Digital Identity Scotland – Attribute Standards

Background

Digital Identity Scotland (DIS) is a programme being run by the Scottish Government to develop a common approach to digital identity for Scottish digital public services.

From the outset the programme stated the following objectives:

1. To develop a common approach to online identity assurance and authentication for access to public services, that supports the landscape and direction for digital public services delivery.
2. To develop a solution that is designed with and for members of the public (service users) and that stakeholders can support.
3. To develop a solution that works: is safe, secure, effective, proportionate, easy to use, and accessible; and forms part of public sector digital services.
4. To develop a solution where members of the public can be confident that their privacy is being protected.
5. To develop a solution that brings value for money and efficiencies in the delivery of digital public services
6. To develop a solution that can evolve and flex with changes that occur in the future (future proofed), e.g. changing in response to new technologies

Within this scope DIS is seeking to develop a range of services covering:

- **Identification** – determining an individual's basic identity
- **Authentication** – securing access to digital services
- **Attributes** – enabling the portability of verifiable data associated with the individual and under the control of the individual.

Enabling attribute-related services will bring several benefits to DIS:

- Access to services often requires individuals to demonstrate more than just their identity. Attribute services will provide the means to do this.
- Well-designed attribute services will give the individual control over their data, addressing the requirements of GDPR.
- Attribute services can support "tell us once" initiatives, lessening the burden on individuals to keep data up to date in multiple places.
- Attribute services may support individuals, who are initially unable to obtain high assurance identity, in progressively building up the assurance of their identity over time.

A key part of the work is to understand the approach to standards that DIS should take in order that it can develop services that are interoperable, future proof and economic. Where possible DIS wishes to align with standards in the market.

Standards for **identification** and **authentication** are relatively mature. In particular, the UK government has well-established Good Practice Guides that the DIS is likely to align with.

Standards for **attributes** are however far less mature. This paper therefore outlines what attribute standards will be needed by DIS in the future, what they will need to cover, considers the status of standards that do exist and recommends the approach that DIS should take.

The need for attribute standards

DIS defines an attribute as “an item of personal information, e.g. name, age, address, and any associated meta-data and assurance information”. Attributes will typically be created when an individual uses a service (whether a Scottish public digital service or some other service). DIS believes access to and use of Scottish public digital services can be simplified by making attributes portable – by providing the individual with the means to take attributes created in one service an make them available to another service.

The exact mechanisms and controls that will be put in place to enable attributes to be portable in a safe and secure way are to be determined and not the focus of this document. Instead this document is concerned with what a service provider (or Relying Party) needs to know in order to be able to rely on an attribute for the purposes of granting access to a service. Attribute standards will help to ensure that the information shared with a relying party meets the criteria necessary to enable this to happen.

What attributes standards should cover

In a fully open and extensible attribute exchange system, standards will be required to cover a number of areas including:

- Language
    - Defining and describing attributes types
    - Defining and describing meta data (data that describes attributes)
    - Defining formatting rules for data and meta data
- Provenance
    - Source of the data
    - Whether the source authoritative or not
    - Process undertaken by the source to establish the data and whether that is auditable / audited
    - Revocation status of the attribute
- Integrity
    - Ensuring that attributes cannot be altered in transit (including authorised alteration by the individual)
    - Ensuring that the provenance of attributes can be verified (cryptographically)
    - Supporting zero knowledge verification where necessary
- Binding
    - How attributes are tied to the digital identity known by the relying party
    - Authentication of the individual at the point of attribute sharing

In a closed system, it may be possible to enable a more limited and less extensible form of attribute sharing that still provides value to individuals. Within Scottish public services it may be possible to define a closed system for a range of purposes. Work undertaken by Mydex, for example, suggests that there can often be local clusters of personal data where such closed systems could develop.

Attribute standards are primarily concerned with providing agency to relying parties – enabling them to determine when a service can be provided. In parallel with attribute standards there will be a requirement for consent management standards that ensure agency is also given to individuals – enabling them to determine when and how attributes pertaining to them are shared and used.

Current status of attribute standards

To date there are no widely adopted attribute standards. This in part reflects the current state of the digital identity landscape. There is however significant work underway that will over time result in much greater standardisation, as follows:

- **Government standards**: Both the US and UK governments have produced guidance relating to attributes, as follows:
    - **NIST SP 800-63C**: Provides guidance to the US government on integrity and binding in the context of federated identity.
    - **GDS Attribute Guidance**: Draft document providing outline guidance on provenance, integrity and binding
- **Industry standards**: The following is probably currently the closest to a fully developed standard for attributes:
    - **W3C Verifiable Credentials**: Candidate recommendation covering integrity and binding and several aspects of language and provenance. There is a significant overlap with Self Sovereign Identity initiatives.
- **Proprietary developments**: There are a variety of organisations developing services and solutions in the area of attributes. These are not standards per se, but in the absence of widely adopted standards may provide helpful reference points. For example:
    - **Factern**: Seeking to develop a universal standard for metadata management[1] primarily focused on language and provenance.
    - **Mydex**: Has defined numerous datasets covering a range of applications that define a language for attributes.[2]
    - **Meeco**: Has published whitepapers describing their personal data ecosystem service[3] that includes examples of language, provenance, integrity and binding
    - **Etive**: As part of their digital logbook work[4] have explored potential attribute sources in local authorities (so called “micro sources”) with a specific focus on obtaining data for identity verification.

As well as identifying, adopting or developing the necessary attribute standards DIS will also need to determine its approach to compliance – how will DIS ensure that at the processes employed by attributes are sufficiently robust and where necessary, auditable?

Future direction

The government standards referenced above will likely develop further. The timing of this is not clear and will depend on the relative priority to the UK and US government of attribute-based services compared to other identity initiatives.

The W3C appears to be the most likely place that a technical standard for attribute exchange will emerge, although it will not cover all of the areas above. If adopted by DIS, it would likely be necessary to define “domain specific” rules that sit above the W3C standard to show how it is used in the DIS context.

The DIACC (Digital Identity and Authentication Council of Canada) is development a Pan-Canadian Trust Framework, which in due course should also include attribute standards.

[1] https://next.factern.com/project/protocol

[2] https://dev.mydex.org/data-schema/datasets.html

[3] E.g. https://www.meeco.me/whitepaper.html

[4] https://www.digitallogbook.org/what-is-digital-log-book/

Other significant developments that may become good reference points include the emerging customer centric attribute exchange initiatives such as Sovrin and Verified.me (Canada).

Recommended approach for the Scottish Government

In the short to medium term it is likely that any attribute sharing facilitated by DIS will need to be treated as a closed system. Depending on the parties involved and the requirements of services it may be possible to identify cases where the requirements placed on attributes (especially in terms of provenance and integrity) are low. If attributes are shared between organisations that trust each other and where liability is in effect shared the need for robust technical integrity and non-repudiation may be lessened for example.

DIS should however maintain a watching brief on attribute standards developments, as well as the adoption of those standards by the industry. In the case of the UK government, DIS should play a greater role, working with the UK government to develop attribute standards that are suitable for public services as a whole.