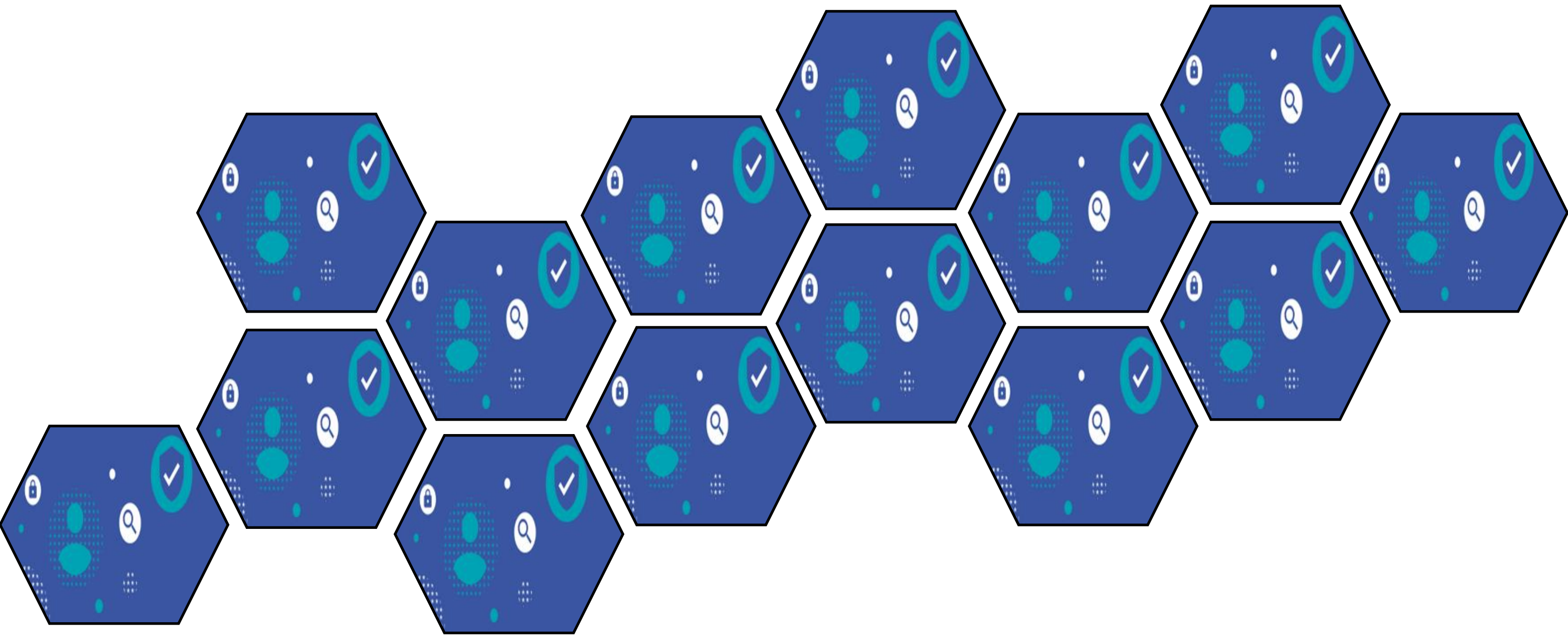
Scottish Government

Digital Identity Scotland

Strategy

June 2020



Date	Version	Notes
30/06/20	Version 1.0	V1.0 – to share with and seek discussion with stakeholders

Contents

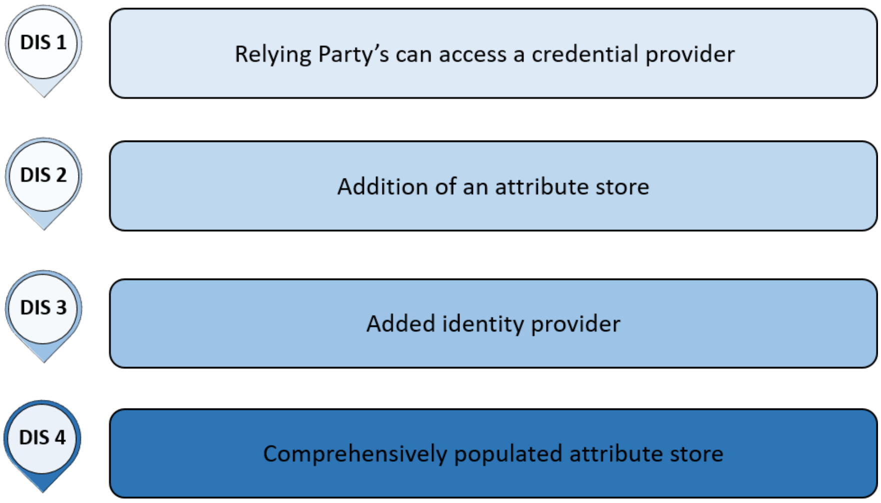
Executive Summary

The aim of the Digital Identity Scotland (DIS) programme is to improve citizens' access to public services by providing them a safe and easy way to prove who they are or that they are entitled to a service. This would enable individuals to create a digital identity, which can be used and re-used for secure access to services from public service providers.

This solution would also contribute to a simplified 'Common Approach' for access to public services, consistent across multiple service providers, and easy to use for individual citizens. As such, DIS would be a key enabler for wider transformation of digital public services in Scotland, providing the means for citizens to share the minimum necessary data about themselves to access services with multiple public service providers – not only online, but also in person where this is preferred.

The main intention is to provide citizens the ability (with their consent) to store their personal information in an Attribute Store which they own and control. The service will be voluntary for citizens and will give them much greater control than at present of their personal information. If they choose to use the service, they will be able to store data which they provide to one public service, and subsequently allow its reuse when they seek to access another public service.

A National Stakeholder Group and Expert Group provide advice to the Programme Board. The Programme follows the principles and practices of Open Government, including transparency by publishing key papers and decisions, regular communications such as blogs, and publically accessible meetings and events. The programme has already evolved through initial Discovery and Alpha stages, and is focused now on delivery of a Scottish Attribute Provider Service (SAPS), (herein referred to as 'SAPS' or 'the service') which aims to deliver key components in four initial phases as shown below:



DIS 1 Relying Party's can access a credential provider

DIS 2 Addition of an attribute store

DIS 3 Added identity provider

DIS 4 Comprehensively populated attribute store

Figure 1.1 - SAPS Phases

The service is intended to provide citizen users with a simple, usable and secure mechanism to access public services if they choose, and a means by which they will be able to manage their data in a way that is under their own control (as detailed in Section 4). We intend that it will provide Public Service organisations with a cost effective, secure and credible service for them to determine identity and assurance of citizens whilst delivering important services to the citizens of Scotland.

1. Introduction

1.1 Mission

Realising Scotland's full potential in a digital world: a digital strategy for Scotland sets out our vision for Scotland as a vibrant, inclusive, open and outward looking digital nation. It aims to make sure that digital is at the heart of everything the Scottish Government does – how we deliver economic growth, reform our public services, and prepare our children for the workplace of the future. As part of this, the Scottish Government is committed to improving citizens' access to public services by enabling safe and easy ways to prove their identity.

The DIS Programme mission is to develop a new way for people in Scotland to prove their identity when they access public services. The intention is to create a **common approach** which would apply across multiple public services. This would enable individuals to create a digital identity, which can then be used and re-used for secure access to personalised services from public service providers. This would support a simplified landscape of access to public services, consistent across multiple service providers, and easy to use for individual citizens.

We are working closely with a range of stakeholders (including members of the public, privacy interest groups, public service providers and the third sector) to develop a simple, safe and secure way for citizens to prove their identity or entitlement to a public service.

1.2 Vision Statement

We will develop the service with the aim of improving citizens' access to public services, by providing them safe and easy ways to prove their identity, or attributes thereof, which are relevant to eligibility for the service.

A successful reusable digital identity service will have the clear understanding, trust, and engagement of the citizen user and relying parties (the term used for public sector bodies that provide services to citizens). It will be founded on user-centric and privacy respecting principles only allowing the sharing of data between services with the active consent of the citizen. No data will be shared for commercial purposes, nor will data be stored in a centralised database. It will ensure that a citizen's data remains under their own control so they can store and consent to share their data with public sector organisations where needed.

Data that has been provided by a citizen to a public sector organisation and assured or proven by that trusted organisation is considered to be *verified* data. The ability to reuse that data delivers benefits to the individual citizen by removing repetition and friction such as the repeated need to provide varied evidence when accessing public services. It can also help to solve governmental data-sharing challenges such as ensuring citizen users are asked to give permission for data to be shared between public service providers. Additionally, reuse of verified data will also reduce costs and burden on the public sector e.g. the costs associated with the unnecessary re-checking of data which has already been checked/ verified by other trusted organisations.

1.3 Digital Identity Scotland Programme Principles

The key principles of the DIS programme are as following:

Inclusivity: Everyone has a right to a digital identity, if they wish one, and the benefits it can provide

Ownership: Individuals always own their identity and personal data

Consent: An individual's digital identity/data should not be used or shared without their explicit consent

Choice: Individuals should have a choice of the data held, who can access it and the right to opt out or to change where they store their data

Control: Individuals maintain control of their data with the right to access, correct, and delete it as they choose

Simplicity: An individual's use of their digital identity should be simple and intuitive

Portability: An individual should be able to access/use their digital identity anywhere. This also means we need to ensure enough consistency with other systems and standards being developed across the world

Transparency: Individuals have the right to understand how their digital identity data is stored, used and shared

Privacy and Security: Identity data and transactions that involve an individual's data should be held with the highest standards of privacy and security.

1.4 Value Statements

The DIS core value statements which support delivery of the service are:

1. **Improving the user experience**
2. **Ensuring better outcomes and inclusion**
3. **Supporting transformation of Scotland's public services**

2. Background

2.1 What have we learned?

As the public sector landscape changes, the way citizens want to interact with public services is also changing. More and more public services, such as accessing council services or applying for Social Security entitlements, are being made available online. To access these services, citizens may need to prove who they are online. Where this is necessary, citizens want to do so in a safe and secure way, exchanging only as much information as necessary and, ideally, do not want to have to repeat the process over and over again when accessing additional public services.

The COVID-19 pandemic has had, and will continue to have, a significant impact on the delivery of public services and citizens willingness and appetite for accessing services remotely, securely and with minimal friction. The rapid roll out of new services and the huge change in working practices it can be argued provides even more fertile ground for DIS to operate on and to help citizens access the services they are entitled to and need.

This is the challenge that DIS is seeking to resolve through the delivery of this service. We have tested different concepts, building on the experience of users, customer organisations, technology providers and other organisations facing similar challenges and believe that this strategy represents the right way for Scotland to proceed.

2.2 Where are we now?

When a citizen has to prove that they are entitled or allowed to access a service or receive a certain product, generally they will need to share information, or ‘attributes’, about themselves with organisations/service providers. This information could, for example, include age, address, disability, etc.

Service providers each take steps to verify that the information provided is accurate and valid. When an organisation has confirmed this, we refer to these as ‘verified attributes’. Currently citizens who require access to multiple services have to provide their attributes to multiple service providers. Sometimes they may even be asked to provide it to the same service provider multiple times. As a result, the information that a service provider requires is likely to have been checked already and held by another organisation.

If there was a safe, efficient system which allowed citizens to store these attributes and consent to share those needed, it would not only streamline identity assurance processes, it could also help service providers achieve other goals. These include:

- Efficiently on-boarding citizen users
- Assessing needs and eligibility more quickly
- Configuring and delivering services, including collaboration with other service providers
- Reducing the need to store and protect a citizen’s personal data
- Efficiently undertaking related administration.

Such a system for the sharing of verified attributes would help service providers reduce repetition, friction, effort, risk and cost to both users and organisations. But to work, the system will require the clear understanding, trust, and engagement of users.

3. Moving Forward

3.1 The SAPS Model and Ecosystem

From a citizen's perspective

Trust, consent, choice and safety.

The central stakeholder in this is the citizen-user. The following presents assumed user needs for digital public services (based on User Research completed by Snook as part of our Discovery activity) and team experience); it presents the capabilities implied by them and illustrates how those capabilities meet the user needs.

- I want to use a public service so that I can fulfil my responsibilities and receive my rights (as a citizen-user)
- I want digital access to public service so that I can obtain service with less effort, fewer and easier steps (lower friction)
- I want a single, secure login so that I can revisit one service or several services through a single and safe means (to save me creating accounts for each service)
- I want to (optionally) reuse something which is already proved about me (my 'verified attributes') so that I have lower effort in entering data, make fewer mistakes, have lower costs of postage, calls or travel, and gain the benefit of obtaining service quicker and without having to provide new evidence
- I want minimum data to be exchanged between all parties so that I can obtain the service with minimum disclosure of my data to the service and across services
- I want to be safe and in control of which data items are disclosed or changed by services, so that I am totally clear about what is being used or changed on my behalf.

The service will provide citizens with digital tools which ease their access to, and use of, **Scottish Public Services** by reusing their verified data, including their identity, across public services. **Citizens have control of their own personal data** and will give **consent** to share this data with public services.

It will be voluntary for citizens to use the service. The aim is to create a clear user-centric service with precise capabilities and a simple **consent-based** user experience. It will ensure public services will always provide **alternative routes** for users who:

- do not have, or do not wish to use the service
  or
- for whatever reason withhold consent
  or
- limit the maintenance of their attributes.

SAPS will enable the user of a strong credential to **incrementally** associate attributes with the user of that credential, so that their subsequent use of public services is of increasingly lower friction, effort, risk and cost. This will enhance usability of the service for all citizens, and will particularly benefit "thin file" citizens (those who may not have any, or a sufficient digital footprint in commercially available data sources to meet required government standards) who currently struggle to access digital public services.

Scottish Government aims to provide citizens the ability (with their consent) to store their personal information, in the form of verified attributes with associated metadata, in an **Attribute Store** which they **own and control** the information within it.

SAPS will give citizens the opportunity to consent to disclose some or all of their **verified attributes** from their Attribute Store with other public services. This can include their overall 'digital identity' - an expression of a group of attributes that reach a level of assurance acceptable to those public services (often referred to as Relying Parties or RPs) as described in the UK Government Digital Service Good Practice Guide on Identity Proofing and Verification of an Individual (GPG45).

Initially, only **verified** attributes will be stored in the Attribute Store by SAPS - **unverified** attributes (user self-asserted or other) may be kept in a citizen's Attribute Store if they desire, but these might not be used by the service.

User centered service design is at the heart of this. More research is needed and will be undertaken on **citizen data ownership and control** as well as options around attribute maintenance and unverified attributes. DIS will continue to test and iterate the service based on user feedback. Educating users on the benefits of the use of the service will be a key success factor. This will happen organically as users interact with RPs that use SAPS, with content design being key as part of the user journey.

In addition, it is acknowledged that a range of engagement activity will require to be undertaken in order to publicise the service, promote the benefits to users and encourage uptake in usage.

From a Public Sector organisation perspective

Reducing friction, effort, cost and risk.

This service will enable Scottish Public Sector services to **decrease their cost and risk** when digitally delivering public services by reducing error and reducing reverification of data. It will do so through creation of a trust framework which limits the parties included in the SAPS closed ecosystem to **public-sector organisations** (or third sector organisations acting on their behalf), known as Relying Parties (RPs) and moving towards personal information only being verified by these RPs.

It will provide a mechanism for obtaining verified attributes and/or digital identity from **commercial identity providers** (IDPs), such as those involved in the UK Government Identity Trust Framework (formerly GOV.UK Verify), until there is sufficient verified data in a citizen's Attribute Store that has been populated by public sector organisations. With user consent, the resulting verified attributes and associated metadata can be **imported into the user's attribute store** to be shared with their chosen public service(s).

DIS has engaged with a range of RPs throughout the programme. For example, a meeting of senior leaders across several organisations took place in November to engage them on this attribute approach. This was followed up with another session in June 2020. In addition, RPs were part of the Attributes Prototype from February through to May 2020. This engagement is ongoing and will ramp up with the programme moving into the next phase of Beta/Live delivery, continuing to explain how citizens and business users will benefit from using the service, and particularly around how RPs can on-board to the service. The roadmap gives an indication of the speed of planned on-boarding.

From a Technical perspective

The service will be made up of a series of components: A Credential Provider (CP), an Attribute Store (AtS) and potentially one or more Identity Providers (IDPs).

The following describes the SAPS service definition, shown at the third stage. Some service characteristics have been derived from the evolution of two previous stages/ iterations of public service definition.

3.1.1 Stage 1

Most public services are still constructed on this model (but will not be after this service definition is implemented). In stage 1, every public service was separate. The service (RP) separately processed applications for service. Most services proved some aspects of the identity *of the user* (name, date of birth, address), and decided on *eligibility for the service*. Each service repeated all of these steps. Usually each service maintains a 'system of record' focused on that specific product or service: a database of all of the data items which the service captured and subsequently verified.

Often, where the law permits it, services interacted with other services to 'share data' (often between organisations) which assisted a receiving service in making its separate determination of identity and/or eligibility. The user entered their data for each service separately.

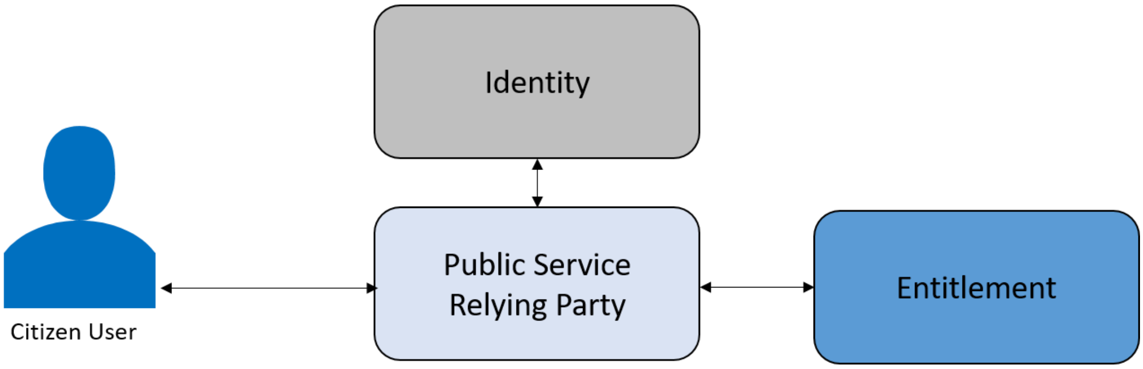


Figure 3.2 - Stage 1

3.1.2 Stage 2

A number of public services have used this model, (HM Treasury has stated no more services will be connected to GOV.UK Verify – the current UK implementation of stage 2). In stage 2, a user obtained a digital identity, which enabled sign in to each service through the reuse of a suitable secure identifier, protected to some 'level of assurance of the credential'[1], and the proof of identity, to some 'level of confidence'[2], and releasing specific verified identity attributes describing the user (names, date of birth, address). The credential provider and the identity proofing were combined in a single offering

[1] Good Practice Guidance 44

[2] Good Practice Guidance 45

by an Identity Provider (IDP). Because Identity was no longer under control of the Public Sector Relying Party, new privacy rules and governance regime were introduced to protect the user.

Data sharing agreements, according to specific laws, still enable direct service to service data exchange. The user entered their data into each service separately (usually including name, data of birth and address because of privacy rules relating to the use of the data).

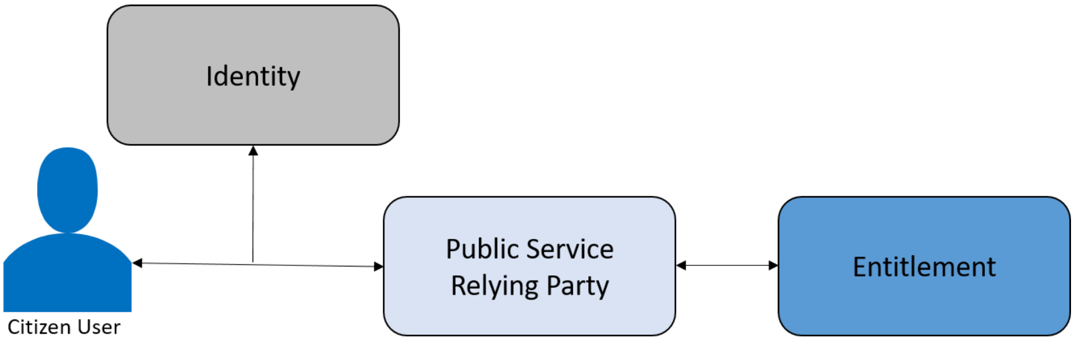


Figure 3.3 - Stage 2

3.1.3 Stage 3 – SAPS Service

In stage 3, a user has a suitable secure identifier associated only with that user, protected to some ‘level of assurance of the credential’, managed by a Credential Provider (CP), which enables sign in to each service. The act of ‘signing in’ discloses no more information to the RP than a unique identifier. The user has ownership and sole control of their verified attributes, including their verified identity attributes. Their verified attributes are managed by an Attribute Store (AtS). RPs may ask for disclosure of the user’s verified attributes, on the basis of which they offer service. RPs may ask the user for other data, and may verify other data. RPs must offer to return all verified attributes to the user, so that the user and other RPs can gain benefit in the future. In all cases, the user gives informed, revocable consent to disclosure and return of verified attributes.

The user only enters data items which are not already in their AtS. Data sharing between services is mediated by the user, and implemented by their AtS.

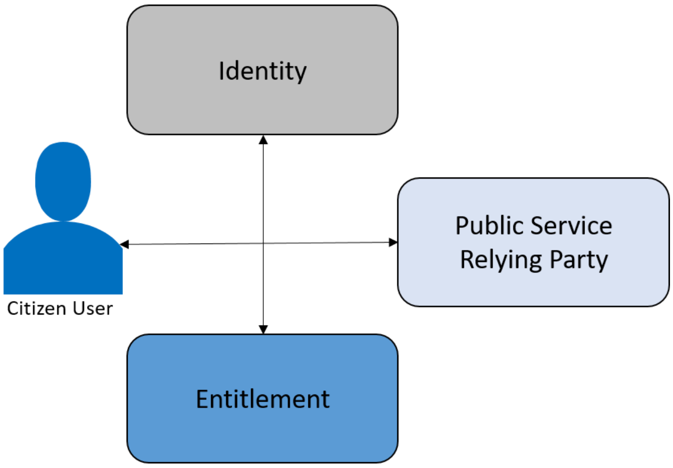


Figure 3.4 - Stage 3

3.1.4 Credential Provider

The service will provide Citizen users with anonymous authentication credentials and single sign on to individual public services. Anonymous in this scenario means that the user credentials will not be used for any purpose other than maintaining the security of the user and their credential and will not aggregate personal information. Credential provision will be provided from best of breed commercial suppliers and will:

- Provide users with a choice of second / multi factor authentication methods (such as SMS text message, One Time Password or via an authenticator application). The chosen supplier must be able to deliver sufficient choice
- Minimise user friction by requiring no proofing of the user before an authentication service can be offered
- Be based on a strong credential (GPG44 Level 2) which, from initial issuance for its lifetime, can be safely assumed to be controlled by the person to which it was issued
- Be designed for digital inclusion and accessibility, in this case, providing second factors for users without access to a smartphone (e.g. landline telephony, grid card, SMS to non-smart mobile)
- Provide credential **recovery options** and/or rebind a new credential to the same person by appropriately secure means
- Protect the privacy of the users of these services.

3.1.5 Attribute Store

The attribute store is a user controlled space where verified attributes and associated metadata from public services are captured and maintained. Users will initially be presented with a single provider of an Attribute Store, but, to further aid citizen trust, it is expected they will have a choice of attribute store in future.

It will be ensured that the attribute stores provide services under full and sole control of the owner of the attributes (the data owner, the data subject). All consent information and all management of consent occurs at the Attribute Store.

Attribute Stores will be capable of presenting attributes which are derived from other attributes (e.g. age over 18 is derived from verified date of birth, etc.) according to prescribed standard mechanisms - this is in keeping with the principle of data minimisation.

The service will also ensure that the attribute stores are appropriately secured, including encryption of data at rest by key material which is only known to the user. Scottish Government standard specifications of metadata will always be associated with attribute values when stored or retrieved.

Whilst the Attribute Store provider may offer other services, and will offer ‘data portability’ services, the service’s privacy and trust framework will stress that its protections and guarantees apply only to the use of the Attribute Store within the SAPS ecosystem, by and for public services

3.1.6 Infrastructure Considerations

SAPS will define the infrastructural components, which may have a variety of deployment models, to enable convenience, security and minimal complexity for the entities. Given the closed nature of the ecosystem, the service will define all the **protocols and profiles** necessary so complexity can be minimised.

3.1.7 Creating An Ecosystem of Trust

The service will deliver a Trust Framework which protects the public service focus, citizen users' rights and ensures clarity of the offer to the user.

The Trust Framework will cover the business, legal, ethical and technical **features** of the ecosystem (i.e. the roles and responsibilities of all parties within the public service remit). It will:

- State the **citizen user's part** in the ecosystem, as data owner, data controller, and consented point of data integration, i.e. the user's data comes from and goes to their attribute store, never from system to system

- Define consent as the **legal basis of operation** of the ecosystem (i.e. not 'public task' for organisation to organisation data sharing). The service will enable the user and only the user to control the disclosure of their data. The data belongs to the citizen and is protected for their use only.

- Define the meaning of the **components** of the ecosystem: Authentication Credential Provider, Attribute Store, Public Sector Service as Relying Party, Public Sector Service as Verified Attribute Provider.

- Incrementally define and publish transparent **data, verification and metadata standards** for verified attributes to be part of the service so that public sector organisations can rely on attributes attested by others in the sector. These will be based on best practice and open standards to enable secure and cost-effective services.

- Define **interoperation with external entities** (such as the proposed UK Government Digital Service (GDS)/ UK Digital Identity Unit (DIU) commercial framework):

  - Define how external parties might **provide data to** SAPS, such as existing commercial IDPs or potential future private sector IDPs, ATPs or other data provisioning services.

  - Define how external parties might **receive data from** SAPS, which is expected to be limited to:

    - the user exercising the DPA18 right to data portability

      or

    - the user seeking to authenticate and provide identity attributes to a public service outside SAPS, e.g. a UK Government public service, perhaps under the remit of EU directive eIDas, or a possible future UK private framework arranged by DIU/GDS.

- The service will need commercial, legal and technical **protections and controls**, which will be expressed in the SAPS trust framework. This might be as simple as including GDS' terms for HMG connection into the SAPS trust framework.

3.1.9 Governance and standards

SAPS will provide governance of data, metadata and verification standards (applied to sources and uses of citizen attribute data) so that the Scottish public sector can rely on attributes attested by other parts of the Scottish public sector.

It will have rules and guidance covering all 'consuming' public services, and all 'origin' services so that the overall Scottish public service attribute eco-system meets its standards. It will be usually required that all services are originators of attributes as well as consumers of attributes.

The service will maintain standards transparently and enable secure and cost-effectiveness by using open standards and publishing its standards for attributes.

It will provide support to relevant relying parties so that the overall operation of the service is compatible with these principles.

3.1.10 Consent and Privacy

DIS will create a detailed privacy policy based on a clear definition of 'privacy protection of what data from which actors'. For the purpose of this document, the service is based on the following privacy related boundaries:

<u>Authentication Credential Providers:</u>

- Credential Providers (CPs) are **anonymous**, in that they must not aggregate personal information, nor use it for any other purpose than maintaining the security of the user and their credential - this needs to marry with **account recovery** and flexible MFA options

- CPs should have a **credential monitoring capability** as required by GDS Good Practice Guide Using Authenticators to Protect an Online Service (GPG44)

- CPs support management of the **binding/connection to the Attribute Store**

<u>Dynamic Consent and Updating Attributes:</u>

- All actions to disclose verified attributes are only performed if the **user is present** to give consent. The service will not enable automatic disclosure of user's data for any reason.

- Consent is **granular** to the level of individual attribute - separate maintenance and disclosure.

- Consent is **revocable** and therefore can be withdrawn.

- User consent to share attributes is **dynamic** - consent is given at the **time of disclosure** from their attribute store to the public service they are in session with.

- Users must consent to all **updates** of their verified attributes to the Attribute Store - such consents can include for the service that originally verified the attribute to **maintain the verified attribute over time, including revocation**. This meets the needs of RPs to receive current information, such as address data for service eligibility and/or correspondence.

- SAPS will provide **support to RPs** so that the overall operation of the service is compatible with these principles, such as avoiding use of 'matching' and 'trust' until these are secure and appropriate, e.g. origin services frameworks to enable update of attributes, frameworks for consuming services to enable use of attributes, management and control of consent.

<u>Attribute Stores:</u>

Personal Information Aggregation:

- The service will be **transparent** in its operation and use of user data.

- System entities will meet regulatory **audit** obligations without the need to disclose the personal data of the data subject.

- **No personal data aggregation** (including of personal identifiers) will occur in the SAPS components, as attributes will persist only in the user-owned and controlled (only the user can read the contents of their attributes store, all other parties must have the users explicit consent to do so) Attribute Store, and authentication and access control information will persist in the Authentication Credential Provider.

4. Roadmap

4.1 How do we get there?

The figure below provides a high level roadmap for the delivery of the service, based on a series of indicative milestones, DIS 1 to DIS 4, in the first 2 years. These milestones are indicative and subject to confirmation and potential change. **NB** Q1, 2 etc refer to calendar year.

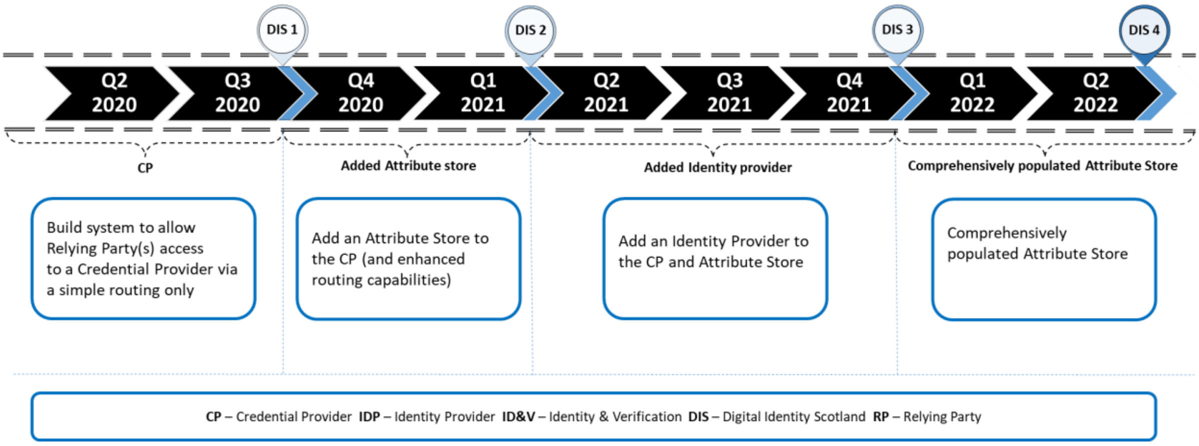

DIS 1
DIS 2
DIS 3
DIS 4
Q2 2020
Q3 2020
Q4 2020
Q1 2021
Q2 2021
Q3 2021
Q4 2021
Q1 2022
Q2 2022
CP
Added Attribute store
Added Identity provider
Comprehensively populated Attribute Store
Build system to allow Relying Party(s) access to a Credential Provider via a simple routing only
Add an Attribute Store to the CP (and enhanced routing capabilities)
Add an Identity Provider to the CP and Attribute Store
Comprehensively populated Attribute Store
CP – Credential Provider IDP – Identity Provider ID&V – Identity & Verification DIS – Digital Identity Scotland RP – Relying Party

Figure 4.1 - DIS Roadmap

4.2 DIS 1

DIS intends to make available a CP to be accessible via simple routing only for RPs with Back Office Processing for Identity Verification where required. It is envisaged that this service could initially be adopted by 1 or 2 smaller RPs, to provide them with a secure credential and develop the maturity of the service.

The benefits include:

- A credible CP is available to allow citizens to apply for services/benefits using a single credential
- This account can be reused for multiple RPs
- This provides save/resume functionality when applying for services
- The simple router provides a separation between the RPs and CP

4.3 DIS 2

In this phase, the CP offering is enhanced with the addition of an Attribute Store, and potentially an enhanced routing capability.

DIS will continue to engage with potential RPs and aims to continue on-boarding public sector organisations during this phase. DIS will continue to test and iterate and work in collaboration with RPs. This continuous on-boarding model is key to develop the maturity of the SAPS.

The benefits include:

- Citizens can use the CP to apply for services/benefits
- Citizens can choose to allow RPs to use verified attributes from their personal attributes store to speed up applications for services/benefits
- Citizens can choose to save verified attributes in a personal attribute store for use in future applications/service requests, to save time, effort and cost
- RPs can use verified attributes, with the citizen's permission, to reduce time and cost, and potential fraud.

4.4 DIS 3

In this phase the CP and Attribute Store service is enhanced with the addition of one or more IDPs.

The benefits include:

- Citizens can choose to save new verified attributes in their personal attribute store to support future service/benefit applications
- Third parties can offer verified attribute capabilities to populate a citizens attributes store
- RPs can be quickly on-boarded by identifying business cases based on available attributes to support their use of the services.
- IDPs are added to allow citizens to use the system and have their identities verified electronically; this will save a verified identity attribute to their personal attribute store. The benefit is to give the citizen the opportunity to have a completely digital experience when applying for or modifying applications. It is expected that IDPs will be able to support an offline journey if an online identity verification fails.

4.5 DIS 4

Over time, as more RPs come on board and the more users and RPs take advantage of SAPS, comprehensively populated attribute stores are achieved.

The benefits include:

- Citizens can apply for services with less friction, effort, risk and cost
- Citizens are attracted to SAPS as the means to more easily access services they are entitled to

- RPs can deliver services to users with less friction, effort, risk and cost
- RPs are attracted to SAPS by the volume of users and the volume of verified attributes which will reduce friction, effort risk and cost when delivering services
- The use of commercial IDPs to provide identity verification reduces as the verified attributes generated by citizens provide RPs with the confidence to rely on these to derive identity assurance as required.

4.6 Relying Party On-boarding

It is DIS' intention to work with a number of smaller organisations in the first phase of the roadmap, who would benefit greatly from the availability of a credential provider. This will allow testing and iteration before extending SAPS to further organisations. DIS will work with these organisations to understand on-boarding requirements and transition arrangements from current processes.

For future phases, DIS will work with an increasing number of organisations, again testing and iterating before scaling more widely. DIS will engage with organisations to agree the most appropriate phase for individual organisations to on-board, as well as agreeing priorities with these organisations.

5. Feedback and Next Steps

As DIS continues to pursue the attribute based model outlined in this draft strategy, we will engage across the public sector to gain further insights and explore needs and on-boarding requirements. Feedback or comment on this is welcomed. We also intend to publish a detailed Service Description and Privacy Policy documentation in due course.

DIS remains committed to the principles and practice of open government. We will continue to publish regular blogs, and key programme outputs, ensuring that this work is as transparent as possible. As timelines and delivery steps become clearer, this information will be shared through these channels.

In the meantime, we would welcome any feedback or comments you may have via:
digitalidentityscotland@gov.scot