initiative focused on digital receipts (details on this remain vague). K-Data generally is also doing work on what it calls 'electronic certificates' with wide applications in non-personal data (e.g. supply chain issues) as well as (potentially) in personal data. Specifically, it is planning an initiative around electronic certificates for driving licences but so far few details are available.
    - The eight projects above have received official government backing, there are another 50 or so projects going on, on the side.

- a programme to educate the public about MyData. The MyData team are concerned that according to their research, at the moment only 8% of the Korean public both recognise the name MyData and can explain its core principles. This is a good indicator of the scale of their ambitions.
- a programme to educate primary school children about their data rights.
- running a series of conferences on the subject. At the last one in Seoul, held in December 2019, over 1000 delegates attended. Mydex Chairman Alan Mitchell was a keynote speaker at this event.

The Korean Government is clearly taking this initiative seriously, seeing itself as gaining international competitive advantage around innovation based on citizen empowerment and trusted uses of personal data.

However, currently, none of its initiatives focus on improving the efficiency and effectiveness of public service provision or on the use of verified attributes in doing so (aside from the general work on electronic certificates described above). As Scottish Government proceeds with the development of its Smart Entitlement Programme we recommend it creates links with the Korean Government to share learnings.

New Zealand Government RealMe®

RealMe is an initiative by the New Zealand Government which allows citizens to access multiple online services with one username and password, and securely prove who they are online. Citizens can use it to apply for financial assistance from the Ministry of Social Development, renew a passport and access their Inland Revenue account. It can be used to apply for a visa from Immigration NZ and access local council services, manage company register details, manage a real estate licence, access the police vetting system

A RealMe verified identity can be used to prove who a citizen is online. It can also offer the ability to verify the citizens address online. To set up a RealMe verified identity citizens need a passport, birth or citizenship certificate or immigration document. If a citizen applies with a NZ passport they have the option to take own photo using the camera on a phone, laptop, tablet or desktop.

If citizens apply using birth, citizenship or immigration documents they need to get their photo taken for free at a participating photo store. The main benefits promoted of RealMe are only having to provide proof of identity and address once. Giving the citizen

control of their personal information held by the state and being able to control who it is shared with.

RealMe is in use across both government and the private sector. The service has been created to build trust and confidence by adhering to New Zealand Government security, identity and privacy legislation. Adoption is growing with some 71 services available using RealMe.

The main benefits of RealMe promoted to organisations are as follows

- simplify online onboarding process - no separate identity checks or paper documents required
- help meet compliance and reporting requirements, including AML/CFT regulations
- receive high confidence identity data online to initiate processes to vet new staff or perform police checks
- increase accuracy, integrity and confidence in the customer information
- help reduce the risk of identity fraud, due to greater confidence in customers' identity information

Oklahoma Digital Driving Licence and REAL ID

Oklahoma has two schemes underway, one a Mobile ID, the other is an ID Card system that is replacing an existing system. The population of Oklahoma has been steadily growing, reaching nearly 4 million people in 2020.

Oklahoma Mobile ID has been developed by the Oklahoma Department of Public Safety (DPS), Oklahoma Office of Management & Enterprise Services (OMES), Innovate Oklahoma and their technology partners. It is the first and only digital US driver's license that is electronically verified against the state's DPS system of record and the first public launch of an ISO 18013-5 mobile driver's license in the United States. Oklahoma Mobile ID builds on the security of the DPS enrollment process while adding extra layers of anti-fraud protection and privacy controls for the user.

Businesses and organisations can verify the Oklahoma Mobile ID with confidence, as customers' information on the digital ID can be verified against the latest DPS record. The ID is updated directly from the DPS system of record. Oklahoma Mobile ID's verification interface enables transactions to occur quickly.

The new Oklahoma REAL ID is replacing an existing card. Prices range from $25 for an ID card or to convert an existing driver license, up to $42.50 for a first-time driver license. Higher fees apply to commercial licenses. The DPS is rolling out the ability to issue the new cards from July 2020 and should be able to support issuance from all offices by October 2020.

The REAL ID cards will be identical to Oklahoma's current cards with the exception of an added gold star in the upper right-hand corner.

Citizens are not required to get an Oklahoma REAL ID compliant license or identification card; however, if they plan to fly domestically or access federal facilities or military bases after October 1, 2021, they must have a REAL ID compliant license or identification card or another acceptable form of identification such as a passport or passport card.

The scheme is based on proprietary technology.

Sierra Leone: Kiva

The Sierra Leone Central Bank is supporting Kiva, a global microfinance organisation, in establishing credit profiles for unbanked individuals (three quarters of the population) which operate under their control and which are based on credentials provided by Government bodies (for example information collected voters' ID cards) and other microfinance institutions are being used as the basis of creating profiles and enabling people to have a digital identity.

Spain: IdentiCat

In Spain, the Catalan government is establishing 'IdentiCAT', a 'self-sovereign' identity system whereby the government mints an identity for a citizen and then places this identity under the citizen's control. Catalonia says it wants to be "the first country in which the citizen is the owner, manager and exclusive custodian of their identity and personal data". Since the announcement of this scheme in September 2019 no new details have been released on its evolution or progress.

The Verifiable Organizations Network

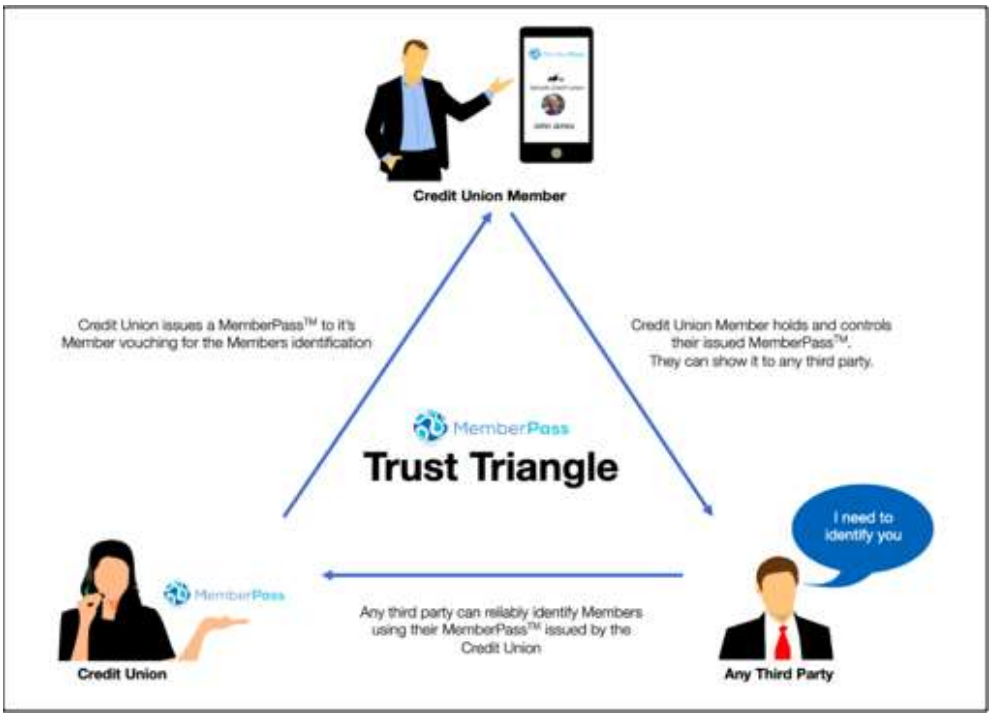
A joint effort between the Canadian Provinces of British Columbia and Ontario, the Verifiable Organizations Network (VON) was launched to improve the way governments and their citizens find, issue, store and share trustworthy data about organizations.

Whilst principally focusing on ensuring organisations can be verified in terms of who they are and what permits they hold. It is an example of the notion of verified attributes in use within an ecosystem.

United States: MemberPass

In the US, credit unions have established MemberPass, an identity system based on the 'Know Your Customer' processes credit unions go through when onboarding customers.

Having completed the KYC process, the credit union issues a 'MemberPass' to the member vouching for their identification. This voucher is stored in their mobile phone. Members can then share this voucher with any third party, who can check its provenance with the original issuing body.



Industry sector specific initiatives

There have been many industry led or sector specific initiatives over the last 20 years ranging from identity schemes, data sharing schemes many with the objective of reducing the friction, risk and cost for service providers within a sector as customers move between service providers.

There has been regulator intervention in a number of cases to mandate schemes to enable portability or ease ease of switching between one service provider and another.

Examples are the **Current Account Switching Service** that manages in the background the process of moving from one bank to another and ensuring things like standing orders and direct debits are paid and any money deposited in the old account makes its way to the new one.

There have also been programmes such as the **midata programme** led by the UK government. The aim of the midata programme was that consumers should have access to the information that companies hold about their transactions in a machine-readable and reusable format. The programme was focused on the banking, telecoms, energy and retail industries.

It met with considerable resistance from these industries partly because the Government's chosen use case was to use the information to make it easier for consumers to switch suppliers.

During it, the government took new powers to be able to mandate data portability and access but promoted sector led initiatives on a voluntary basis which ultimately were taken over by other regulations and decisions by OfGen and Competition and Markets authority which resulted in two main initiatives Open Banking and midata for the Energy sector. While the midata programmes immediate effects were small, it did have a longer term impact: its original formulation of the concept of data portability was picked up by European policy makers and formed the core of what became Article 20 (Data Portability) of GDPR.

There have been seemingly endless landscape reviews and consultations across government and sector organised programmes to determine responses to data portability obligations and build new schemes to manage portable identity and data transfer between organisations in specific sectors.

We have reviewed a large number of these for this project and have been actively involved in a number of them in one form or another over the last 9 years. Our observations are that very few took a citizen centred approach even though they were supposedly designed to empower citizens. The adoption rates and approach to implementation have not delivered the empowerment expected or not been implemented at all. Our recommendations in this paper address the principle failings

of these initiatives which in summary are.

- No involvement by public or third sector in terms of being attribute providers or attribute users, therefore offering no value in terms of improving public services
- Focus on the private sector and data exchange between organisations within the same sector to increase ease of migration for consumers, principally to drive more competition in those markets. This can create a positive message around data portability but is a limited use-case.
- No sense of portable verified attributes that are reusable by the citizen in any other contexts than the narrow confines of a sector scheme. The trust in the attributes did not travel with the attribute itself, rather it was about the infrastructure of exchange between known parties.

Financial Services

Open Banking API

Open Banking is designed to bring more competition and innovation to financial services. It was set up by the Competition and Markets Authority who issued an order to the market to open up bank account information. They undertook this on behalf of the UK Government.

Every provider that uses Open Banking to offer products and services must be regulated by the FCA or European equivalent. Open Banking also supports the implementation of Payment Services Directive 2 from the European Union designed to make data available and allow for easier mechanisms for payment within the European Single Digital Market and make more transparent fees relating to cross border transactions.

Open Banking enables Third Party Providers who are organisations or natural persons that use APIs developed to open banking standards to access customer's accounts, in order to provide account information services and/or to initiate payments. Third Party Providers are either/both Payment Initiation Service Providers (PISPs) and/or Account Information Service Providers (AISPs).

The customer whose accounts are involved has to provide consent and also authenticate themselves with the TPP and with their own bank. This consent is time limited and has to be re authenticated at regular intervals. The citizen at no time has

access to the data directly themselves for onward independent use. It is possible for a TPP to be a personal data store service provider who can enable a citizen to collect and store their bank data.

The range and scope of information available is limited to bank transactions and account data. There is no specific portability of trust in terms of the transaction history beyond the confirmation of its source.

Access to bank current account data can be valuable in providing debt and financial advice to citizens as well as enabling the aggregation of data from across different bank accounts and improving online services in which evidence of the nature of financial transactions are required and existence of a UK Bank Account.

Open Banking would not have happened without the introduction of regulation mandating its creation.

Viewed from the perspective of a Smart Entitlement Strategy, a number of key features of Open Banking stand out.

- It operates in a highly regulated sector and participants acknowledge that it would not have happened without powerful regulatory impetus. This makes it difficult to extend to less regulated industries.
- All data sharing is organisation-to-organisation. Individuals never directly access or control their data.
- While individuals provide consent to each instance of data sharing, were it to scale the result would be a) their data would be dispersed further and further across multiple different organisations and never aggregated to create a 'single view' of the individual's financial circumstances, b) individuals would almost certainly lose, not gain, effective control over their data because they do not have any simple, effective means of keeping a record of consents they have been given or managing these consents over time.
- As yet, it has not resulted in any 'breakthrough' services of any scale and has not challenged incumbents in the sector, as promised,

Pensions Dashboard

Pensions dashboards will enable people to access their pension information in a single place online, in a clear and simple form, whether that is on a laptop or tablet. Putting individuals in control of their data, pensions dashboards will bring together all pension

information from multiple sources, which can then be accessed at a time of their choosing.

The UK Government has committed to facilitating the pensions industry to develop this initiative and have given specific responsibilities to the Money & Pensions Service (MaPS) which include:

- Bringing together a programme team to lead the implementation of pensions dashboards
- Appointing an industry steering group to set the strategic direction of the programme
- Beginning work to create and run a non-commercial pensions dashboard – the MaPS Dashboard.

This is another example of where the UK Government has had to introduce primary legislation to require pension schemes to make consumers' data available to them through their chosen dashboard.

Energy Sector

midata energy project

The midata in energy intervention was intended to be a near-term reform, which aimed to enable the sharing of consumer energy data. There will be ongoing review and evolution of the standard, so that the benefits of sharing additional data sets are realised. Customers will be able to share their data with accredited third parties quickly and easily, which will ultimately encourage consumer engagement and drive market innovation and competition.

In May 2020 Ofgem stated that their retail market programmes, particularly the Switching Programme and Market-wide Half-Hourly Settlement (MHHS) programme, will be enacting or designing significant changes to the energy data landscape progressing over 2020 and 2021. Given the synergies and potential overlaps between activities for these programmes and activities required to deliver midata, they have paused development of midata in 2020/21.

The midata intervention complemented customers' new right to data portability provided for under the GDPR. This new right empowers customers by giving them more control over their personal data and midata will provide a means through which energy

suppliers can readily fulfil such data access and portability requests without hindrance.

The midata framework would enable automated and instantaneous fulfilment of a verified and consented customer's data request, across all of the requested data fields, by their energy supplier to an accredited third party. The scope of the initial iteration of the midata standard is limited to enabling the fulfilment of data requests (one-off or ongoing) in the context of current (rather than previous) supplier—customer relationships. Any data processing activities post fulfilment of the data request, such as switching, are out of scope and would need to be handled using alternate, relevant processes..

The primary use case for the mandatory midata framework is sharing domestic consumer data to allow tariff comparison (which could be based on a range or factors, including price, customer service or generation mix). Tariff comparison could occur on a one-off or an ongoing basis, which may therefore require access to data on an ongoing basis.

Midata will support the Ofgem Switching Programme by enabling easier, quicker and more accurate price comparisons, as the first step in switching tariffs or suppliers.

It is envisaged that at some point in the future the midata standard would be expanded to enable the fulfilment of data requests for transfer of relevant datasets that facilitate the following:

- An indication of Warm Home Discount (WHD) status of customers
- Time of Use (ToU) meter data comparisons for Economy 7/10 meter data as a minimum (e.g peak and off peak/day and night readings).

This is another example of regulation having to be put in place to change the private sector behaviours supported by the implementation of GDPR. Energy consumption, expenditure and tariff data can be a valuable source of information to support advice and guidance services, including energy management, debt and financial advice.

midata in the energy sector is not to be confused with the smart meter programme which is designed to save energy companies the cost of meter reading manually and opens up consumption data to third parties over the smart meter network as well as enabling customers to directly observe their own energy consumption via consumer access devices.

Care Sector

The care system for children and young adults in Scotland

The recent Independent Care Review in Scotland found that data is often captured and held by a range of different agencies in varying formats and not readily shared and concluded that "Care experienced children and young adults must have ownership over their own stories and personal data so that they can understand and influence how their stories are shared."

It continued:

> "Scotland has the ability to support the development of innovative digital tools that reflect how children communicate and allow greater ownership and control of information so official narratives reflect their story, not just the facts the system holds about them.There are technologies that can demonstrate entitlement and eligibility without sharing any personal information or history.
>
> "Scotland must be committed to the development of digital tools that incorporate the principle of information ownership. These digital tools must operate at a scale that allows care experienced children and young adults to have control over their information and how it is shared. The development of new ways to share information that recognise the ownership of care experienced children and young adults over their own stories will benefit all children in Scotland.

Providing the tools (e.g. personal data stores) for children and young adults to do all of this is beyond the scope of this report. But the ability for different elements of the system to share data, safely and efficiently at different stages of the young person's journey is not.

DHI has conducted a simulation in its demonstration environment to show how the use of verified attributes can help those in care manage key transitions such as moving from care to university. DHI's proposed 'Care Review Wallet' contains a small number of key verified attributes, some of them specific to the care environment (e.g. proving they are a care leaver to access bursaries) and some generic - e.g. verifying they have passed

exams, their financial status, the fact that they are a person with a disability etc.

The simulation shows the need for safe, efficient sharing of data between key parties such as the individual's care provider, UCAS, the university, a new landlord, the student's bank, and all those involved in her house move.

Education

Portability e..g certificates of education, achievement and education has been the central agenda across education for many years to avoid misrepresentation and improve trust in asserted capabilities. Two examples of such an approach are summarised below

Cities and Guilds - Digital credentials programme enables qualifications and certificates to be produced in machine readable form with cryptographic protection meaning the relying parties can trust the information on the

Open Badges - an open standard for portable digital certification of experience and qualifications is being taken forward by an organisation called IMS Global Learning Platform which also certifies organisations and services that work with and use Open Badges https://openbadges.org/.

Degree Qualifications A number of universities have also collaborated on issuing degree certificates as part of an online service in the USA.

There is no consensus on standards but ongoing attempts to create specific standards for different levels of education continue.

Scotland has a significant opportunity to take advantage of its National Entitlement Card and Scottish Qualifications Authority to create smart entitlements for education attainments that can be linked securely and safely to citizens which can support the broader employability agenda under the National Performance Framework and access to a range of benefits.

Transport

Transport for London

TfL has an extensive array of API based services for non personal data which is available to third parties. TfL also offers travellers access to their travel history which can be

emailed to them directly in machine readable format. TfL do not retain personal details of citizens travel beyond a period of six months but do aggregate journey history to aid with planning. Tfl also have a mature GDPR compliance service.

DVLA and DVSA API services

The Driver and Vehicle Licensing Agency (DVLA), holds over 48 million driver records and over 40 million vehicle records.

The Driver & Vehicle Standards Agency carry out driving tests, approve people to be driving instructors and MOT testers, carry out tests to make sure lorries and buses are safe to drive, carry out roadside checks on drivers and vehicles, and monitor vehicle recalls.

Both have a range of API based services that enable third parties to access information on drivers and vehicles and related information online. They also provide online web based access to the same information Summary examples of these as followers:

- MOT history -The ability to access test history information about any vehicle including reasons for failure and related vehicle information and test meta data.
- Hiring a vehicle licence code service - enables API based access to driving licence information for hire care companies, individual applies for time limited code
- Check driving licence online service - used by insurance companies as part of applications for insurance
- Access Driver Data Service providing employers and businesses needing to check driver records instantly over API's.
- Vehicle Enquiry Service used by insurance companies and other service providers to check the current state of any vehicle in the UK

Standards, concepts and scheme initiatives

There are many standards and specific initiatives underway across the globe, each seeking to define a standard for verified attributes, whatever terms they use and the metadata that must exist for verified attributes to be trustable and machine readable. There are standards working groups on areas such as consent management, the structure of verified attributes (tokens, credentials), data standards for a range of human activities and the encoding of personal data across a number of different areas of human existence such as health and care and, everyday living, financial services,

telecommunications, ecommerce, adtech, search, energy and social media.

These are distinct activities that some are dealing with the encoding of data, some with the exchange of data and others with the ability to understand and trust data

WC3 Verifiable Credentials standard and Distributed Identifiers

In November 2019, the World Wide Web Consortium (W3C), which develops web standards, published its Verifiable Credentials standard which seeks to provide a standard way to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable. It identifies a number of potential use cases in education, retail, finance, healthcare, and proofs of professional credentials and legal identity.

UMA - User Managed Access

User-Managed Access 2.0 or UMA is a new federated authorisation standard protocol which enables party-to-party sharing.

UMA gives a resource owner (citizens) the ability to control who can access his or her protected resources (digital assets) from an authorisation server by creating authorisation policies no matter where the resources reside. For example, an elderly person sharing health-related data (such as medical prescriptions and blood reports) with doctors, and family members.

Sharing of resources can be done selectively which helps citizens gain control of their resource sharing in a reliable and secured manner. The specialty of this protocol is that resource owners need not to be present online at the access time as the cross-party sharing is driven by predefined policies.

Consent Receipts

A consent receipt is a notice created from a record of consent provided to an individual the moment a person agrees to the collection, use and sharing of personal information. Its purpose is to decrease the reliance on privacy policies and enhance the ability for people to share and control personal information. Citizens could maintain a central record of all such receipts for subsequent review and revocation. This is being developed as an open specification.

OpenIDConnect

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It allows relying parties to authenticate the citizens credentials with a credential provider based on the authentication performed by an Authorisation Server, as well as optionally obtain basic profile information about the citizen over a secure API.

OpenID Connect allows relying parties of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, allowing participants to use optional features such as encryption of data, discovery of OpenID Providers, and session management, when it makes sense for them. OpenID Connect also supports the concept of a self issued OpenID that enables citizens to be their own credential provider and supports the concept of self sovereign identity.

OpenID Connect is growing in popularity and has taken over from SAML as the preferred protocol for many relying parties and credential providers as well as attribute providers who wish to use it to authenticate against specific APIs.

Data Transfer Project

The Data Transfer Project was launched in 2018 to create an open-source, service-to-service data portability platform so that all individuals across the web could easily move their data between online service providers whenever they want.

The contributors to the Data Transfer Project believe portability and interoperability are central to innovation. Making it easier for individuals to choose among services facilitates competition, empowers individuals to try new services and enables them to choose the offering that best suits their needs.

The contributors believe that people should be in control of their data on the web, part of this is the ability to move their data. Currently users of services can download a copy of their data from most services. The Data Transfer project focuses on a different aspect of data sharing, making it easier for users to move data between providers.

At its core the issue being addressed is data portability between services for each of switching or migration. Given the expertise of these organisations, there may be things Scottish Government can learn from the open source project on data portability. The contributors currently are Facebook, Apple, Google Microsoft and Twitter. We

understand (from private conversations) that attempts to expand the number and range of participants have so far been rebuffed. The Project has no work streams focusing on public services or verified attributes or support for smart entitlements.

Self Sovereign Identity

There has been much confusion over the use of the term self sovereign identity. A specific branch of technology advocates have adopted it to promote their approach to delivering verified attributes and identity services. The concepts and principles of self sovereign identity can be implemented in a number of different ways and can make use of different technologies to achieve the end state

Self-sovereign identity (SSI) is a model for managing digital identity credentials and verified attributes (which can be called tokens or credentials) which an individual or organisation has sole ownership over the ability to control their accounts and personal data. Individuals with self-sovereign identity can store their data to their preferred devices and attribute stores and provide it for verification and transactions without the need to rely upon a central repository of data. With self-sovereign identity, citizens and organisations have complete control over how their personal information is kept and used.

In all models of identity management, a digital identity requires identifiers, which ensure the citizen or organisation is who they say they are. However, with self-sovereign identity, identifiers do not need an intermediary e.g. a credential provider.

This means that a citizens or organisations self-sovereign identity can be registered to one or more registers or ledgers protected by encryption in a range of forms.

The person can then share that identifying data or subsequent verified attributes when making a transaction with another entitle such as a bank, for example.

With self-sovereign identity, a citizen or organisation can control the flow of their data using an online app from one of their devices then use an identification number and identity information to verify who they are and release information from one or more attribute stores they control. Self-sovereign identity concepts include:

- Self-sovereign identity is made up of claims, proofs and attestations
- A claim is an assertion of about a specific matter
- Proofs are the verified attributes (forms or documents, transactional data) that

act as evidence for a claim. So, for example, a proof could be a passport or birth certificate or a specific range of transactional data such as location or income or a specific entitlement to state benefit.
- An attestation, or validation, is when the other party validates the claim is true. Attestations can be stored in the citizens attribute store, device or service and is machine readable.

The W3C standards for distributed identifiers and verified claims are gaining significant momentum within this specific approach.

The technology and vendor community promoting the use of blockchain and distributed ledger technology have embraced and promoted the generic term 'self-sovereign identity' to present their particular solutions as the only way the concept can be implemented. This is generating wide confusion.

However SSI can be implemented using a range of technologies and is not predicated on blockchain or distributed ledgers to work. It can be implemented anywhere with the following elements:

- User agent: A program, such as a browser, mobile App or other Web client, that mediates the communication between holders, issuers, and verifiers.
- Universal Resolver: a server featuring a pluggable system of DID Method drivers that enables resolution and discovery of DIDs across any decentralised system
- Universal Registrar: a server that enables the registration of DIDs across any decentralised system that produces a compatible driver.
- Identity Hubs: **secure personal data stores** that coordinate storage of signed/encrypted data, and relay messages to identity-linked devices.

Decentralised Identity Foundation

The Decentralised Identity Foundation has been set up as a community for those wishing to explore decentralised identity solutions. One of its working groups is investigating "standards and technology that create, exchange, and verify claims and credentials in a decentralized identity ecosystem".

Oasis COEL Classification for Everyday Living

The OASIS COEL specification provides a privacy-by-design framework for the collection and processing of behavioural data. It is uniquely suited to the transparent use of

dynamic data for personalised digital services, IoT applications where devices are collecting information about identifiable individuals and the coding of behavioural data in identity solutions. The specification pseudonymises personal data at source and maintains a separation of different data types with clearly defined roles and responsibilities for all actors. All behavioural data are defined as event-based packets. Every packet is connected directly to an individual and can contain a summary of the consent they provided for the processing of the data. A combination of a taxonomy of all human behaviours (the COEL model) and the event-based protocol provide a universal template for data portability. Simple interface specifications enforce the separation of roles and provide system-level interoperability.

In the longer term, COEL could be a valuable means of capturing structuring living activity data that can be useful in determining a person's real world activities. It may also be used to form a digital signature of a person and to help with eligibility assessments.

NIST Schema for Attribute Metadata

In February 2018 NIST published a proposed schema (Attribute Metadata – A Proposed Schema for Evaluating Federated Attributes (NIST IR 8112), which contains a metadata schema for attributes that may be asserted about an individual during an online transaction.

Open Badges

Open Badges are a leading format for digital badges. Open Badges are verifiable and shareable, and they contain detailed information about the achievement and what the recipient did to earn the badge. Originally launched by Mozilla Foundation with a defined specification, the focus is now on life long learning. Open Badges are visual tokens of achievement, affiliation, authorization, or other trust relationship shareable across the web. Open Badges represent a more detailed picture than a CV or résumé as they can be presented in ever-changing combinations, creating a constantly evolving picture of a person's lifelong learning.

openEHR

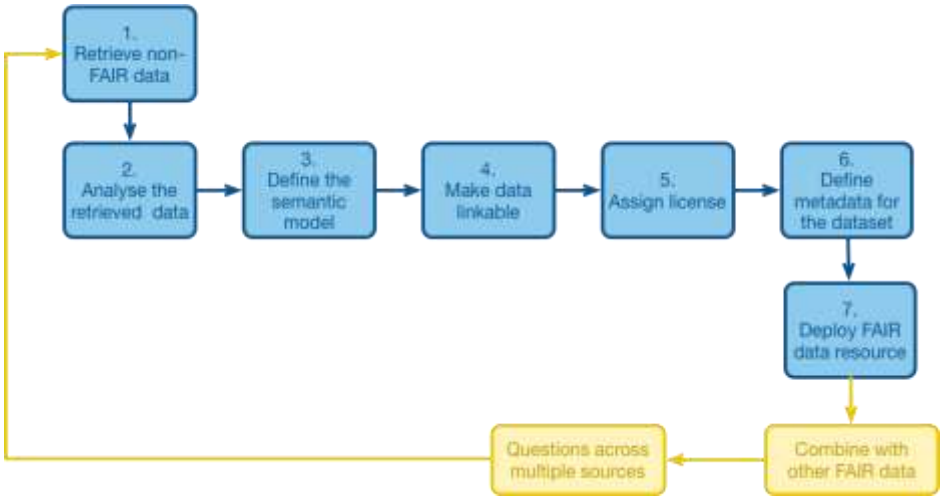
openEHR is the name of a technology for e-health, consisting of open specifications, clinical models and software that can be used to create standards, and build information and interoperability solutions for healthcare. The various artefacts of

openEHR are produced by the openEHR community and managed by openEHR International, an international non-profit organisation originally established in 2003 and previously managed by the openEHR Foundation.

The Scottish Health Service has adopted OpenEHR for its core clinical data repository under development by the NES Digital team and for data exchange between healthcare providers.

GO FAIR Initiative

The GO FAIR Initiative has some Fair Data Principles[3] apply to metadata, data, and supporting infrastructure (e.g., search engines). Most of the requirements for findability and accessibility can be achieved at the metadata level. Interoperability and reuse require more efforts at the data level. The scheme below depicts the FAIRification process adopted by GO FAIR, focusing on data, but also indicating the required work for metadata. The Data Delivery Group are investigating the adoption of this approach as part of the broader Data Transformation agenda in Scotland.



Trust over IP Foundation

The Trust over IP Foundation is a recently launched (May 2020) initiative that brings together private sector corporations like Mastercard, Accenture and IBM with non-profits to "provide the digital trust layer that was missing in the original design of the

[3] This is not to be confused with the Trustmark FairData that offers independent certification for how organisations deal with personal data, it also has FairData Principles

Internet". It aims to develop a global standard to ensure digital trust "using digital identity models that leverage interoperable digital wallets and credentials and the new W3C Verifiable Credentials standard" to address the challenges consumers, businesses and governments face when trying to manage risk, improve digital trust and protect all identities online.

Sovrin Foundation

The Sovrin Foundation is a nonprofit entity that provides the business, legal, and technical support for the Sovrin Network, an open source project. Charged with administering the publicly created Governance Framework for the Sovrin Network, the Foundation is committed to transparency and neutrality. The Sovrin Network makes use of the Hyperledger projects to create a distributed network for self sovereign identity and the exchange of verified attributes.

Technology and Service Providers

The technology needed for implementation of a Smart Entitlement Strategy already exists. Scottish Government does not need to commission a big IT infrastructure project to make this happen.

There are a number of technology providers, some working with and implementing offerings based on open source components as part of collaborations, others developing proprietary technology.

They principally focus on enabling inter-organisational to data exchange, offering citizens an opportunity to participate in these point to point data sharing transactions to support a specific service provision. Almost every systems integrator and digital consultancy service has a practice or service surrounding a range of technologies that they hope to win projects with organisations to build, configure and implement such inter-organisational data sharing.

Personal Data Stores and Personal Data Exchanges

There are multiple services now operating claiming to empower individuals with their own data in one way or another. The best, most recent overview of these services and their characteristics is the MyData Operator paper produced by MyData Global. The broad stated goal of these different organisations is the same: the creation of a 'human

centric personal data infrastructure' but they have a range of different business models, focus on different types of data (e.g. health data or social media data), and different purposes. However none that we know of are focused on enabling the collection, use and sharing of verified attributes for the purposes of improving public administration and services.

An Esade Business School research paper My Data, My Rules reviews a number of organisations operating in this space, including Mydex CIC.

Distributed Ledger based Technology and schemes

Hyperledger is an open source community focused on developing a suite of stable frameworks, tools and libraries for enterprise-grade blockchain deployments.

It serves as a neutral home for various distributed ledger frameworks including Hyperledger Fabric, Sawtooth, Indy, as well as tools like Hyperledger Caliper and libraries like Hyperledger Ursa.

Zortrex is an example of how token minting can be done. Organisations wishing to 'tokenise' a piece of data send it to Zortrex via an API. Zortrex returns the token, keeping a copy in its data vault. The token represents real personal and non-personal data (e.g. financial data, Identity data, investment data, debt data) but cannot be converted back to the original data.

Service Providers

There are any number of large and small scale consultancy and system integration organisations who are supporting deployment of distributed ledger technology, personal data stores, credential providers and brokers and hubs using a variety of proprietary and open source components

The Improvement Service is well established and limited by guarantee service provider to the Scottish Government and Local Authorities across Scotland and deliver operational services and project based services as well as supporting investigations into new shared services and new approaches.

Condatis a Scottish SME and part of SiteKit Group. They provide a range of consultancy,system integration and platform services built on the Microsoft Azure platform and have undertaken a number of projects in the public and private sector

addressing the issues of identity and vouching services.

Wallet.Services a Scottish SME who has developed its own blockchain technology and range of business applications designed to enable the sharing of attributes on an organisation to organisation basis with the concept of a citizen wallet to control the consent of sharing verified attributes. Their future plans are the open sourcing of their core block chain technology in order to focus on developing applications built on top of it.

Analysis of current state and future requirements

Analysis of requirements of future state

A number of things fall out of our analysis of the Current State. They include:

The power of portability. Improves access, removes duplication of effort, cuts costs, speeds up processes (and therefore efficiency and capacity), reduces effort/hassle. Cuts down the time and effort looking for information, waiting for it to arrive, checking that it is valid and passing it on or uploading it to a portal or posting it into a service provider.

Make once use many times. As an example the National Entitlement Card (NEC) generates a strong verification of the individual from the relatively early age of 12. This is something that could be carried through that individual's life, becoming a door opener to a wide range of other services offered outside the scope of the scheme itself. Reuse of the National Entitlement card verified attributes were used during the Attribute Prototype to show how an application for a bank account and an independent living transition support grant could be streamlined.

Separate data infrastructure from transactions and devices, and be technology agnostic. As an example NEC was originally developed to unleash the potential of a new technology - the smart card. Its approach and infrastructure was designed and built before the advent of other technologies such as the smartphone, and the ability to give phones smart card capabilities. Currently, there is work under way to adapt the NEC system to the opportunities opened up by smartphones.

However what this experience shows is that a key design principle of a Smart Entitlements strategy should be that the data layer should be separated out from the transaction and device layer. Data needs to be made available no matter what device is being used, or what transaction is being undertaken. The data infrastructure needs to be able to respond quickly and flexibility to new device technologies as they emerge and new transactions and services.

The role of vouching. Some forms of verified attribute have been rigorously checked by a responsible trusted authority against a defined process that may be regionally, nationally or internationally recognised: the information on passports and driving licences for example. But not all verification processes need to take this form. As an example the NEC also relies on 'vouching' where one trusted person or organisation confirms a piece of information about an individual. In the case of the NEC a school may say an individual is a student at that school, a teacher may confirm they teach that student and the photograph of the student is accurate, parents may vouch that they are parents and again vouch for the accuracy of the photograph.

A Smart Entitlement strategy needs to be open to the opportunities created by such vouching while ensuring that the accuracy and reliability of the resulting information is as high as possible.

With vouching it would also be possible to secure multiple vouches for the same piece of information from different sources adding further levels of cross checks to a core piece of information.

One data point many uses. Very often, data that has been collected or generated for one purpose can be re-used for a range of other purposes. For example, the concessionary fares component of the NEC requires that an individual's identity be linked to their usage of public transport. This is necessary for the administration of the scheme (e.g. reconciliation of payments between different bodies). However, it can also be used for other purposes such as 'proof of physical economic existence', help in searching for missing persons, or building pictures of individuals' carbon footprints.

This extends the above design principle of a Smart Entitlements Strategy: (separation of data infrastructure from transaction devices) that data generated for one use case should not remain trapped by that use case. The data needs to be separated out from the use case, being held in a different infrastructure, so that it can be accessed and re-

used for other purposes.

Technology requirements

The key requirements for a robust resilient Smart Entitlement Strategy is that any technologies used should be reliable *and* flexible - and not a source of lock-in either to a particular vendor or a particular technology. For this reason, the programme should be based on open source, open specification and when available open standards. The focus should be on reusable building blocks.

There are many technical options that can be employed but this Strategy is not something that requires proprietary technology. Please see Appendix C for more details on technical architecture for an attribute ecosystem over which Smart Entitlements would travel and be stored.

Identified user needs

From our joint (DHI and Mydex CIC) work on service design, and their work on the verified attribute prototype and multiple other projects we have identified a range of common user needs and wants, especially in the context of applying for and receiving services from public and third sector providers. Users in this context are citizens and front line teams in service provider organisations. The top user needs and wants are:

Friction reduction. Users want to eliminate all possible obstacles, barriers and sources of delay to getting the job in hand done. Friction is not only operationally inefficient, it has powerful negative emotional impacts (see below).

Effort reduction. Services that are clear, simple and easy to use get used. Services that are not simple, clear and easy to use either do not get used at all, or only get used under protest. The service design challenge here is to create citizen processes that:

- minimise the steps needed to complete a task,
- eliminate all work that is unnecessary (we believe based on experience working in Scotland that most form filling is unnecessary work),
- minimise cognitive load on the user (time and effort spent trying to understand what is required and how to meet this requirement),
- avoid friction.

This does not mean that all citizen processes should require zero effort - only that it

should be genuinely productive. For example, stopping to think about 'whether I really want to do X' or to 'ensure I really get what I need' is sometimes very important.

Risk reduction: If citizens are unable to provide the right information at the right time they risk missing out on services or benefits they may be entitled to, making errors that result in the wrong service being provided or being accused of fraud. If consent processes and security issues are not addressed properly they may also end up giving the wrong information to the wrong people with multiple possible consequential harms. A Smart Entitlements Strategy needs to be designed so as to minimise if not eliminate all such risks.

Cost reduction: very often, citizens incur direct costs (e.g. money spent on travel, time at work lost due to the need to present documents manually at a physical location or paying for child care) as a result of having to spend time/travel to locations to present information. The more processes can be digitised and automated the more these costs can be avoided. (Citizens can also benefit indirectly but greatly from contributing to processes that help service providers reduce their costs and thereby improve their ability to provide good quality services). As can be seen from the user research from the attribute prototype citizens were largely unaware of the cost, risk, effort and friction service providers face in validating and processing applications.

The above user needs are all operational. What is often overlooked but very important is that each one of them can and often does have powerful emotional impacts. When citizens experience friction, effort, risk and cost when attempting to access public services they may feel a range of negative emotions including frustration, stress and anxiety, a sense of helplessness, defeat and being overwhelmed, of doubt and uncertainty, and of boredom.

On the other hand being citizens feeling empowered to use information to *'get things done easily and efficiently in my life'* can trigger a range of positive emotions including a sense of agency, mastery and effectiveness, confidence, reassurance and satisfaction.

Very often the 'real' effects of good or bad service design - including the provision of public services and the potential for Smart Entitlements - lie in these emotional realms of how they make citizens *feel*. To the degree that a well-implemented Smart Entitlement Strategy can address both operational and emotional harms/benefits at the same time, it can become one way in which many of the goals of an inclusive wellbeing economy and the National Performance Framework can be implemented practically.

While reduction in friction, effort, risk and cost lie top of the list of user needs (for all of the above reasons) there are other broader citizen needs that the Smart Entitlement Strategy can support. These include the need for:

- Quality services that more *'exactly fit my particular circumstances and needs'*, made possible by improved ability to provide exactly the right information at the right time
- Timeliness: accessing services *'when I need them'* (and not two weeks or a month later)
- Resilience: having the resources and capabilities to new and different needs as they arise.

From a social/economic point of view this last user need is perhaps one of the most important while also being the most overlooked because it is an absence - a *'dog that is not barking'* - rather than a present, felt, irritation. One of the most important benefits of the Smart Entitlement Strategy going forward may lie in this area: in increasing citizen resilience, in providing them with the means and capabilities of rising to new challenges as they come along (Covid 19 being one example), and multiple changes in their circumstances as they go through their lives.

This is a 'need' that most citizens do not think about because the possibility of its existence has not yet been recognised. It is a classic case of an unarticulated (versus articulated) need - and is all the more important because of that. This aligns strongly to widespread calls to 'move forward better' as we recover from the pandemic.

Stakeholders

Very often 'stakeholder analysis' satisfies itself with a generalised assessment of broad, abstract categories of 'stakeholders' such as 'citizens', 'employees' or 'organisations'. If left at too high a level, such analyses can be interesting but operationally useless. We have developed a spreadsheet model (see Appendix A) that identifies the highly specific interests and characteristics of the key stakeholders of the proposed Smart Entitlement Strategy. This analysis is action-oriented - focused on specific initiatives and actions that may be needed to ensure the full positive participation and support of each particular stakeholder.

Citizens are an important case in point as stakeholder they may be an employee, student, parent, child, family member, voucher, patient, carer and any number of other

roles, all of which require personal data and different proof points.

Organisations are another critical case in point, acting as relying parties, and attribute providers, employers, service providers to citizens and others.

Above all context is a critical consideration and the smart entitlement strategy must be able to support different contexts of use which is why data independence is so important in attribute architecture which is the rails on which smart entitlements will travel.

The motivations of organisations may vary in different contexts and may require incentives or consequences to ensure and promote participation. The Stakeholder analysis has considered the influence of Scottish Government on different stakeholders and how some stakeholders represent a higher priority as anchor participants in a Scottish Attribute Provider Service across which Smart Entitlements can flow.

Design principles

In considering what the design principles should be we have taken the policy objectives and current state into consideration and the broad range of initiatives we have reviewed. The potential of smart entitlements is so significant that ensuring the it can be implemented in a manner that is low risk whilst delivering maximum benefits has informed the core design below that we recommend

- **Available 24/7 -** Individuals should be able to use their attributes whenever they want to.
- **Instantly usable -** Citizens should be able to access, share and use their attributes whenever and wherever they need, without operational or other barriers. This means, in turn, that:
    - they should be able to carry their attributes (or means of accessing these attributes) with them (e.g. by means of a mobile phone app);
    - there should be easy navigation to the data (which requires the development of a metadata directory with clear, easy-to-understand descriptions/nomenclature for different bits of data (proof of age is different to proof of birthday, which is different to proof that the individual is over 18);
    - It should be easy for citizens to send the data and for relying parties to recieve/use it

- **Permanent and resilient -** The citizen's attribute/personal data store should be a permanent resource. This means, for example, that it should not be stored solely or only on a particular device which can be lost, stolen or broken.
- **Untethered/independent -** Attribute providers (and relying parties) should not be able to control or influence what citizens use their attributes for, or how they use them. Operationally, independence means that a certified copy of verified attributes should be stored separately from their sources and consumers.
- **Trustworthy and trusted -** Relying parties need to be able to trust the attributes they receive. Trust (i.e. proof of verification/provenance) should travel with the attribute. This also means that, where necessary, attributes should be constantly updated. (Some attributes, such as 'I am over 18' remain the same once established. None of us are getting any younger. Other attributes such as marital or employment status, or whether the individual has a valid driving licence or passport, change over time, but relatively slowly. Other attributes, such as the amount of money in my bank balance, change rapidly. In the first instance, the Core Attribute Set should consist only of un-changing and slowly changing attributes, with mechanisms for real-time updating as and when changes happen (e.g. linked APIs).
- **Easy and safe to use -** Attribute providers and relying parties should be able to plug into the system easily, quickly, safely and cheaply without needing to engage in large scale overhauls of their existing systems or processes. The new infrastructure should be built on top of, and plug into, what already exists.
- **Extensible / Expandable -** No limits should be placed on the number/range of attributes that citizens can acquire, store and use. The citizen's attribute store should be seen, and treated, as an appreciating asset which is always being added to.
- **Safe by default -** A new system of smart entitlements will result in the creation of rich, valuable new data assets. This means bad actors will seek to gain access to this data for their own ends. Safe by default includes:
    - Data security: highest standards possible
    - Data protection: rules and processes to ensure that external parties only gain access to attributes that are strictly necessary for the purposes of providing a specified service, that they only hold the data so long as they need to provide this service, that they do not use this data for any purposes other than provision of this service; and that they do share this

data to any other party other than is strictly necessary for the provision of the service.

We have created the above list with some key principles in mind specifically that:

- **Together, the design principles should be complete** in the sense that if one of them is missing, the system as a whole won't work properly.
- **They are not abstract** - they should flow directly through to operational requirements. For example, design principles for successful commercial passenger flight include ability to be propelled safely through air, ability to take off and land safely, keeping passengers safe and comfortable in flight. These translate through to operational requirements in terms of propulsion mechanisms, wing flaps, retractable landing gear, pressurised cabins etc. The same applies to the principles listed above: they translate into a series of specific actions and requirements.
- **They are solution agnostic**. They do not specify, for example, if the propulsion system is a jet engine, propeller or any other system, so long as it meets the necessary requirements.
- **They can be implemented today and represent a low risk way forward**. This is about delivering value and transformation today not in some theoretical future requiring wholesale change.

Interoperability

For a smart entitlement system to work, high levels of interoperability will be needed so that verified attributes can flow from and to many different organisations/institutions with different software and IT systems, data schema, meta-data etc. There are two main ways to reduce/eliminate such barriers: the creation of common standards or the provision of 'translation' services (e.g. improved interoperability).

Where practical and feasible, it is desirable to create common standards but often the quest for such standards becomes a source of delay and cost (see Appendix F).

Our analysis suggests that the conditions for successful standards development outlined in Appendix F do not apply in the context of a development of a system for the sharing of verified attributes, mainly because existing IT systems and vested interests are too embedded and the costs of forcing change too high.

For this reason we recommend prioritisation of interoperability between organisations and systems working to different standards. This creates a need for interoperability enabling 'translation services' that enable:

- information to be taken or accepted from one organisation/system using one schema, format etc,
- new metadata to be created that describes the information
- this information to be translated into new, different schema, formats etc with the new metadata attached to it
- this information to be forwarded safely and securely to other organisations/systems using different schema, formats etc
- The ability for the trust and confidence in the data not to be diminished during the translation and transformation from one format to another, it must carry the trust with it

Criteria for recognition/inclusion of attribute stores

One of the risks of a Smart Entitlement Strategy is that a key component of the system - citizen attribute stores - fails to fulfil its functions. This can happen across many dimensions including operational and security failings and business model incentives i.e. a desire of vested interest in undertaking or allowing invasions of privacy for financial gain.

It is strategically unwise to place all eggs in the basket of a single attribute store provider: the system should allow for and encourage citizens to be able to choose from a range of (interoperable) attribute providers, thereby encouraging healthy competition between them. But all of these attribute store providers need to be fit for purpose.

Scottish Government will therefore need to create clear criteria to determine whether an attribute provider is fit for purpose, and to require attribute providers only to provide attribute stores that meet these criteria.

Issues which need to be considered in the creation of these criteria include:

- **Data security** - e.g. independently certified company wide ISO 27001?
- **Privacy** - we recommend that Scottish Government requires accredited attribute store providers to operate zero knowledge platforms, where each citizen attribute store is uniquely encrypted with the encryption key held by the citizen,

so that the attribute store provider cannot 'see' the citizen's data and cannot exercise any control over its sharing or use.

- **Trustworthy business model**. Attribute store providers should not have financial incentives to monetise citizen data or otherwise influence its sharing or use. Financial incentives need to be aligned to enabling citizens with tools that enable and empower them in the use of their own data.
- **Mission commitment**. What safeguards are in place (legal or otherwise) if/when an attribute store provider goes bust, is merged with or acquired by another party? It is not a strong enough safeguard that an attribute store provider has a 'policy' to protect and empower citizens if this policy can be changed at will by a new CEO, Board or owner. The commitment to protect and empower must be strong enough to survive such changes. One example of this is the legal mission protection provisions of Community Interest Companies that do not allow the sale or acquisition of the CIC's assets to another body which is not equally, legally committed to the mission upon which those assets were built.

  In line with this, Scottish Government should consider if a company created with the expressed purpose of 'selling up' at some future stage is appropriate to act as an attribute store provider.

Potential benefits and risks

The potential benefits are significant and across multiple dimensions and link directly back to the National Performance Framework. Appendix A: Analysis of Potential Benefits of a Smart Entitlement Strategy analyses, in detail, potential benefits for five key stakeholders: citizens, public and third sector service providers in their roles as attribute providers and relying parties, Scottish Government and the wider society. It identifies 15 different types of benefit across these different stakeholders.

The include reductions in friction, effort, risk and cost, improved outcomes/service quality, increased operational delivery capacity, increased equality of access to services, improved citizen wellbeing, citizen and system-wide resilience and adaptability, increased security, easier innovation and improved, lower cost regulatory compliance.

For public services in Scotland, sharing of verified attributes could deliver a system-level transformation in efficiency and effectiveness plus increased ease and timeliness of access for citizens. The net result would be improved outcomes and more effective

delivery of policy programmes across Scotland.

In the longer term, and in the context of the quest for ways to move forward better from the pandemic, by combining the increased sharing and use of verified attribute with attribute stores which build in citizen privacy and data protection, the proposed approach transcends the fundamental privacy between privacy and efficiency/ innovation that is constraining the growth of the digital economy as it relates to personalised digital services.

This is akin to the breakthrough represented by Henry Ford's moving assembly line which transcended the previously unavoidable trade off between volume production and quality. Before Ford, people had to choose between price *or* quality. He made it possible for them to have both. In today's digital economy, citizens have to choose between privacy protection or enriched personal services. What is being proposed makes it possible for them to have both.

Henry Ford's moving assembly line cut the cost of making a motor car by over 90% thereby democratising it, making it inclusive - available to ordinary working people. The approach recommended in this report promises to unleash order-of-magnitude reductions in the cost of service provision while democratising data and making inclusive - placing the power of data in the hands of Scotland's citizens. These underlying economics aspects of the proposed way forward are discussed further in Appendix G.

In terms of timing, these benefits will be felt incrementally, starting small as just a few verified attributes are made available to streamline just some steps in the delivery of some initially targeted services. But increasing returns and network effects kick in as more verified attributes are made available, as they streamline large proportions of service delivery processes (ultimately ending in complete automation of some) and as these attributes are used by more and more service providers to provide an ever widening range of services.

The key underlying point is that one, single structural/infrastructure change has the potential to unlock a wide range of benefits. This is because many of the problems we experience derive from a common source - no longer fit-for-purpose data infrastructure and processes.

The spreadsheet teases out and isolates these benefits for the purposes of clarity and

analysis. However, in reality, they are all likely to be present, to some degree or other, in every transaction and process.

For a Smart Entitlement Strategy to be successful the benefits of implementation must be clear and palpable. These benefits will vary from situation to situation. They include:

- **Financial** - direct process costs
- **Operational**
    - time spent working on transaction and elapsed time from beginning to the end of the process (with knock-on consequences for operational capacity e.g. how much can get done using existing resources)
    - quality, including percentage of tasks fully completed correctly and on time, error rates
    - Risks e.g regulatory risk, reputation risk, health and safety risk
- **Emotional** - what emotions, both positive and negative, those involved in the process on both sides feel as they go through the process.

Most benefits are measurable

Most (but not all) of the benefits identified are measurable either directly or indirectly (e.g. through quantitative and/or qualitative) research. Some are not measurable but remain extremely important. For example, we are not aware of any widely agreed, robust, effective measures of system resilience.

Crucially however, while most of the key benefits (such as reductions in friction, effort and cost) *can* be measured, under current business as usual processes they are *not* currently measured. For the Smart Entitlement Strategy to succeed this needs to be rectified. This is because most reporting lines and metrics are:

- based on financial rather than operational metrics
- focus on the performance of 'departments' rather than the completion of end-to-end tasks
- only measure internal costs while ignoring externalities - in particular what cost impacts current service designs impose on citizens

In terms of designing the new Smart Entitlement programme therefore, specific attention needs to be paid to the design, collection and use of appropriate metrics.

This analysis *needs to cover both sides* - both service provider *and* citizen - and needs to

cover operational impacts of administrative processes including:

- time spent
    - looking for information
    - understanding what needs to be done or provided
    - providing the information, including manually keying and re-keying information that could be provided electronically and automatically
    - travelling/physically moving documents from one location to another
    - waiting
        - in queues
        - for documents to arrive
        - for information to be processed
    - redoing all the above in case of errors, incompleteness or dealing with a new party
- money
    - for service providers, the financial costs of paying staff to spend time undertaking the above tasks
    - for citizens, paying for duplicate documents, processes or access to information, for postage and packaging, travelling to offices to present documents

It is important to collect this information a) to inform service design and b) to measure progress.

Risk assessment and mitigation

The biggest risks we have identified are listed below. We have discussed ways of mitigating these risks in each appropriate section.

- **Attribute providers** Resistance to incurring the costs of attribution provision, or fears about liabilities created by doing so (see discussion of liability issue below)
- **Data security** Poor system design, or poor implementation of this system leads to data breaches.
- **Data quality** Poor system design, or poor implementation of this system results in inadequate quality verified attributes being shared e.g. presentation of a driving licence as valid, when the driver was barred from driving yesterday.
- **Citizen** indifference or suspicion from a failure to design processes that are

simple and easy to use and/or from a failure to explain and communicate safeguards and benefits

- **Consent** Consent processes can become a source of confusion and doubt and of administrative complexity and overload.
- **Metrics** Inadequate metrics systems fail to recognise a) costs that are currently being incurred and b) cost reductions that are being achieved because these improvements are lost in noise created by current financially oriented, department-based performance metrics.
- **Bad actors** Bad actors providing a component of the conceptual architecture are a constant threat. The most important mitigations of such risks are independent certifications and external audit e.g. ISO 27001, tScheme

The liability issue

In our experience one of the most common claimed reasons for service providers refusal to engage in the creation, sharing or use of verified attributes is uncertainty about who will be liable for what should something go wrong, for example is an individual forwards a verified attribute that is wrong, through no fault of their own and the service provider makes a mistake because of it.

There are two answers to these liability concerns. First, the system needs to be designed to minimise the possibility of them occurring. Second, all parties need to recognise the realities of liability and service provision *as they exist today* and to recognise that what is being proposed is no different (in fact, many ways better) than how our systems currently work.

The current approach is one of risk management based. For example, when a human being inspects a document, that human being is making a judgement as to whether: they think the document is real, whether the person in front of them looks like the picture in the document, etc. Credit reference agencies do not promise 100% accuracy. They only offer percentages of accuracy so users of credit reference agency data have to make a judgement as to whether to accept the risk implied by the percentage or not. Sometimes service providers make checks against white lists or black lists. But there is no 100% guarantee that these lists are 100% accurate and up to date.

In other words, all current processes have risks associated with their use, and these risks are managed by a mixture of risk reduction techniques *coupled with judgement*. The proposed Smart Entitlement Strategy is no different - except that the processes that it

creates are designed to, and are likely to, significantly reduce risks by creating new mechanisms (e.g. persistent API links and secure electronic tokens that are verified attributes) for the avoidance of error and fraud.

When errors or shortcoming occur (as they will) the issue is not 'liability' but remedy. Any attempt to create liability models with financial penalties can only increase the costs of system operation. The crucial issue, operationally speaking, is to be able to identify errors and shortcomings as they occur - via processes focused on continuous improvement - and to immediately address any harms that might have resulted. For example, if a citizen has been underpaid a benefit, then monies need to be made up. If they have been overpaid they have to repay the money. And if the transaction was fraudulent, those involved are liable to criminal prosecution.

Liability is a very important consideration in terms of designing systems and processes that work well to reduce risk. It is not an excuse not to act.

Implementation issues

Addressing the collective action problem

One of the biggest obstacles to successful implementation of a Smart Entitlement Strategy is that ensuring the provision of verified attributes represents a collective action problem. When acting in their role as 'relying parties', every service provider wants to be able to access the right, reliable information (verified attributes) quickly, easily and cheaply. In this role, they want other organisations holding these verified attributes to make them widely available, securely and cheaply.

However, the same organisations in their role as attribute providers may be reluctant to make verified attributes available. This is for many possible reasons. They may feel that:

- **Cost/benefit**: it is extra work and cost for them for which they receive no direct benefit.
- **Monetisation**: having invested in the collection, storage and curation of such data they should be able to earn a revenue stream from it or recoup at least the costs.
- **Fiduciary duties**: as an activity, provision of verified attributes takes them beyond their fiduciary duties; it is beyond their remit in terms of service provision.

- **Legal risk**: providing verified attributes could open them up to a range of different liabilities relating to customer consent, responsibility for errors
- **Security risk**: any form of data sharing may open their systems up to additional vectors of attack

For these reasons, when asked to support a programme for the provision of verified attributes, most if not all organisations are inclined to refuse (if they can) or to stall and obstruct (if they can't refuse). This has been the experience with multiple other data portability projects including the UK's midata programme.

Yet, at the same time, these self-same organisations stand to benefit from a system of verified attribute sharing, once it is up and running. The more verified attributes are made available, the more every organisation and citizen can benefit from their use. While individual organisations may feel they have few incentives to become attribute providers themselves, they would all benefit from operating within an ecosystem where other organisations are attribute providers.

To be successful a Scottish Government lead Smart Entitlement Strategy needs to cut through this logjam, using a five pronged approach:

1. Establish mechanisms, systems and processes that ensure efficiency and minimise risk
2. Education and communication about the potential benefits of being an attribute provider
3. Changed incentive structures
4. Administrative requirements and orders
5. Reinforcement of legal obligations under the General Data Protection regulations to ensure data portability.

Establishing efficient low risk systems

The rest of this report outlines ways of doing this, so for the purposes of this section we are assuming that this is taken for granted.

Potential benefits of being an attribute provider

While many potential attribute providers may be reluctant to make attributes for the reasons outlined above, there are many potential benefits to becoming an attribute provider. These potential benefits need to be widely explained and promoted.

Resistance to becoming an attribute provider is likely to erode as service providers' awareness of the benefits grows. It is important that these potential benefits are widely communicated. They include:

- **Reduction of distribution costs** Many organisations are routinely asked to provide copies of documents (e.g. birth and marriage certificates, educational qualifications, verification of employment, financial documents). Posting these documents in physical or electronic forms can be costly. If delivered electronically to an individual's personal data store acting as a digital letterbox, both costs and risks can be reduced. If this information is delivered via a persistent link, it can be automatically updated as and when needed.
- **Reduction in effort and cost of cross division, system and domain data sharing within the organisation** Very often, large organisations have data systems and silos that do not 'talk' to each other, where sharing data between them is costly for technical reasons (e.g. interoperability) or risky for regulatory reasons. If the data is delivered to the individual, and the individual re-shares this data to a different part of the same organisation, integration can be achieved while avoiding the cost and complexity of bespoke integration between internal systems and regulatory issues.
- **Regulatory Compliance** Delivering data to a secure personal data store under the control of the individual meets GDPR compliance obligations around data portability, transparency around use, processing, sharing and access by other parties.
- **Liability and Risk reduction** Once data has been shared to the individual, the individual is free to choose what data they share with which organisations. The original data controller is no longer liable for an in-transaction consent step which is required if the data is not shared directly from the original data controller to a third party. By releasing data to a personal data store the service provider can avoid unplanned access to its customer accounts and services as further requests for data go to the personal data store. This has two specific benefits to the organisation:
    - **Reduced cyber risk** Distributing the data to a personal data store means the organisation's servers are not exposed to a growing range of unplanned demands for data from unknown sources, thereby expanding the number and range of potential API attack vectors.
    - **Reduced infrastructure loading** All data is sent on a scheduled basis

over VPN type secure links at the time to optimise capacity usage and done on a trickle feed basis following an initial load. This share once to the citizen approach is much more efficient and secure.

- **Differentiation / value recognition** Helping those you serve get things done elsewhere based on the data you provide to them for use elsewhere can be an important way in which the service provider can demonstrate the value of their association with the citizen. Public and Third Sector represent trust anchors and consistency in terms of relationships with citizens.
- **Demonstrating social responsibility.** The ability to demonstrate support for the National Performance Framework, through enablement to portable verified attributes which underpin many major elements of it.
- **Increased potential access to other personal data** Organisations that act as 'helpful' attribute providers are more likely to elicit reciprocal data sharing by individuals. The best way to 'get' more data may be to 'give' more data.
- **Easier innovation and extension of services** - By distributing the personal data to a personal data store (PDS), new apps and services can be created on a distributed basis where personal data is read and written to the PDS. The only data that is served up via the corporate servers is content and information services which are personalised based on the profile and preferences of the individual and the contextually relevant personal data. Data logistics between organisations' back end systems is handled via secure APIs.
- **Service innovation and improvement** Public Services that have permissioned access to relevant combinations of verified attributes can move to personalised notifications and better delivery of the right content at the right time. The vision of proactive awards and access to service benefits based on the notion of smart entitlements / verified attributes becomes a practical reality while greatly reducing if not eradicating the need for form filling and expensive campaigns and marketing of initiatives.

The communication of these benefits may best be accompanied by public debate/government policies that frame provision of verified attributes as a core, expected element of every service provider's service. Once the public *expects* service providers to provide verified attributes when requested, resistance becomes much harder.

Changed incentive structures

To a degree, the creation of a system for the sharing of verified attributes rests on the resolution of a chicken and egg problem. Once the system is up and running and multiple verified attributes are available for use by relying parties. the existence of these verified attributes would create compelling incentives for organisations to join the scheme.

This can be used to incentivise would-be attribute providers by ensuring that the commitment any relying party must make when joining this scheme would simply be that in order to access verified attributes they also have to provide them: if you want to 'get' data, then you have to be prepared to 'give' it. This requirement should be built into the operational and rules of any new system.

Direct intervention / mandates

However, to create these incentives, the data sharing ecosystem in Scotland has to get up and running.

The best way to do so, we think, is to *mandate* a specific initial set of public sector organisations to make (an initially) core set of verified attributes available to citizens. The effect of this 'mandated first mover' strategy would be to kick-start the workings of the system, make core attributes available, demonstrate the value of the approach, and create incentives for other organisations to join in.

The more other organisations join in, the bigger the incentive becomes for yet others to join. Breaking the logjam in this way should form a key pillar of a Scottish Government Smart Entitlement strategy and should be reviewed and reassessed in the light of experience.

For example, Scottish Government is able, now, to commission attribute provision for all services they are in control of. But Scotland's NHS boards and 32 local authorities all have degrees of legal autonomy. Scottish Government should take a leadership position in this matter to promote the benefits of collective action which can be implemented incrementally with minimum risk and effort.

However, the logjam-breaking action of the Scottish Government in creating the basic digital tool kit of public service provided verified attributes could be decisive in terms of pump priming a self-reinforcing, continually extending nationwide data logistics ecosystem.

The Scottish Attribute Provider Service as proposed in the Attribute Prototype project is a recommendation that can be implemented today and whilst its scope is narrower than the overall recommendations in this paper it would provide the foundation from which this strategy could be implemented.

As can be seen from the research already undertaken communication in clear and plain language is a critical success factor of any proposed scheme. It is important that each stakeholder within such a scheme, service providers acting as relying parties and those also acting as attribute providers coupled with the citizens themselves can see the benefits which are broadly the same but perhaps articulated differently based on their context.

The four opportunities identified in public service data infrastructure are the reductions in Friction, Effort, Risk and Cost, (FERC) all things easily recognisable as desirable by all stakeholders.

Strategy Recommendations

Overview: It's doable, now

Scottish Government has the ability to implement a Smart Entitlement Strategy right now, under its own direction and leadership, using existing resources and under its own control. It does not need to wait for, ask permission of or otherwise rely on other, external organisations and institutions (such as UK Government bodies not under the direct control or influence of the Scottish Government), standard setting and other international institutions, or software vendors/systems integrators. It can act independently, now, with what it has already got.

The following Strategy recommendations are designed to enable this to happen. In our experience effective strategies of this sort need to demonstrate certain core design features, with the right combinations of continuity and change.

- Continuity: They build on existing strengths and opportunities based on what has already been done - they are grounded in *what is*.
- Change: They offer a significant improvement on this status quo while avoiding the risks and disruption caused by attempting to make too many changes too fast.

The recommended strategy below:

- **Minimises dependencies and maximises agency.** The strategy outlined below relies on attributes that can be generated or confirmed directly and immediately by Scottish Government and those it may influence directly in Scotland such as local government. Critically, these do not require the permission or active support of UK Government bodies. It learns from but does not wait for international standard setters to complete complex multi-party standard setting processes. It does not create or depend on long term, multi-billion pound supply contracts with IT suppliers which make SG dependent on their performance.

- **Builds on what already exists.** Verified attributes are already used widely and frequently in the provision of public services. Citizens are required to present proofs about themselves using documents provided by other parties (e.g. passport, driving licence, bank statement, official letter etc) Consumption of proof about a range of factors relating to a citizen are currently risk based assessments undertaken on inspection of physical evidence provided or uploaded and on occasions assertions provided by organisations. Smart Entitlements simply enable the same things to happen digitally, safely and securely in a more efficient manner. They also make it possible to improve risk assessments and confidence in the veracity of claims as they make it quicker, cheaper and easier to access and use a wider range of information points about individuals.

- **Minimises risk and disruption**. The recommended strategy does not require any significant changes to existing back office systems that provide attributes or consume them. It does not require existing organisations to significantly change their processes, culture, operations or systems. Instead, it connects with and integrates into these existing systems adding a new layer of capability, flexibility and opportunity. In taking this approach it minimises disruption to existing operations and builds on existing capabilities.

  At the same time, it can proceed incrementally, taking one step at a time, so that the risks of big leaps into the unknown are avoided. Instead, it allows for a test-and-learn approach that builds momentum and impact over time.

- **Generates compelling win-wins to gain active buy-in**. The recommended

strategy focuses sharply on the compelling win-win for both public/third sector services and their users. By better using information assets that already exist, It provides public and third sector service providers with the opportunity to deliver more, better quality services both faster and cheaper (where cost reductions can be used to increase service delivery capacity). At the same time, it makes it much quicker and easier for citizens to access and use these services, generating better experiences from fewer hurdles, reduced delays, fewer errors and improved personalisation. Given the size of the public sector in Scotland and the number of citizens using its services this is a significant opportunity, and all the key stakeholders have good reasons to contribute to its realisation.

- **Brings immediate benefits that set the right course for the future.** The recommended strategy enables SG to start improving selected services *now*. But along the way, it also builds the infrastructure and capabilities to *further* improve these *and other* services as momentum builds (rather than sacrificing long-term goals for short term gains). In other words, it opens up a road-map for continuing improvement (see next point).

- **Pump primes further developments** that accelerate, deepen and extend this momentum. The recommended strategy identifies a core set of verified attributes and attribute providers that can be targeted immediately to make a significant impact on service provision very quickly. But this initial set of attributes and attribute providers is just a springboard. Once the infrastructure and processes have been put in place, an increasing number and range of attributes and attribute providers can be added incrementally, thereby expanding the number of use cases that can be supported and benefits that can be realised. This is true in the short term, in terms of rolling the approach out to all public services. It is also true in the long term, for example potentially expanding its scope to include private sector services and attribute providers both domestically and internationally.

- **Builds momentum automatically and incrementally** Big change-everything all-at-once system-wide initiatives have a strong tendency to eat up huge amounts of time, money and energy and fail anyway. The recommended strategy is to build the generation and use of verified attributes into the way

existing systems already work, in ways that generate close to zero risk and require minimal changes to current ways of working - but which increasingly embed the new approach into how the system as a whole works, building momentum incrementally over time until it becomes the 'new normal'. *A simple example is that idea of minting digital copies of birth certificates during the certificate creation process, and placing them into the child's attribute store at this point so that from now on, new attributes can be easily added as the child grows up.*

- **Has built in flexibility**. The recommended strategy is not making a bet on a single 'most likely' future. It is able to adapt to and flourish in multiple different scenarios e.g.
    - the UK Government adopting/not adopting a similar approach;
    - large software vendors and systems integrators actively joining/resisting the approach;
    - standard setters succeeding/failing to agree and implement global standards;
    - private sector corporations seeking to join/stay away from the approaches developed by Scottish Government for Scottish Attribute Provider Service.
    - different technologies such as blockchain transforming/failing to transform how data is collected and used or how services are provided

Scotland needs to create and operate an attribute service - the Scottish Attribute Provider Service - the expressed purpose of which is to use the safe, easy sharing of verified attributes to remove friction, effort, risk and costs for *both* citizens and service providers within the public and third sectors in Scotland.

By enabling the safe, secure use of verified attributes under citizens' control it will be possible to reduce delays in accessing services, reduce the burden of proof provision when applying for services, reduce the need for expensive and unnecessary face-to-face meetings (thereby ensuring that those that do take place genuinely add value), enable safe and secure transactions over digital channels, enable automation of routine processes.

To achieve this Scottish Government needs to:

1. **Agree a standard definition/structure for the portability of verified attributes** so that it can be implemented now within Scotland public services. This approach enables the highest levels of interoperability and integration into existing systems and services within the minimum of change to back office systems that provide attributes or consume them.

2. **Enable citizens to accumulate, store, and control the use of the verified attributes about them.** As part of this,
    a. establish standardised processes by which citizens can receive and access attributes from public sector bodies to their attribute store in ways that minimise confusion and complexity and maximise clarity and simplicity. To this end, these standardised processes should use existing and validated approved channels for introduction and initial engagement wherever possible. For example, they should use currently accepted mechanisms for the validation of email, mobile phone and home address, or those used for the MyAccount or National Entitlement Card.

    b. Enable citizens to keep their verified attributes in their own safe, secure attribute store, which enables them to aggregate data about them independently of each and every particular service provider, and to pass on/verify bespoke combinations of these attributes when required to do so for the purposes of service provision.

    c. Enable citizens to have their verified attributes maintained and updated by attribute providers on demand or automatically and have it safely and securely delivered to their attribute store (e.g. via API links).

    As part of this the Scottish Government needs to establish criteria by which attribute stores should be accredited as bona fide destinations for attributes provided by attribute providers. Any future attribute ecosystem should encourage citizen choice in terms of which attribute store services they use. Any future Trust Framework or scheme must set out the standards for involvement of attribute stores and any certifications that may be required.

3. **Establish metadata that provides standardised, easy-to-understand**

definitions of verified attributes and their use in smart entitlements. These definitions need to be unambiguous and precisely targeted to the context of the transactions they are used in. The end-goal is to capture the metadata relating to citizens and their personal data and map this effectively into all public services in Scotland.

Specific areas the metadata standards need to address are:

- Ensuring maximum levels of machine readability avoiding concatenation of data rather dealing with specific attributes and composite attribute structures. For example, machine readable date of birth as opposed to a composite of date of birth, postcode and full address.
- Clarity about levels of assurance about the data, including descriptions of how the data was collected, created, protected and verified. At all times, the standards need to answer the question 'How can a relying party trust that data is or was correct and verified and not modified since generated,in storage or transit?'. Critically understanding if the attribute is being maintained and updated and how long ago it was verified.
- Clear, standardised processes and procedure for accessing attributes. Any proliferation of such processes and procedures risks creating a complexity catastrophe where, the more usage grows, the more confused and complex ways of making it work become.
- Clarity about the nature of the attribute. Is it a single root attribute from a trusted attribute minting body? A secondary attribute *verified by some form of inspection process that verified that a root attribute has been checked by a third party*. Provision needs to be made for data minimising and zero-knowledge uses of data. For example, in relation to 'address' different services may require different levels of information e.g. verification that the individual is on the electoral register of a particular local authority, verification of the individual's postcode, or verification of their postcode *and* road/flat number.

4. **Establish a directory of attribute sources.** Such a directory would not hold the data itself, but provide the routing to that data along with information relating to the nature and type of data that is available. In the long term this directory

should list all of the personal data held by Scottish Government and where this data is held. It should also specify what level of assurance relates to that data (for example, was it generated for the purposes of an email newsletter or to verify a person's identity? Such a directory can be used by service providers to signpost citizens to where they can obtain the attributes they need to complete specific applications and other processes and eradicate duplication of effort and form filling and speed things up.

In developing this directory, attention needs to be paid to attributes' source and provenance. For example, many widely used attributes may be minted by the UK Government's Department of Work and Pensions, which the Scottish Government has no control over. However, it may not be necessary for DWP itself to make these attributes available. Via the Employee Authentication Services project, local authorities, other organisations can look up attributes held by DWP relating to citizens. This enables local authorities to act as providers of these attributes but only if provided directly back to the citizen. Similarly, in order to qualify for a National Entitlement Card citizens have to show their passports if they have one, thus verifying an attribute minted by another UK body, the Passport Office.

In such cases, the directory needs to list where service providers/citizens can most easily and practically access the attributes in question. This won't always be the same as the original attribute minting organisation. In making this listing, the directory will also need to make clear how, and on what basis, the attribute in question remains up to date and valid (e.g. is updating automatic, periodic or occasional?)

5. **Establish easy-to-use and understand consent processes and mechanisms that maximise citizen control and minimise citizen effort**, while enabling safe, efficient data sharing. Citizens should be able to easily control, reflect on, choose and modify how their attributes are used. These consent processes and mechanisms need to be flexible and appropriate. Strategically in the longer term, wherever possible citizens should be able to specify a generic consent policy that gives automatic consent if the data in question is used only for the provision of the service requested and not for any other secondary use or for use by any other party, and that they are happy for attributes to updated by agreed processes when needed/appropriate.

6. **Establish open reusable mechanisms and processes for the consistent, incremental generation and verification of attributes that citizens use to build up an ever more detailed picture of themselves** along with *increasing confidence* that the data that is held about them is correct.

   National Records of Scotland provides a good example of the opportunity for consistent incremental enrichment of attributes. Currently NRS does not have a direct relationship with the citizens the records relate to. For example, it did not mint the birth certificates it holds. Furthermore, anybody can ask for a copy of anybody's birth certificate. While NRS may process a request from a person asking for a copy of a birth certificate and may collect some basic information to complete the transaction, that birth certificate does not have to relate to the person seeking a copy.

   However, if a school student has a recognised official relationship with their teacher, and the teacher vouches that a birth certificate relates to that school student, then the birth certificate becomes linked to the individual. Via a process of vouching the level of assurance about the data point is increased.

   Most interactions and transactions requiring the sharing data have this dual - rather than single - role. In this case, the pupil is asking the teacher to help them apply for a National Entitlement Card. But at the same time, the same interaction/process can also be used to round out and enrich the verified data that is held about that pupil at close to zero cost.

   The incremental enrichment and extension of the available bank of verified attributes can grow almost automatically by piggy-backing off existing processes. Such additional 'piggy-backing' data capture and verification processes need to be built-in to all public sector data processes so that the new personal - and national - data asset of verified attributes reaches critical mass in terms of volume, scale and richness as quickly as possible.

7. **Establish a consistent, long-term communications campaign to inform, and incentivise and educate the public about the verified attribute/smart entitlement programme**, its benefits, and how to access and realise them, so that over time every citizen can use them as automatically and instinctively as they currently use their mobile phones. Ideally, wherever a data-related process

involves the collection or sharing of personal data, citizens should be provided with an opportunity to add this data to their attribute store; or at least some awareness raising or explanation should be embedded into the process (even if it is only a short sentence or a link). For example, the forthcoming Census 2021 could be an opportunity to invite every citizen in Scotland to add the data they provide into their own attribute store and create a persistent connection between their attribute store and the census.

8. **Establish metrics systems and processes** to support and guide future steps of the programme. As explained above in the section on Potential benefits and risks most of the KPIs underpinning an effective Smart Entitlement Strategy relate to operational factors, covering arenas such as time spent on different steps of an information process. These are metrics that most organisations do not currently collect.

   Moreover, many of the intended and actual benefits of a successful Smart Entitlement Strategy will not be felt by the organisation at all - but by citizens, e.g. in terms of reduced time and effort invested in trying to access and use public services, reduced emotional costs (e.g. frustration, anxiety) and increased emotional and wellbeing benefits (such as sense of effective agency and confidence). Again, this data and information is not currently routinely collected by service providers - and needs to be in the form of operational metrics and citizen report outcomes and experience measures.

   To measure the benefits of this programme and demonstrate its effectiveness this data needs to be collected, and standardised methods for the collection and analysis of this data need to be developed. Without these metrics, resulting benefits will only be measured indirectly and potentially lost in the noise of other factors affecting overall financial costs of operations.

   The added plus of developing this broader, richer metrics system is that it aligns perfectly with the wellbeing goals of the National Performance Framework and *could become one of the first ways in which these goals are practically operationalised* - i.e. in identifying palpable, demonstrable ways in which citizens' wellbeing is being improved.

9. **Build a public services monitor that analyses transaction volumes and costs of all public services**, including average length of application process, burden of proof required to complete application and operation of service. The specific purpose of this is to help prioritise the targeting of attributes and services for adoption, but it can also be used as a general yardstick of progress for digitisation of Government services and degree of cost reductions achieved.

Strategic roadmap and immediate next steps

While the paragraphs above describe the end-goal in terms of capabilities and outputs, a key requirement of this Strategy is that it offers immediate, practical opportunities for improvement. For this, a prioritisation and gating framework is required.

1. **Establishing standardised metadata**. Scotland needs to develop its own standards for attributes. This is for two main reasons. 1) It cannot afford to wait for other bodies to do so (it could take decades). 2) It needs to be in control, ensuring that the standards are fit for its purposes.

   It is possible to learn from and link to other parties' efforts to establish related standards (such as those of WC3). But it is important to avoid dependence on them. Once Scotland has developed its own metadata standards, adaptors can be developed to make sure that they are interoperable with other metadata standards built by other bodies.

   As a workstream, this needs to begin immediately.

2. **Prioritise the most important attributes** Some sort of 80/20 (or 90/10) rule applies to verified attributes. Some attributes will be required for a large number of transactions others only rarely, for highly specialised purposes. Yet other attributes may be substitutable - if this attribute is not available, another could be used in its place.

   To make rapid progress, the initial focus of the Smart Entitlements Strategy should be to identify which attributes are the most important. Criteria for this ranking will include:

   - **Volume demand for attribute:** how many times does it need to be used? (The only way to create a complete, comprehensive picture of

demand for verified attributes is to view demand for the total set of services from the point of the view of the citizen: which verified attributes will be most helpful to most citizens in accessing and using most services?)

- **Frequency demand for the attribute:** how often does it need to be used?
- **Benefit to stakeholders of availability:** The degree to which availability of the attribute in terms of reducing cost, risk, friction, reducing delays for citizens and service providers.
- **Relative importance of the service:** to the achievement of public policy
- **Ease of access:** Are the systems in place capable of serving the attribute up today or with relatively small amounts of work? Is there a pre-existing or easy path to making the attribute available to the citizen? For example, if the data is already being processed by a data hub, it may represent a more fruitful and quicker win than if new processes have to be created for access and delivery.
- **Ease of creation of correct metadata:** and including ease of assessing the veracity and provenance of that data
- **Assessment of the level of confidence about the source of the attribute:** Is it recognised today as being a reliable source of attributes and attribute verification? For example, the National Entitlement Card process already defines how a citizen gets their card and what attributes need to be verified and in what manner, so the attributes used in this process already have a degree of verification. The same can be said for educational qualifications issued by SQA. While there are a number of recognised standards for inspection of documents their application is not consistent. This needs to be assessed: at all times ensuring confidence in the attribute is key

NB. It is *essential* when assessing these criteria that the needs of *both* citizens and service providers are taken into account. Some processes impose few costs on the service provider but many costs and effort on the citizen, and vice versa.

Failure to analyse both will create a distorted set of priorities. Ideally, first applications should bring clear, palpable benefits to both sides.

3. **Prioritise the most important attribute providers** A relatively small number of attribute providers will be able to provide a high proportion of all the attributes needed for a Smart Entitlements strategy to be effective in Scotland. A much longer tail of other attribute providers will provide the rest. Scottish Government needs to prioritise bringing the small number of anchor attribute providers on board.

4. **Identify a critical mass of initial use cases** that offer mutual benefit to citizens and service providers alike. The National Entitlement Card is a clear candidate as it already reaches most young people plus older citizens entitled to receive concessionary travel. Using the NEC would be a way to reach the core 'target market' for verified attributes quickly and in one go.

5. **Develop a public service data directory** The ultimate goal is to establish a data directory that enables every service provider and every citizen to quickly and easily identify, find, reach and use every single one of the attributes they might need for every possible service at every life stage.

   Ultimately, this directory should hold metadata about every public service in Scotland, describing the data required for the completion of every single service. Viewed across all services, this directory would list 'all the data you will ever need' to access and use public services. But this ultimate goal can and should be approached incrementally. Initially, the development of the public service data directory should relate directly to the prioritised attributes and attribute providers. The data directory can then grow organically as new attributes and new attribute providers come on stream.

   Developing this metadata capability and related data directories is the responsibility of Scottish Government. As a work stream it needs to be carefully designed and adequately resourced. For example, service designers need to be trained to publish information describing to citizens, in advance of their beginning an application process "this is the data you need to complete this process and this is where you can get it from".

The process of developing this metadata capability and related data directories will require careful management. Who will be consulted? Who will be informed? What powers will they be given to who, to do what? How will these powers be exercised and enforced?

6. **Establish a set of certification standards for connectivity to attribute store providers and a Scottish Attribute Provider Service.** For attributes to start flowing, citizens need to be able to access them and store them in their attribute store. What key criteria should such attribute store providers meet to be recognised as bona fide? What rules and standards should apply to the connections made between attribute providers and attribute stores?

   These criteria need to be established early on if the system is to deliver quick wins. As discussed in strategy recommendations and risk assessment and mitigation sections considerations include security, privacy and trustworthiness.

7. **Extend the Scottish Government's Digital First Service Standard** so that any new service being developed must take into account of, and design in, what it takes to enable attribute provision and attribute consumption.

8. **Interpret and implement GDPR to clarify that citizens have a right to obtain copies of verified attributes about themselves.** GDPR does not explicitly mention "verified attributes" in its provisions for rights to data portability and to subject access. This creates some areas where different interpretations might be possible (see Appendix). However, the spirit and intent of the legislation is clear and for the avoidance of doubt the Scottish Government should make it clear that for all services it is in control of, and for participation in the Scottish Attribute Provider Service, it is interpreting and implementing this legislation in such a way that verified attributes are included under data portability as well as subject access rights.

9. **Establish mechanisms to embed attribute creation and provision into all standard administrative processes.** Existing services should also be reviewed to see how they can be adapted to accelerate the momentum of the Smart Entitlement Strategy as a whole. For example, if a citizen's attribute store was created as part of the process of minting a birth certificate, with a digital copy of

the birth certificate going into the citizen's attribute store, over time, every single citizen would be automatically provided with their own attribute store. The same could apply to other certification processes. For example, in creating records of examination results the Scottish Qualifications Authority could automatically populate citizens' attribute stores with digital copies of these certificates as they are being minted.

This incremental approach to the enrichment and extension of the data asset minimises the need for significant, expensive additional data capturing or sharing activities, and instead embeds the creation of verified attributes into everyday data processing activities - creating a 'new normal'.

By adopting such an approach it would take a minimum of 18 years to have the entire population covered. Other processes such as those of immigration, marriage, divorce and death should also be added as quickly as operationally possible.

Appendices

Appendix A - Stakeholder analysis and benefits matrix

We have created a stakeholder matrix looking at who they are and their incentives and motivations for participation and overall value to any Scottish Attribute Provider Service. There are some 47 different services and possible sources of verified attributes, many storing the same attributes for different purposes at different levels of assurance.

We have also created a stakeholder benefits matrix that looks at benefits through the lens of each stakeholder. The same stated benefit may resonate with different stakeholders for different reasons.

ANALYSIS OF POTENTIAL BENEFITS OF A SMART ENTITLEMENT STRATEGY Public and third sectors					
	Citizens	Attribute Providers	Relying parties	Scottish Government	Wider Society
A consistent means of delivering and presenting proof	Citizens are able to prove specific things about themselves in order to get things done e.g. proof of identity, address, age or benefits currently on	Easy means of producing and publishing verified attributes	Easy means of consuming proof points in a consistent manner regardless of source	Ability to map policy to underlying requirements of proof and plan for easier implementation, reducing the time and cost for public services and service providers	A society where trust is built into processes and context of transactions in a consistent manner
Reduce friction	Reduce the time citizens have to taken to find the information they need and to present it, e.g. when filling in forms and undertaking application processes. This often extends the time take to complete a task	Reduce time spent fulfilling multiple requests for information using existing manual processes	Reduce the delays created by self- asserted that data needs to be checked, often manually. Reduced turnaround times improve customer experience, reduce cost to serve (see below) and increase delivery capacity (ability to serve more people using same resources - see below)	Implementation of policy made easier as these sources of friction are removed.	Citizens and organisations feel it is 'easier to get stuff done'
Reduce effort	Reduce the effort of the above plus massively reducing the duplication of effort required in providing the same information to different people/organisations or different parts of the same organisations, or at different times.	multiple requests for confirmation of status of individuals they serve	initiatives can be implemented more quickly and easily. No duplicatin of effort net effect much more efficient, response set of public services, better reputation. Sensitive categories DBS checks, evidence of activities. Audits - significant amount of monitoring that has to happen. At moment its a manual exercise.	easier implementation of policy	time freed up to do other things! freeing up resources.
Reduck risk	Reduced risk of missing out on services they are entitled to or of being treated unfairly. Reduced risk of making mistakes (e.g. providing wrong information or providing wrong consents). Problems avoided from faster access to services that are needed- prevention.	making mistakes - info generated out of systems, not manually produced; of cyber attack	application, onboarding, service provision for fraud, error, and service failure, of cyber attack	misuse of public funds, failures of initiatives and policies especially in times of crisis e.g. pandemic. Reduced risk of inequality.	
Reduce cost	travel costs, service fees	request costs for multiple confirmation requests, infrastructure costs of multiple access requests to systems	Staff costs for processing and verifying data	improved ops efficiency, reduced demand on public purse.	reduced demand on public purse.
Improved outcomes	faster access to services you need, increased wellbeing -		initiatives can be implemented more quickly and easily. No duplication of effort net effect much more efficient, response set of public services, better reputation. Sensitive categories DBS checks, evidence of activities. Audits - significant amount of monitoring that has to happen. At moment its a manual exercise.	easier implementation of policy and achievement of intended outcomes	
Increase capacity	citizens empowered, enabled, equipped; time freed up to do other things	less demand on infrastructure and staff resources fulfilling info requests = increased capacity	from line teams' capacity to handle higher volumes of cases significantly because much of the admin and checking of data is reduced. Reduced admin = increased focus on actual service delivery	increased opportunities to implement policies faster and run concurrent programmes due to eradicate duplication and repetitive processes	No delays
Increased equality of access	once a person is set up the PDS is working while they sleep. People who aren't digitally enabled, or visually impaired. Cognitive burdens on say, visually impaired, is greatly reduced. Freed up resources can be repurposed to help those less able to cope.	Easy to implement process to ensure citizens have access to the info they are entitled to.	Being able to make use of consistent user experience for gaining approval for, access to and use of personal data, thereby enabling streamlines citizen journeys, increasing take up and sign up rates from digital channel.	Ability to define and implement policies and programmes that will drive higher adoption rates across full demographic of the population	No one left behind, no one excluded

ANALYSIS OF POTENTIAL BENEFITS OF A SMART ENTITLEMENT STRATEGY Public and third sectors					
	Citizens	Attribute Providers	Relying parties	Scottish Government	Wider Society
Increased wellbeing	It is easier for people who are entitled to services to obtain them. Negative emotions of undertaking these processes are reduced, and positive emotions increased. For citizens, an increased sense of coherence and empowerment about their lives.	reduced number of customer service requests and complaints from citizens; reduced burdens/stress on customer service staff, including for Subject Access Requests	reduced number of customer service requests and complaints from citizens	easier access to services delivers improved wellbeing in two ways: 1) improved access to services/increased volume, 2) reduced costs and stress for citizens in accessing and using these services.	A safer, easier more integrated place to live and work
NPF	Opportunity to create comms programmes which visibly and map and demonstrate process on delivering of NPF underpinned by smart entitlements and verified attributes.	Ability to demonstrate support for NF thorugh enablement to portable verified attributes which underpin many major elements of it.	Ability to demonstrate support for NF thorugh provision of services enabled byto portable verified attributes which underpin many major elements of it.	Moving from articulation of ideals to progress that is measurable. Establishment of invastructure and processes that enable operational delivery of NPF goals without duplication of effort.	More supportive, equal society
Increased resilience	meeting new challenges and life events more easily and ably; being able to transition between life stages with less stress and disruption; better able to respond to new or changing policy requirements	Being able to respond to new information requests in a consistent and stable manner; to avoid having to create customised solutions to new requirements via already-established attribute provision systems and processes	Able to adapt and choose services to meet changing needs within mamumum amount of disruption for those they serve, without extensive service redesign	Able to envisage new policies and fine tuning of existing policies, and to introduced them with minimum amount of disruption, waste and duplication.	a profound and established understanding of how information flows and can respond to broader needs of society
Increased agility and adaptability	Ease of adoption or switching from one service to another without the burden of migration or reentry of information		The ability to quickly and easily configure and reconfigure service provision, and to work with other relying parties to deliver new services as and when needed	The ability to develop and implement policies and programmes that take quicly and easily configuration of service provision based on reliable information for granted. Ability to use a platform that enables relying parties to work together to deliver new services as and when needed. The ability to respond more effectively to unforeseen circumstances requiring personalised services at a national level.	As a nation, we can respond to changing circumstances with greater easier a) because with an infrastructure that enables verified attributes to flow, minting new attributes (e.g. Covid 19 test results) is easy and cheap to do at scale b) because the infrastrture enables easier faster innovation (see below)
Increased security	control of and access to the data about their lives, and a means of controlling its use. Reduced risk of hacking because of the distributed nature of the architecture.	Large scale databases and back end systems are no longer exposed to the Internet and APIs from third parties thereby reducing risk of cyber attack. They have unique connections to individuals about specific points of data.	Large scale databases and back end systems are no longer exposed to the Internet and APIs from third parties thereby reducing risk of cyber attack. Reduced fraud rate through corruption of verified attributes over secure APIs, thereby reducing potential to game the system and make false statements.	The ability to have a trustworthy ecosystem for proofs of claims reduces threats and risks across Scotland.	Increased trust, from use of public services.Reduced numbers of scams.
Increased opportunities	When it is easy to apply for services, more citizens will do so. Potentially automatic access to services increases opportunity to be served as needed.	Ability to deliver value adding services and information to citizens along with new means of meeting regulatory compliance obligations	Ability to introduce new services quickly an efficiently with minimu of effort required from citizens	Better able to envisage how policy objectives could be implemented and innovative approaches to policy programmes	Ability for wider society to imagine new ways of working driven by ease of access to the information needed to implement an end to end solution
Easier innovation	Ability to enjoy the benefic of innovation made possible by creation of new never-seen-before data sets	Backend systems can be updated and migrated against their own unternal programme plan by maintaing standard external interfaces	Creation of new never-seen-before data sets enable innovation of new never-seen-before services. Automation of processes enables provision of service automation - e.g. automatic service provision to those who are entitled to it, without the need to market these services, or require forms to be filled in	Ability to create new policy programmes with the assurance of the information needed to implement them being readily available and the infrastructure to distribute in place	A more innovative economy as social and commercial entrepreneurs can use data directories to identify opportunities and ways of seizing them, using infrastructure for data sharing and access that is already available.

ANALYSIS OF POTENTIAL BENEFITS OF A SMART ENTITLEMENT STRATEGY Public and third sectors					
	Citizens	Attribute Providers	Relying parties	Scottish Government	Wider Society
Improved value recognition/ satisfaction	Increased sense that public services 'are working for me'. An increased sense that it's easy to apply for things, 'so I may as well'.	Being seen by citizens as being helpful and making it easy for them to exercise their rights.	improved rates of satisfaction, higher take-up rates and improved customer retention (where relevant), improved trust and reputation.	Closer alignment and understanding of how government policy is helping and can be more easily monitored and tracked through tangible evidence of information flows and adoptio rates	Improved citizen sense that society's services are working for me and making my life easier builds trust and cohesion
Compliance	Ability to exercises rights under the law easily, safely and securely and gain value from doing so	Meeting regulatory obligations more easily, more security and with less time and cost and effort in the design and development of approach	Be able to demonstrate informed consent, data minimisation and transparency about how data is being used within a service and minimise the risk from sharing personal data	To design policies and programmes that are compliant from the start and maximise the potential to increase trust and confidence and reduce the burden of service design	Increased trust and confidence in public services through transparency and consistany in approach that empowers citizens to be active participants and in control

Appendix B - Verified attributes matrix

The range and diversity of verified attributes that would be the foundation of a smart entitlements strategy are diverse and readily available in Scotland. As part of the project we have built a matrix to assist in the analysis of attributes of value and availability. They can be broken down into a number of categories

- **Specific single attribute** - Examples are date of birth, place of birth, parents name and address
- **Composite attributes** - A collection of attributes that together provide a verified document or attestation, e.g. Birth Certificate (date of birth, place of birth,

parents names, nationality and name of registrar recording the birth and the location of registration) or home address (name of verified individual, verified address, the date from and too at that address, where and how verified that the individual resides at the address). Other examples are driving licence, employee ID card, work permit, passport, DBS certificate, bank account details etc.

- **Derived attributes** - a value generated from either a verified single or composite attribute that can provide a confirmation of something such as verified age today, does have a bank account, does live at an address, does hold a valid driving licence or passport is legally allowed to live and work in Scotland etc.

Unique Identifiers are a special case in point, developed to ensure that data is correctly linked together and tracked with organisation systems and services but also used by citizens to ensure they are correctly identified along with other single and composite attributes e.g. CHI number coupled with date of birth and home address

Smart Entitlements can be generated to reflect either a composite attribute or one or more derived attributes. Examples are

- a benefit entitlement statement containing details of entitlement (composite attribute) or
- confirmation of being on a specific benefit or a specific value of monthly value of the benefit or the date it starts, ends or is reviewed (derived attribute).

Smart Entitlements can be made up of single attributes, composite attributes and derived attributes as well as creating new attributes such those that demonstrate the process of generating them and the steps taken to complete the assessment of entitlement including vouching or professional reports relating to an individual.

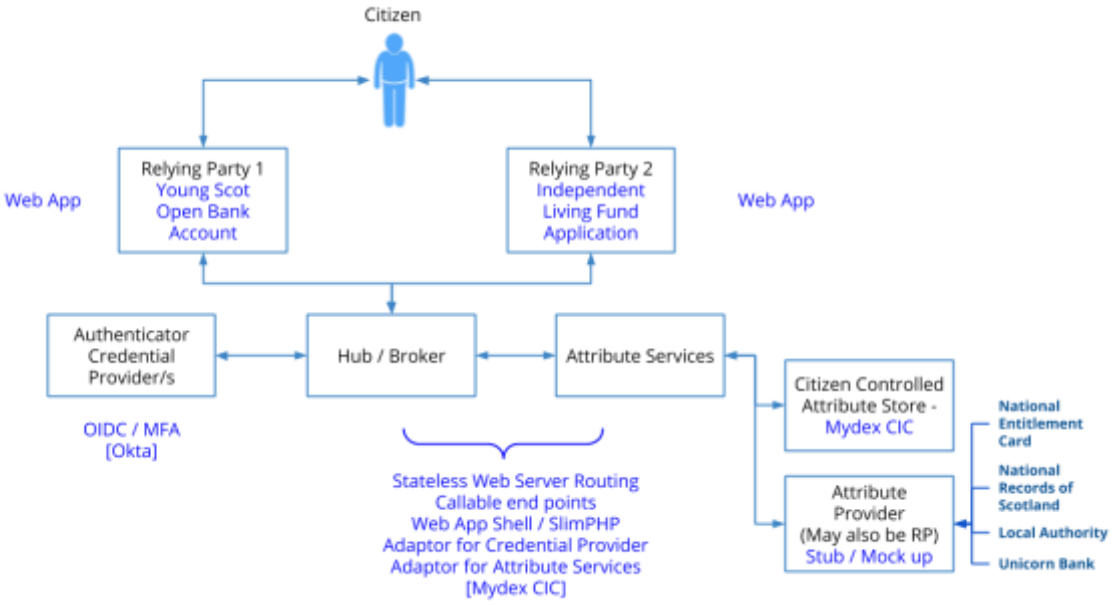
The recommendations for Smart Entitlements Strategy includes agreeing the metadata to describe verified attributes, a cross mapping of verified attributes to sources of the attribute and where those attributes are most likely to be consumed in public services.

This will aid in the prioritisation and focus of initial targeting of verified attributes and sources that can pump prime the Scottish Attribute Provider Service.

Appendix C - A Scottish Attribute Provider Service

The Attribute Prototype project delivered a series of outputs which can be viewed as the rails on which a Smart Entitlement Strategy could be implemented. The concept of a Scottish Government Attribute Service provides the rails on which smart entitlements (verified attributes) can flow safely and securely. The following deliverables from the Attribute Prototype project are

- **A working prototype** of the conceptual architecture including a stateless hub/broker, a credential provider, citizen attribute store provider and two relying parties both retrieving and delivering verified attributes from and to a citizens attribute store.



- **A Final Report for the project** including specific recommendations for next steps and implementation
- **Technical and Security Architecture** - Attribute Prototype
- **Data Protection Impact Assessment** - Attribute Prototype

Appendix D - GDPR and Verified Attributes

Do new European data protection regulations on data portability give citizens the right to receive copies of verified attributes?

The new European General Data Protection Regulations introduce a new right to data portability (Article 20) in addition to the long standing right of 'Subject Data Access' (Article 15).

The two Articles use different terminology relating to different requirements, creating potential grey areas of interpretation and implementation.

Article 20.1 says:

"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
>
> (b) the processing is carried out by automated means."

For the purposes of provision of verified attributes, the key words here are "which he or she has provided to a controller". Some may argue that verified attributes are not 'provided' by the citizen to the controller and therefore do not fall within the requirements of Article 20 (Data Portability).

However, Article 15.3 ('Subject Data Access') is much broader, saying "3. The controller shall provide a copy of the personal data undergoing processing" (e.g. whether or not the data was 'provided' by the individual). Verified attributes are indeed 'personal data undergoing processing' so, whether or not they are deemed to be covered by Article 20 on data portability, they are covered by Article 15: the citizen has a legal right to a copy of this data.

In considering interpretation of these clauses, the Article 29 Working Party (now European Data Protection Board) ruled as follows:

> "The right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject for example, on an online form."

By including the phrase 'personal data generated by his or her activity' the Article 29 Working Party has clarified that Article 20 is not narrowly restricted to only data 'provided' by the individual. Verified attributes could be interpreted as being part of the data 'generated by' the individual's activity.

However, so far, the Article 29 Working Party/European Data Protection Board has never *explicitly* addressed the specific case of verified attributes and its other rulings could be interpreted as *excluding* verified attributes from rights to data portability.

Specifically, the Article 29 Working Party ruling goes on to say:

> "Inferred data and derived data are created by the data controller on the basis of the data 'provided by the data subject'. These personal data do not fall within the scope of the right to data portability. For example, a credit score or the outcome of an assessment regarding the health of a user is a typical example of inferred data. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right."

Clearly, verified attributes are not 'inferred' data. But could they be seen as more 'derived' than 'generated' and therefore *not* covered by Article 20?

The detailed nuances and implications of these different wordings with their potentially different interpretations can only be tested in courts of law. However, for the purposes of a Smart Entitlement Strategy, recognising the potential grey areas and confusions, it is important that Scottish Government makes a clear and explicit decision that it is interpreting the spirit and intent of GDPR to mean that citizens should have a right to obtain copies of verified attributes minted by organisations in a structured, commonly used and machine-readable format.

The formal Justifications for such a decisions are that:

a) Whatever the strict interpretation of the words of Article 20 (e.g. 'provided' by), under Article 15 the citizen has a right to a copy of this data.
b) The exclusions identified by the Article 29 Working Party relating to 'inferred' and 'derived' data are intended to address data controllers' concerns relating to

proprietary *analysis* of the data they hold, not the data itself.

c) In order to achieve the goals of improved public services at lower cost, it is the provision of verified attributes that is key. It would therefore be illogical for one party of the public sector to incur costs and for another part of the public sector to incur the same costs when there is a simple mechanism to transfer the data via the citizen at next to no cost.

Appendix E - Consent: what are we trying to achieve and how?

To succeed, the Smart Entitlement Strategy needs to cope with multiple design and administrative challenges thrown up by our current reliance on the concept of, and mechanisms relating to, the operation of citizen consent for data processing.

Many people now assume that 'consent' is required every time an organisation or service collects or uses personal data. This is not true. GDPR has many different definitions of what makes the processing of personal data lawful. One of them is the processing of data necessary for the provision of a service. When this happens *no consent is required - if*, that is, no other data is processed (data that is not necessary for the provision of the service) and if the data is not used for any other purposes.

Consent only became a ubiquitous 'must' for a combination of two reasons.

1) Lawyers' risk aversion. Just in case somebody argues that a particular piece of data or a particular piece of data processing was not strictly necessary for the provision of the service, why not add consent as well, as a belt-and-braces catch-all.
2) By asking for consent, and wording this request in a lengthy, obscure document such as a privacy policy or terms and conditions, companies could get citizens to consent to data processing that went far beyond what was strictly necessary for the provision of a particular service.

This created a complexity catastrophe, with each new privacy policy 'hand crafted' to deal with a particular organisation, service and customer. (For a discussion of hand crafting see Appendix F below.) It duplicates cost exponentially, imposing high administrative and operational costs on service providers and equally high cognitive and administrative load on individuals who, in order to access the services they want, are expected to read, digest and fully understand long tracts of legalese.

The resulting complexity has created room for large scale cynical gaming of the system where the consent process is regularly used as a (largely underhand) mechanism to obtain 'consents' for data processing that goes far beyond what is necessary for the provision of services: it has become the mechanism to achieve a data landgrab, pursued as a means to monetise individuals' data rather than serve them.

Faced with the overwhelming effort needed to read, understand and act on every privacy policy they are presented with, most consumers/citizens have lapsed into learned helplessness, resulting in endemic loss of trust and cynicism about how persoal data is collected and used.

None of this is necessary. In our view, specific bespoke processes for consent provision should be the rare exception, not the rule. For the vast majority of services three simple, universal, automatic 'safe-by-default' rules can, and do, cover most situations. They are:

1) Only collect the data needed to provide this service, and no more
2) Only use this data for the purpose of providing this service, and nothing else
3) Don't share this data with anyone not involved in providing this service.

Please note: such a 'policy' is not one written by an organisation's lawyers. It's assumed stance is that of the citizen - it is an expression of the citizen's requirements.

When we talk about 'consent' for the purposes of a Smart Entitlement Strategy we are talking about the exact opposite of the sorry state of affairs described above. The purpose of consent in the proposed Smart Entitlement Strategy is to make it as quick, easy and simple as possible for citizens to exercise genuine control over how their data is to be used. This is a design challenge, not a legal or compliance challenge. It is about designing processes that are a) first and foremost designed to protect rather than take advantage of citizens and b) quick, easy and simple - echoing the goals of the Strategy as a whole, which is to empower individuals with their own data and help them use this data to access services in ways that eliminate friction, effort, risk and cost from their lives.

Consent mechanisms that fit this approach are likely to display three characteristics.

1) **They are Safe By Default.** Once data is held in an Attribute Store, none of this data can go anywhere without the individual's expressed permission. If service providers seek access to an individual's data, the Default expectation is that they

will only seek to access and use data that is strictly necessary for the provision of the service in question. It will not be used for any other purposes. It will not be shared with any other parties (as above)

2) **Consent as a policy**. It should be possible - administratively and practically - for individuals to set common base line terms for giving consent that organisations can access, agree to and confirm without the individual needing to duplicate effort or undertake any extra work. The Smart Entitlement Strategy should establish mechanisms to enable this to happen.
3) **Dynamic consent**. Where further granular consent is required for specific, exceptional situations that go beyond, or potentially contradict the general terms laid on in 'Consent as a policy' - the exception, not the rule - then these processes should be as simple and clear as possible, embedded logically and operationally into different parts of the process as it unfolds. It should not be necessary, for example, for citizens to have to read and agree to long and complicated terms and conditions before embarking on an application form. Rather, in the process of completing this application form, small, specific, granular pieces of consent can be obtained for specific uses of specific data points as and when necessary.
4) **Flexibility** Exactly which of these approaches are adopted, and the degree to which they are adopted, depends entirely on the context of the data processing in question. Some transactions are more sensitive than others. Some data is more sensitive than others. Most situations should be easily manageable via a combination of 1) and 2) above. But some riskier situations may require much higher levels of bespoke consent giving.

Appendix F - Interoperability and standards

In an ideal world, most if not all interoperability challenges would be dealt with by common uniform and universally adopted standards. But all too often, attempts to create new standards (or to impose them on bodies that have already built their own systems) fail or worse: creating competing standards systems that fail to interoperate with each other.

Often, when faced with barriers and restrictions related to the adoption of incommensurate processes and systems, a cry goes up for the creation of new common standards. Such standards are desirable in theory but very often extremely difficult to create and implement in practice, so much so that the quest for new standards can

become an expensive, time-wasting wild goose chase.

Why do standard setting attempts often fail? There are a number of reasons including:

- there isn't a central coordinating actor powerful enough to 'knock key heads together'.
- the creation of a new standard increases rather than decreases complexity. This often happens when the boundaries of the system being standardised are too closed, too porous or where there is jurisdictional overlap.
    - Too closed. Many attempts to develop standards are sector specific (e.g. banking, healthcare). But many real-life use cases require data sharing across these sector boundaries. In this case, the existence of incommensurate sector specific standards actually undermines rather than promoting interoperability
    - Too porous. If the Scottish Government were to mandate certain standards to be implemented in relation to digital identity, many organisations would need to adopt these standards who also operate in other parts of the UK outside Scotland (e.g. DWP, HMRC) where the new standards would not apply.
    - Jurisdictional overlap. In the above case, these organisations would then need to operate to two or more different standards (e.g. the Scottish standards as those used outside of Scotland), increasing duplication of effort rather than reducing it.
- powerful vested interests oppose the adoption of a standard and are able to make non-compliance possible through a range of measures that create delays whilst appearing to be supportive resulting in an endless cycle of debate.
- there is gaming of the standards creating process, for example, where a powerful player promotes the adoption of its system as a way of locking other parties into its approach
- the speed of change is too rapid. By the time the standard has been agreed and ready for roll out, technologies, context or issues have moved on, making the standard less relevant/urgent
- many actors do not deem the benefits of standardisation to be high enough to justify costs of change
- embedded legacy systems and already-sunk costs mean the costs of changing from one standard to another are too high e.g. ripping out all UK plug sockets to

conform to EU plugs for electricity, of changing over road signs when moving from right to left hand driving, or abandoning the qwerty keyboard for a different configuration

For standardisation to be successful, therefore, a number of conditions need to be play:

- the standards need to apply to a stable rather than fast-changing situation where the new solution which has longevity (to maintain relevance and likelihood of RoI)
- where there is a powerful central authority with the power to incentivise and or force resistors to adopt the new approach
- where countervailing powers/vested interests are not too strong
- where there are clear, definite exclusive boundaries of application, not requiring dual operation of systems (e.g. where costs can be genuinely halved rather than doubled)
- where the benefits are high improved access to services and entitlements, achievement of key policy drivers and better outcomes for citizens
- where these benefits evenly spread, creating win-win incentives rather than win-lose conflicts
- where the costs of change are low

It is possible for standards development programs to succeed without all of these factors in play, but it is difficult - and the less factors there are present, the more difficult it gets. The more likely outcome is that large amounts of time and effort are wasted trying to create a new, single standard 'to rule them all' that never reaches critical mass.

Appendix G - Potential broader economic significance of the Smart Entitlement Strategy

In this Appendix we draw parallels with fundamental innovations that unleashed the potential of a previous industrial age, we want to highlight the potential broader social and economic significance of the proposed Smart Entitlement Strategy.

This broader economic impact of the proposed Smart Entitlement Strategy derives from the way it addresses fundamental limitations and restrictions built in to the way digital

processes currently work - limitations and restrictions which result in pervasive wasted, duplicated effort at system-wide scale and complexity catastrophes that suffocate growth and innovation.

The two equivalent breakthroughs from previous eras are those of the mass production moving assembly line and the national electricity grid.

The moving assembly line

Before Henry Ford's mass production assembly line, production of products like motor cars was hampered by layer upon layer of wasted effort and duplication. These were 'built in' - unavoidable outcomes of how craft production worked.

Under the craft approach each part of each car was made separately by hand. This precluded the potential cost savings derived from automated production of standardised parts. In addition, to fit two hand-made parts together, each one had to be re-worked. To add (or replace) another part, they had to be re-worked again. And so on.

Most of the costs of making a motor car went into this wasteful duplication of effort. But until Henry Ford's moving assembly line nobody had stepped back to view the system as a whole - to see the waste it created. Result: mountains of waste and duplication of effort were both institutionalised and hidden.

Ford's innovation reduced the cost of making motor cars (and all other appliances) by 90% or more, making them available and affordable for everyone. It placed the fruits of industrialisation citizens' hands in the form of empowering tools (like cars and household appliances) that they could use to make their lives better.

Today's information services are hampered by exactly the same high levels of waste and duplication of effort. Just like the parts that made up cars, the same items of information are collected many times (often, hundreds of times) by different organisations undertaking the same processes. To fit these bits of information together they need to be re-worked - checked and verified anew (often manually), reformatted, perhaps even re-keyed (manually). Each new information service has to be constructed and crafted anew, because there is no available infrastructure that provides the necessary information components along with the means of quickly and easily assembling them.

The Strategy proposed in this paper turns verified attributes into the equivalent of the standardised parts of Henry Ford's system. Attribute stores act as the assembly lines (data logistics hubs) of information-driven services. Ford transcended the trade off between cost and quality that lay at the heart of traditional craft production and that constrained its potential. This Strategy transcends the trade-off between privacy/data protection and access to and use of information that currently constrains many of the traditional organisation centric approaches in which large collections of personal data are required.

The National Grid

Before the introduction of the national grid, electricity was supplied by hundreds of different companies, each with their own power station working to their own standards and approaches.

In the early 20th century, for example, Greater London had 65 electrical utilities, using 49 different types of supply systems, 10 different frequencies, 32 voltage levels for transmission and 24 for distribution, and about 70 different methods of charging and pricing. None of these systems 'talked' to each other. The results of this system of isolated islands of energy generation and distribution were extremely high costs and low take up. London's electricity industry was very profitable but also very small.

It required both institutional and infrastructure innovation to unleash electricity's full potential as an enabler of wealth creation:

- municipal and (later) nationalised suppliers focused not on profit maximisation and monetisation but on total cost reduction and inclusive access and use - making sure every household had access to electricity. This universal provision created a platform for an explosion of new services, supporting economic growth across the entire economy - only made possible by reducing total system costs and ensuring universal, inclusive access.
- infrastructure that joined the dots to enable electricity to shared and moved safely, quickly and cheaply where it was needed, when it was needed (rather than locked up in a series of isolated competing islands of electrification)

This was the equivalent of a 'Mission' long before the word 'mission' was invented to describe such initiatives.

The Smart Entitlement Strategy recommended in this report displays similar characteristics. It is recommending mission-led institutional and infrastructure innovation to reduce total system costs and ensure universal, inclusive access to the fruits of digital data - to provide a platform for further innovation and inclusive economic growth.

It is a Government-led (not market driven) initiative focused on total cost reduction and inclusive access to and use of data focused not on profit maximisation but community benefit. It builds an infrastructure that joins the dots, to enable data to be shared and moved safely, quickly and cheaply where it is needed, when it is needed (rather than locked up in a series of isolated competing islands of data).