Digital Scotland
Digital Identity Scotland

OPEN IDENTITY EXCHANGE White Paper

# Digital Identity provision in Scotland

Scottish Government
June 2019

Authors:
Steve Pannifer (Consult Hyperion)
Margaret Ford (Consult Hyperion)
Alan McDougall (Scottish Government)
Marianne O'Loughlin (Scottish Government)
Tim McKell (Gemserv)

# EXECUTIVE SUMMARY

The Scottish Government's digital strategy sets out to make sure that digital "is at the heart of everything" it does – including delivering economic growth, reforming public services, and preparing children for the workplace of the future. Digital identity is central to this strategy.

Digital Identity Scotland (DIS) is a programme being run by the Scottish Government (SG) to develop a common approach to digital identity for public services in Scotland. The aim is to ensure digital identity services are available to all individuals enabling access to the services that they need. These digital identity services must be safe, secure, effective, proportionate, easy to use, accessible and cost effective.

This does not mean the SG will create and manage digital identities. Instead individuals should be able to use trusted digital identities, that they already have and use for other purposes, to access public services also. This is similar to how individuals pay for public services today - they use payment accounts they already have and which are used for many other purposes. It is not necessary to set up a special payment account for government.

Delivering a common approach to digital identity is not trivial. The public services that individuals access have a wide range of requirements for identification and authentication, some regulated, some not. The information that public services require to determine eligibility (referred to as "attributes") will vary too.

The individuals themselves will have widely varying needs. There will be differing views on privacy and the role of government in the provision of identity systems. Individuals will have differing levels of access to and familiarity with digital technology, and differing levels of access to evidence that can be used to create a digital identity.

The SG has undertaken a substantial OIX Alpha project with OIX members to explore the approach it should take to digital identity. This built on the findings of the Discovery Project[1]. It included building a Proof of Concept prototype, undertaking user research and analysing technical and commercial aspects. This report is a detailed discussion of the findings of the Alpha project which can be summarised as follows:

- **A Flexible Approach**: Catering for the differing needs of individuals and the public services they wish to access will be complex and these needs vary considerably. The Alpha project included user research to understand some of those needs. This will need to continue as the service develops to ensure the needs of all parties are addressed. A key recommendation of the report is that the SG makes available a publicly owned identity provider (IDP) alongside private sector IDPs. This will ensure that the common approach includes sufficient choice to meet the range of needs of individuals wishing to access public services in Scotland. The recommendation includes ensuring that there are still sufficient incentives for private sector IDPs to participate.

- **A Standards Based Approach**: A flexible approach will require the adoption of appropriate standards - both technical standards and identity assurance standards. This, in conjunction with appropriate governance arrangements, is the best way to ensure that services are interoperable, future proofed and to avoid DIS building expensive proprietary solutions.

[1] https://www.gov.scot/publications/online-identity-assurance-programme-board-papers-23-may-2018/

- **A Phased Approach**: The vision of DIS is to support a wide range of digital identity uses, enabling all kinds of public service. To achieve this vision, DIS will be dependent on the digital identity industry to develop standards-based services that support the full range of capabilities that DIS will need. Existing digital identity services are often focused on identification and authentication. DIS will need to work with providers to ensure that there is a route to the wider support of attributes, which will unlock many valuable use cases and support the concept of “tell us once”.

Getting digital identity right will bring enormous benefits to the people of Scotland and there are good examples where this has been achieved elsewhere - such as the BankID schemes in the Nordics that provide access to public services, and the Estonian eID which was part of a complete transformation of public services. The models followed in these countries do not translate directly into the Scottish context. They do however serve to illustrate the benefits that a joined up approach to digital identity will bring. As has been the experience in these countries the ambition of DIS is to remove duplication, error and waste. A common approach to digital identity will reduce the need to own and maintain silos of technology, enabling transformation of public services. It will also make it easier for people to interact with those services.

# CONTENTS

# 1 INTRODUCTION

## 1.1 Scope

Digital Identity Scotland (DIS), the digital identity programme of the Scottish Government (SG), has worked with several members of OIX to run an Alpha Project as part of its wider programme. The purpose of the Alpha Project was to test the hypothesis that DIS can meet its objectives by adopting a flexible approach to digital identity that builds on existing digital identity capabilities in the market and provides choice to individuals.

This report documents the key findings of the Alpha Project which considered:

- The needs of individuals - the people of Scotland - who wish to access digital public services in Scotland.
- The needs of relying parties (RPs) - the digital public services provided to individuals.
- Technical interoperability of identity services in the market.
- The role of identity assurance standards in ensuring equivalence across service providers.

The intent of this paper is to inform the future direction of DIS and also contribute to the future development of the digital identity industry in the UK and further afield.

The Alpha Project produced the following additional documents:

- **In person identity verification requirements** - a distillation of the capabilities that would be needed to deliver an in person identity verification service to support identity providers (IDPs) in meeting the requirements of GPG 45.
- **DIS Relying Party Service Description** - a forward looking definition of the business services that DIS anticipates offering to digital public services in Scotland.

## 1.2 Approach

The project was collaborative involving many interested parties and stakeholders and consisted of four main activities:

- User research facilitated by the SG
- Building a proof of concept
- Analysis of digital identity standards
- Discussions with industry players on potential commercial models

This document discusses the findings from all these activities. We have included a list of the many organisations who supported the project in Appendix C.

## 1.3 Intended Audience

This report is intended for OIX members and any other interested party. We hope it will contribute to the successful development of a vibrant digital identity industry in Scotland, the UK and further afield.

# 2 REQUIREMENT

## 2.1 Background

In Scotland public services are provided by a wide variety of different organisations, including central government departments, the NHS, local authorities, arms-length bodies and others. The SG is committed to ensuring that these services are delivered effectively, for the benefit of the people of Scotland, regardless of who provides the service. The implementation of a robust, shared digital identity ecosystem for Scotland will help to support delivery of high-quality services, increasing convenience and reducing costs.

## 2.2 Vision and Scope

DIS is a programme being run by the SG to develop a common approach to digital identity for public services in Scotland.

From the outset the programme stated the following objectives[2]:

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

## 2.3 What is digital identity?

In the broadest sense, digital identity enables a party to share (digitally) trusted information about themselves for other parties to rely on. This means:

- Individuals, organisations or devices can have digital identities. Any one of these parties can share trusted information or rely on information.

- The information is trusted because governance arrangements provide assurance on the provenance and reliability of the information. This may include providing that information in a way that is verifiable.

Digital identity involves three functions:

- **Identification** - allowing a party to assert that they are real and unique.

[2] https://blogs.gov.scot/digital/wp-content/uploads/sites/5/2017/12/Online-Identity-Assurance-Programme-Plan-5-December-2017.docx

- **Authentication** - allowing the same party to assert in the context of a service access, that they are the same party previously identified.
- **Authorisation** - allowing a party to link trusted information (referred to in this document as “attributes”) and have agency over who that information is shared with and purpose for which it is used.

DIS is concerned with allowing individuals to use digital identities to access digital public services in Scotland, referred to as “Relying Parties” (RPs). Individuals will be able to use digital identities for identification, authentication and authorisation. Attributes, in particular, will be used to demonstrate entitlement to a service. They may also help to reduce the friction that individuals would otherwise experience when accessing digital public services.

## 2.4 Individual needs

The approach to digital identity must take into account the needs of all individuals who may differ in their:

- access to identity evidence sources needed for identification
- access to digital technology
- confidence in the use of technology
- attitudes to privacy including differing views over which organisations can be trusted to provide them with digital identities.

The approach needs to be inclusive and responsive, so that if an individual encounters an issue, resolution of this issue is straightforward, avoiding the need to perform steps multiple times and ensuring legitimate access to digital services is not denied.

The approach must ensure that all of these concerns are addressed, not least aligning with the SG privacy principles[3].

## 2.5 RP needs

The approach must also address the needs of digital public services. These will include:

- Services requiring different combinations of identification, authentication and authorisation services.
- Services requiring different levels of assurance.
- The ability to fit digital identity at the optimal points in the customer journey, dependent on the service in question.

[3] https://www.gov.scot/publications/identity-management-and-privacy-principles/

# 3 DIS SERVICES ROADMAP

**QUICK READ:**

DIS must address competing short term and long term goals. In the short term, DIS will focus on providing identification and authentication services to satisfy the immediate needs of digital public services in Scotland. This includes the need to support the delivery of Social Security in Scotland as part of the Scottish Social Security Act (2018). Once fully operational, Social Security Scotland will administer a total of 14 benefits, supporting 1.4 million people and providing approximately £3.5 billion in payments every year. In the longer term, DIS recognises the potential transformation that could be enabled by providing individuals with the tools to make their data (attributes) portable. DIS is developing a roadmap that will allow it to meet the short-term requirements, but with a view to more significant transformation in the longer term. The speed of this transformation will depend both on the ambition of public services in Scotland and the readiness of the market.

The approach taken by DIS must address a number of competing concerns. The aim is to provide a service that can support a wide range of current and future needs. Some of these needs are known, others will emerge as digital services develop and as the utility of digital identity becomes apparent.

Furthermore, the digital identity industry itself is far from static:

- **Identification** – new mobile ID&V solutions, alternative data sources
- **Authentication** – use of mobile, FIDO
- **Authorisation** – giving the customer much greater control over their personal data and making that data verifiable.

During the Discovery Phase a conceptual architecture for DIS was developed[4] that aimed to:

- Provide an approach that can work with the identity services and providers that are available commercially in the market today; and
- Be flexible enough to support anticipated future services that will be needed to realise the full potential of digital identity across public services.

For the Alpha project, a PoC was built that focuses on the immediate needs of public services in Scotland.

This chapter describes the potential future state, suggests a possible roadmap towards that future state and summarises what was demonstrated by the PoC.

## 3.1 Future State

In the future, we expect digital identity to provide the means for individuals to share assured and verifiable data about themselves with whichever digital service they wish to interact with in a way that is secure, privacy-respecting and convenient.

[4] https://www.gov.scot/binaries/content/documents/govscot/publications/minutes/2018/05/online-identity-assurance-programme-board-papers-23-may-2018/documents/2666250e-6220-41c6-88fb-68d86b7cc763/2666250e-6220-41c6-88fb-68d86b7cc763/govscot%3Adocument/Technical%2BSolution%2BCharacteristics.pdf

This includes:

- Portability of data between organisations (but shared via the individual)
- Flexibility to support a growing set of use cases leveraging a growing range of attributes, although early use cases are likely to be focused on a much narrower set of data – the data used to identify an individual.

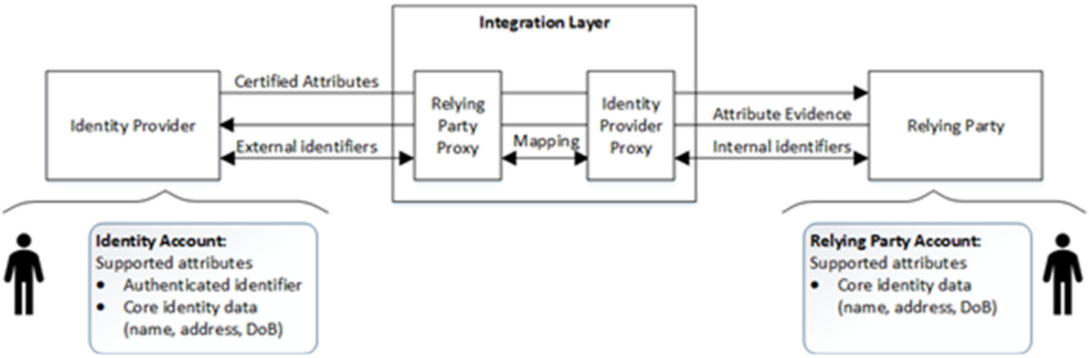
Enabling attribute-driven services will bring several benefits to DIS:

- 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 agency over their data, in line with 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.
- Attributes may allow services to be personalised.

## 3.2 Migration Stages

The speed at which the Scottish public sector can move towards the above future state for digital identity will depend on how quickly digital identity is adopted, the rate of digital transformation more broadly and the development of the market. Whilst the timing of these elements is uncertain, DIS should envisage stages of development in its own services – allowing it to meet short-term requirements with a view to evolving the service towards the longer-term vision. Three stages are proposed:

### 3.2.1 Stage 1 - Focus on core identity attributes



Initially DIS would focus on allowing individuals with an "identity account" to use it to access public services. Individuals without an identity account would be able to obtain one. There are a number of potential providers of such accounts, which provide individuals with a re-usable digital version of their core identity attributes (name, address and date of birth).

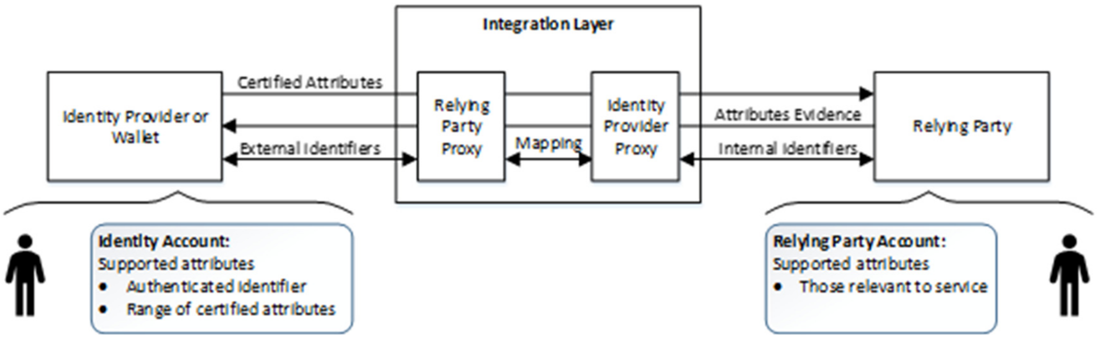
These core "certified" attributes would likely be established through a bundled identification process similar to that followed by GOV.UK Verify providers today. The IDP would need to show that the processes they follow meet the requirements of GPG 44 and 45 (and any addendum to these that DIS defines).

Where identification cannot be completed successfully online, DIS may facilitate the identification of the individual by allowing information concerning identification steps undertaken by Scottish public services to be shared with the IDP. This would result in “attribute evidence” flowing from the RP back to the IDP enabling individuals to achieve a higher level of assurance. Any such process would clearly need to address all associated data protection requirements, privacy and liability concerns.

Authentication of the individual, when accessing services, would be performed by the IDP and communicated to DIS. The exact mechanism for doing this is to be defined. The intention is that the mechanism will be designed to minimise the personal data being passed, to prevent surveillance or collusion that would contravene the SG privacy principles.

Stage 1 itself may need to be delivered in phases in order to meet the various critical path dependencies within wider SG initiatives. The detail of these phases is beyond the scope of this document.

### 3.2.2 Stage 2 - Controlled use of attributes



The next development of DIS would increase the number of attributes supported. This would require the attribute standards to be developed. These standards would provide a means to gain assurance in the quality of attributes. Early work has been done in this area by GDS and others but further development is required.

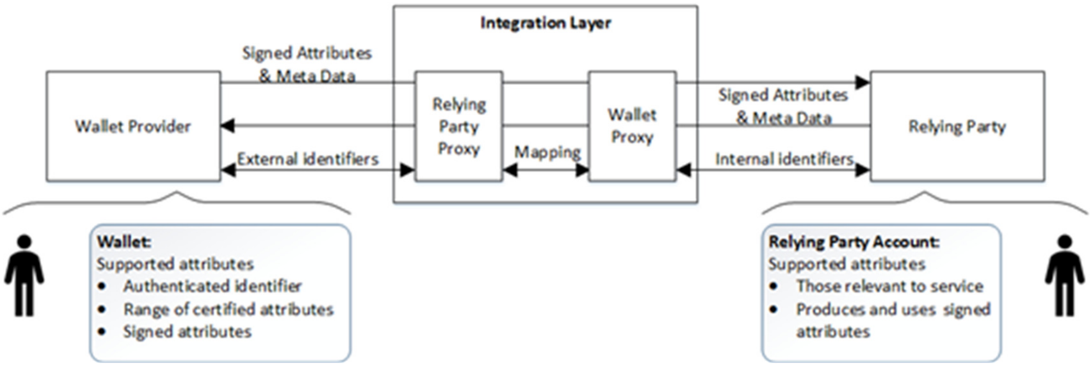
Following the current identity assurance paradigm, in addition to attribute standards there may also need to be certification arrangements put in place so that attributes can be assigned an assurance level that can be relied upon. The need for such certification processes could constrain the speed at which attributes can be adopted.

For attributes that are generated by Scottish public services to then be consumed by Scottish public services, it may be possible for DIS to bypass the need for such certification processes, so long as the RPs consuming such attributes are aware of the limitations and risks of such an approach. DIS will still need to ensure that whatever approach is taken, appropriate specifications are in place. As far as possible these should align with emerging attributes standards.

DIS will need to need to place constraints on management and use of attributes by IDPs, especially for attributes originating from public services. These constraints could include, for example:

- Requiring that certain attributes are for public sector use only.
- Ensuring that Scottish public services are not liable for use of public data in the private sector.

### 3.2.3 Stage 3 – Open verifiable attributes



It may be possible to address the scalability concerns with attribute assurance, and in particular certification arrangements, through the use of verifiable attributes. By verifiable attributes we mean attributes that:

- Are digitally signed so that the originator of the attribute can be cryptographically verified.
- Contain metadata describing the process that the originator employed to establish the attribute in the first place.

This may allow RPs to form their own decisions concerning the suitability of the attribute to meet their needs.

This approach would still be able to align with the standards used in the earlier stages (including GPG 45 and the emerging attribute standards). The same set of rules would determine the quality of an attribute. However, the process of calculating an attribute assurance score may be done by the RP rather than an IDP.

In a fully developed attribute ecosystem, organisations will take on multiple roles. Any organisation an individual interacts with could be both a RP (needing the individual to share attributes obtained elsewhere) and an attribute provider (giving the user attributes that they can use elsewhere). As a consequence the current concept of an IDP would change.

Firstly, organisations that are currently IDPs will become attribute providers alongside other organisations. Secondly, the limited attribute management currently performed by IDPs would need to be expanded. Individuals will need to be given tools to manage, use and protect their attributes, regardless of where those attributes come from. This will likely require something more like a “wallet” than an “account”, using person-centric strong cryptographic controls. This reflects overall direction of the digital identity market – as it appears today.

# 4 IMPACT ON INDIVIDUALS

**QUICK READ:**

The needs of individuals are central to DIS. The entire initiative is concerned with enabling individuals to access digital public services in Scotland with convenience, privacy and security. Consequently, the DIS team has undertaken significant user research and worked with privacy interest groups to test how individuals perceive digital identity and to understand their needs and expectations. The focus was on the anticipated short-term use cases that DIS will support. Further user research will be needed as DIS evolves.

In the user research, participants were able to understand the need for digital identity as well as point out potential areas of concern. The findings appear to broadly support the direction of travel of DIS, although it is clear that significant effort will be needed to show individuals that services are safe and reliable.

User research plays an important role in exploring the use of identity services in a public sector context in Scotland. During this Alpha project, a programme of user research has been used to:

- Validate and extend the user needs identified in Discovery.
- Get citizen input into the online and offline user journey for identification.

## 4.1 User research scope

The scope of the user research was broadly defined to complement the technical proof of concept that ran in parallel, by looking at:

- The end-to-end journey of a citizen going from having no digital identity to have one with level of assurance of LoA2 (see section 6.2.6).
- The use of in-person verification as a specific way to identify individuals who are unable to complete a fully digital identification journey.

## 4.2 User research approach

The SG team has run regular rounds of user research throughout the Alpha. The approach has been rapid in order to elicit feedback on aspects of the user journey, apply learnings and iterate the design quickly. The team has used wireframes to enable citizens to provide feedback and understand how the design and content can impact their experience of the service.

This approach allows for rapid and actionable learnings about how the user journey should be shaped. We recognise that this approach has some limitations, in particular that the rapid nature of the process does not allow for in-depth research and analysis.

## 4.3 User research scenarios

The scenario used for the online journey involved applying for a social security benefit and being required to get a digital identity at LoA0 at the beginning of this journey, raised to LoA2 by the end. This journey was selected, as it is expected to be an early use case for DIS.

This user journey also highlights the opportunities arising from separating Authentication from Identification. Based on feedback from the SG Expert Group and learnings from GOV.UK Verify, this approach is believed to be important in making services more flexible and accessible.

Aspects of this journey have been refined, specifically around consent and data sharing, understanding why an LoA0 digital identity has to be established and choosing an IDP.

Research for in-person identification involved looking at what people would be willing to do in person to identify themselves against an online identity. For example, sometimes a person may struggle to apply for a benefit such as Child Disability Living Allowance through the normal online channels. This could be because they do not have the requisite documentation, or simply because they are not confident in working through the online application process. In order to ensure that people can access the benefits that are due to them, some kind of in-person process could be provided. This would enable the claimant to associate their digital identity with their real world presence. This could be offered via a number of different providers with physical premises e.g. Post Office branches, local authority offices. It would not necessarily have to take place on SG sites.

## 4.4 User research constraints

Given the time constraints of having only three months for the Alpha, the user research has been limited to using wireframe mock-ups to replicate the user journey for feedback. This meant that some key areas could benefit from further investigation, including:

- Extending the work already done with the Pension Agency and local councils to investigate the Service Provider user journey.
- The IDP process within the Social Security application process.
- The full experience of getting an LOA2.
- Verification by a proxy.
- Journeys that do not follow the “happy path” i.e. failure to verify.
- Accessibility.
- Sharing of attributes and associated metadata.

## 4.5 User research questions

A succession of user engagement sessions were held in different locations, with individuals from a variety of backgrounds, including some with physical impairments. There were a total of six workshops, with 26 participants in total:

- 3 workshops with Social Security Experience Panel members in different locations – including a mixture of those who have conventional identity evidence and those who do not.
- 1 workshop involving people who all have access to documents, half of the group having applied for a benefit in the last two years.
- 1 workshop involving people who had specifically expressed concerns about sharing their personal data online.

- 1 ad hoc workshop with individuals in a First Stop Shop.

These sessions involved structured interviews, followed by discussions around screens showing a choice of four IDPs (myaccount, Post Office, Experian and Digidentity). These providers were selected in order to provide a mixture of well-known brands, non-consumer brands and a government option. They are simply representative examples for user research and any service implemented by the SG might include an entirely different set of IDPs. In these sessions, the following questions were explored with attendees:

- What are citizens' attitudes, needs and expectations around sharing their personal information?
- Why would citizens trust a private or government identify provider (IDP)?
- What concerns would citizens have about using a private IDP?
- What can be done to alleviate those concerns?

These questions were selected to develop the user journey on the lead up to selecting an IDP and elicited a wide range of responses across several themes.

## 4.6 User research results

### 4.6.1 Re-usability and processes

**Citizens want a reusable ID account**: The benefit of having an IDP account is important to convey ("what is in it for me"?). When this was explained, participants actively understood the benefits of setting up an ID account they can use to access other public services.

**IDP log in was accepted**: Participants did not object to having to register with the Post Office to create an "identity account" at the start of the application process. Participants would look for a brand that they had an account with. Some participants already had a myaccount, i.e Young Scot or concessionary travel and gave that as a reason for selecting. Another had a current account with Bank of Scotland (in the prototype as an IDP to gauge reaction) and would want to log in to that account.

**Sources of identity data were potentially a concern**: A participant who had a carer who was their Power of Attorney said they would find it very difficult to prove who they were in real life as they had no bills, bank account or photo ID. They felt they had a stronger online presence. Participants frequently cited their concessionary travel via the National Entitlement Card as photo ID. One participant had even used theirs as their photo ID for an internal flight in the absence of anything else.

**There were no strong requirements regarding the point in the journey at which consent was established**: Participants appreciated having a smooth journey, with consent handled at the IDP stage.

**Participants tolerated the double entry process to apply for the service**: In the journey citizens would need to fill in their details for the benefit application, and then again for the identity check. In the mock-up participants accepted this, however it should be noted that this was not a full end-to-end application.

**It was necessary to manage expectations around the LOA0 process**: On the prototype we had three reasons for setting up an LoA0 account. Participants were advised that setting up an

LoA0 account would enable them to perform the following tasks as part of their benefit application:

1. Save their application – so they do not have to fill it all in at once.
2. Prove their identity online – so they do not have to send in identity evidence.
3. Apply for other benefits or other government services

Most participants could remember the first (save and resume) but not the other two. When pressed, participants did understand that they would have to complete a second part at the end of the application and that they had not yet verified their ID. Save and resume was recognised as important functionality for a social security process.

### 4.6.2 Familiarity and acceptability

**Participants wanted choice but not unfamiliar options**: Many participants did not expect to create an account and have their identity verified outside of a government body. In principle, having a choice of IDP was liked, giving people who did not fit into the mainstream more options and allowing for personal choice over provider. Most participants looked for an IDP they had an existing relationship with.

**Branding was important**: Participants were uncomfortable when they had never heard of an IDP and had to judge by branding. The Post Office is a recognised brand and is considered "local" because of their branch network. However, some citizens selected myaccount, even if they did not recognise the brand, because it was described as "government" and therefore could be considered trustworthy. Private IDPs generally were viewed with some suspicion, as they would be looking to make a profit.

The branding employed at the integration layer is also important. In user testing, the integration layer pages were unbranded. Some participants referred to this as "limbo", others said they expected to see the IDP brand. This should be examined with further user testing

**Financial providers were more acceptable than social media**: Participants would not want to see social media accounts (Facebook, Twitter, Google) as IDPs. Financial bodies were considered more authoritative, although some citizens were clear they did not want to mix finances and government. One participant said that they were worried that if their bank knew they were applying for a benefit it would impact their chance of being offered a loan. However, participants also felt that their own bank had a high standard of verification so it would be an "easy" option to log into their own online banking.

**The precise role of the IDP was hard for participants to grasp**: Participants' mental model is that they verify their identity with a body who has existing information about them, which is why we saw people considering who might already know them or who they have an account with. Citizens would need reassurance that the SG has chosen to offer them specifically selected private partners and that these partners are to be trusted.

### 4.6.3 Clarity and simplicity

**Citizens need to understand why they are being asked for information**: There was confusion over why participants were being asked for information about their financial history as part of the Post Office process. This was confused with credit checking.

**IDP content impacts the citizen's understanding and experience**: The journey had screen shots from the Post Office verification process. This process was selected because it was readily available and believed to be sufficiently representative of other IDPs for the purposes of this research. The Post Office knowledge page referred to the “credit facility”, which was unclear to participants. Where public bodies such as Social Security are aiming to produce content at or below the average reading age, IDP content must be in line with this.

**Participants liked to see confirmation about the data which is being shared being explicitly shown on the screen**: This included both highlighting what was going to be shared at the start of the process and confirming sharing choices at the end. Users were observed to simply click through this part of the process without any noticeable hesitation or major concern. However as the prototype used test data it is quite possible that participants were less cautious than they would ordinarily be.

### 4.6.4 Privacy and control

An expert workshop was used to consider questions of privacy and control. This highlighted a number of key themes:

**Managing personal data**: The group made a very strong point around users being able to manage the data they are sharing. This includes users being able to view, change or revoke their data. This aligns strongly with user research that highlighted how some users would like to be able to view the data that is being shared and more importantly, ensure it is accurate to avoid incorrect data being used as part of applications for services. Data shared for identity purposes only should not affect eligibility assessment but subsequent attribute sharing could have an impact. The data being used to assess eligibility, needs to be accurate to avoid overpayment. Being able to manage data is closely linked to the privacy aspects of the service.

**IDPs**: Similar to questions asked by citizens during user research sessions – the group were interested in what benefits the private IDPs received for providing the identity checking service and consequently their motivation and investment in ensuring the journey works for users and our ability to influence the journey. This has strong connections with the ‘trust’ aspects of selecting an IDP discovered during previous research. The group also questioned which part of the Post Office was dealing with identity. This draws parallels to the user research with citizens who were often looking for existing relationships, several assuming that they could login with an existing account to verify their identity, e.g. logging into their digital banking account if their bank was an IDP option.

**Designing for difficult experiences**: The group discussed designing a service that people may interact with under duress/distress – especially services with sensitive subject matter such as cDLA. This included emphasising that financial IDPs do not perform credit checks when verifying identities and that the data being shared will not affect other benefits or legal decisions. As before, this aligns with views from participants in other research sessions as they expressed their preference to keep different aspects of their lives separate e.g. financial matters and benefits or social media and benefits.

### 4.6.5 In-person identity verification

Previous studies of in-person identification are of interest and potentially complementary to the user research undertaken by DIS:

- https://oixuk.org/projects/walk-in-assisted-digital-on-the-high-street-discovery/
- https://www.charleypothecary.com/facetoface-identity-proofing

## 4.7 User research outcomes

The results of the research in many ways reflect the fact that digital identity is a new concept to most individuals.

**Understanding of concept**

The precise role of an IDP was hard for some participants to grasp. Some of the content was considered challenging for some participants too. It is essential, therefore, that DIS provides clear guidance that is accessible and understandable for all individuals. Incentives should also be considered for people to read and assimilate the information being provided.

**Choice of IDPs**

Participants' attitudes to the choice of IDP appeared somewhat contradictory. On the one hand participants were in favour of offering choice, but, in practice, when asked to make a choice most participants opted for the government provided IDP.

Participants were cautious of private sector IDPs although they viewed certain organisations (e.g. banks, Post Office) as being potentially suitable. The relationship between the private sector IDP and the government and between the private sector IDP and that same organisation's other interests, were not clear to participants. So this is another area where education will likely be needed.

Participants did not trust social media firms to deliver identity services. Individuals had substantial concerns regarding data sharing and did not see these firms as potential IDPs.

**Identification vs Authentication**

Participants were accepting of starting the user journey at LoA0 (as defined in section 6.2.6) and only subsequently increasing this to LoA2 (as defined in section 6.2.6). This shows that the decoupling of different aspects of digital identity is acceptable to users, so long as the user journey is smooth and well understood.

Participants liked to see details of data being used both before and after they confirmed a transaction. This gave them confidence in choosing to complete the transaction. It also gave them reassurance that it had completed successfully. However, when questioned later, it was unclear whether individuals had fully grasped the extent of the information being shared. Some thought that all information entered (e.g. passport number) would be shared.

## 4.8 Potential future user research

This research was intended to support the basic user journey described in this paper. In order to support future developments, the following research might be considered:

- Research into individuals' understanding of managing the portability of data between organisations:
    - Understanding whether individuals regard this as desirable.
    - Exploring the role an individual is willing and able to take in any data migration.
    - Identifying ways in which the individual can meaningfully express their wishes.
    - Exploring ways in which the individual can verify that their wishes have been actioned as intended.

- Helping individuals determine the trustworthiness of an RP with whom they may wish to share data.

- The ability to support "tell us once":
  - Exploring user perception of the nature and desirability of the "tell us once" process.
  - Exploring the logistical challenges of managing consent to achieve "tell us once".
  - Exploring the privacy requirements and means of achieving them around "tell us once".
  - Exploring the practical constraints associated with implementing "tell us once" within RPs' processes.

- How best to support individuals in protecting their privacy and meeting the privacy principles of the programme including, for example:
  - Approaches to consent management
  - How best to provide redress and to enable correction of errors
  - Use cases where consent is not the basis for processing data under GDPR.

- Flexibility to support a growing set of use cases leveraging a growing range of attributes, although early use cases are likely to be focused on a much narrower set of data – the data used to identify an individual:
  - Exploring the individual's perceptions around handling their own attributes.
  - Exploring the individual's desire to handle their own attributes.
  - Exploring any sensitivities in this context, such as privacy and control.
  - Exploring ways of implementing statutory obligations with minimal impact to the user journey.
  - Assessing different individuals' abilities to manage their own attributes in different contexts.
  - Identifying issues arising from the involvement of multiple organisations.
  - Exploring ways of handling these issues with minimal impact to the user.
  - Exploring ways in which individuals can understand and engage with the metadata associated with their own attributes.

- Research into user journeys that diverge from the "happy path" due to:
  - Insufficient documentary evidence.
  - Issues with working through the process.
  - Issues with engagement.

  - Implementation of a proxy process so that a trusted person can represent the individual.

- Research into the extent to which RPs:

  - Can create online identities face-to-face.

  - Are willing to reuse identities created in the face-to-face environment by other organisations.

  - Would be prepared to trust attributes established by other organisations.

# 5 IMPACT ON THE MARKET

**QUICK READ:**

The SG's guidance for the public sector on the design, development and delivery of future digital public services[5] includes the principle to "re-use, before buy, before build". Sourcing digital identity services from the private sector is in keeping with this. However, the provision of digital identity differs from many other digital services that the SG may deliver. It is not the case that the SG can go to the market to find a single vendor who will meet their needs. That would amount to a single SG identity service which would be against the identity assurance principles quoted above (in section 2.2). Instead it needs to engage with the evolving digital identity market, so that individuals can choose a digital identity that works for them to access Scottish public services. To achieve that goal DIS needs to find the optimal way to engage with the market, which could include the SG providing identity services alongside private sector providers.

Alongside the Alpha Project, Consult Hyperion held confidential conversations with a representative sample of potential suppliers to DIS. The goal of these conversations was to understand the current state of the identity market and to consider how the SG should engage with it. This section considers the key findings from those discussions.

## 5.1 DIS - Scheme or RP

Perhaps the most important consideration is how DIS positions itself. From the outset, the goal has been to benefit from and align with developments in the market. This should result in a service that is lower cost and more sustainable.

DIS can be positioned as either:

- a **Scheme**, where it governs the rules and operation of the end-to-end identity service.
- an **RP**, or "Master RP" for Scottish public services, where it uses identity schemes and services in the market but does not govern end-to-end identity services.

The choice of approach could have significant implications on the cost of operating DIS and the way the market engages with DIS.

### 5.1.1 DIS as a scheme

DIS could be positioned as a scheme. This would suggest that DIS would define and control all aspects of the identity service - business, regulatory and technical. This could involve:

- Setting commercial terms for participation including fees, liability and dispute resolution.
- Defining and owning the technical, assurance and operational rules and standards.
- Defining and operating a compliance programme to ensure all providers meet required standards.
- Operating the central infrastructure that underpins the scheme.

Whilst DIS has an interest in all of the above, to do so in a fully controlling way would imply:

[5] https://www.gov.scot/publications/scotlands-digital-future-high-level-operating-framework-version-2/pages/2/

- DIS has a team of the appropriate size and with the necessary skills. The evidence from GOV.UK Verify suggests this would be a significant undertaking.
- DIS generates sufficient transactional volumes (and revenue) to justify it being its own scheme. Compared to the volumes that could potentially be generated in the private sector this seems unlikely.
- The market would need to develop DIS specific services, the cost of which would need to be borne exclusively by the public sector.

### 5.1.2 DIS as an RP

DIS could act as an RP (or "Master RP") on behalf of Scottish public services. This could include:

- DIS participating in other schemes following their rules including GOV.UK Verify and one or more private sector schemes, should they emerge.
- DIS buying digital identity services from other providers outside of a formalised scheme.
- Aligning with industry standards (and external certification arrangements) in order to ensure services and providers chosen are of suitable quality.
- Operating an interface layer for connecting to IDPs and schemes.

This approach would be less demanding for DIS but with the following implications:

- DIS would have less control over the future direction of the schemes and providers it works with.
- DIS would need to address any differences that exist between the services offered by external schemes or providers. Depending on the nature of the differences this may be non-trivial.

### 5.1.3 Recommendation

The difference between these two approaches may not always be clear cut. However, as far as possible DIS should be an RP. In doing so it should seek to align with and adopt industry standards rather than defining its own. This will avoid the industry needing to build proprietary solutions that DIS would need to pay for.

This approach should reduce the size of team required to operate DIS. DIS will still require digital identity expertise but the need for this should be significantly less than if DIS was seeking to create a new scheme in its own right.

As a significant RP, representing all public services in Scotland, the requirements of DIS will of course carry some weight in the market. Where the requirements of DIS are not met by standard market solutions, DIS may choose to define specific requirements to meet their needs. The aim will be to leverage standardised services as far as possible however.

## 5.2 Number and type of IDPs

DIS will need to determine how many IDPs to work with to provide the right amount of choice for individuals. A number of approaches could be taken.

### 5.2.1 Private Sector IDPs only

In the UK, there is a nascent market of digital IDPs and the potential for other organisations to seek this role (e.g. as a value add to complement other services being offered to individuals).

One approach for DIS would be to support private sector IDPs only. In other words, any individual wishing to use a Scottish public digital service would be required to have an account with one of these private sector providers.

In this approach, the aim would be to treat all IDPs equally and give them the same opportunity to acquire customers (i.e. individuals accessing DIS). This would create a competitive environment that would help to drive down the costs of using these services, so that ultimately they become commoditised.

The viability of this approach depends on the digital identity market developing and maturing sufficiently quickly. DIS would also need to take care to ensure that all individuals (especially people who may struggle to provide evidence of their own identity) are catered for.

### 5.2.2 SG provided IDP only

A second approach would be to create a single Scottish public services IDP. This could be sourced from one of the existing commercial providers or elsewhere.

This approach is not believed to be viable for DIS for a number of reasons:

- The approach would not give choice to individuals.
- There would be concerns about privacy, as the single provider, whether outsourced or not, would in effect become a single central identity system for Scottish public services.
- The approach would not create re-usable digital identities (that are reusable in the private sector) and therefore would be unlikely to benefit from commodity pricing.

### 5.2.3 Combination of private sector IDPs and a SG provided IDP

A third approach would be to build a hybrid of the above two approaches allowing individuals to choose from a selection of private sector IDPs or a SG provided IDP.

For this to work, DIS would need to ensure there is sufficient incentive for commercial IDPs to participate. One way to achieve this could be to position the commercial IDPs and the SG provided IDP differently. For example:

- If use of the SG IDP is limited to public services, private sector providers would be able to market the flexibility and utility of their services.
- If the SG IDP focuses on serving individuals without common forms of identity evidence, there would be less of an imperative for private sector providers to address those individuals, although they could choose to do so.

Careful service design and user education would also be necessary to ensure that individuals understood the implications of the choice they would make.

A key advantage of this approach to DIS, is that the publicly owned IDP would provide a contingency in case the developing digital identity market is not sufficiently ubiquitous or fails to reach the critical mass where it becomes self-sustaining.

### 5.2.4 Role of GOV.UK Verify

In parallel with the above options DIS will need to determine how it interoperates with the IDPs that are part of the GOV.UK Verify scheme - whether to engage those IDPs directly or via GOV.UK Verify. There are pros and cons with each.

Engaging with GOV.UK Verify IDPs directly will allow DIS to have more control over the digital identity services that IDPs deliver. For example, DIS may be able to develop a more granular approach to levels of assurance (see section 6.2.6) than is supported via GOV.UK Verify (at least today). It will also allow DIS to have greater control over the user experience ensuring that the specific requirements of individuals are met, as far as possible.

Engaging via GOV.UK Verify will be a simpler commercial engagement. A key issue for DIS, with this approach, will be the future direction of GOV. UK Verify. DIS will only be one voice regarding any future development of GOV.UK Verify.

### 5.2.5 Recommendation

DIS should pursue the hybrid approach providing individuals with a choice of private sector IDPs or a SG provided IDP. The SG IDP would be created for public sector usage only and should focus on plugging gaps in the reach of private sector IDPs. It will also provide a contingency in the event that the IDP market does not develop sufficiently.

For this approach to work it is critical that private sector providers see sufficient benefit in being involved. The SG should work with potential providers as it develops and delivers its detailed roadmap, to ensure the full engagement with the market in order to achieve the best outcome.

## 5.3 How to engage private sector IDPs

Assuming that DIS does seek to engage private sector IDPs, it will need to determine the most appropriate way to do this. Broadly speaking there are two approaches.

### 5.3.1 Bilateral arrangements

DIS could seek to contract with each private sector provider separately, negotiating separate terms with each. Whilst this may allow the SG to negotiate the best price possible with specific providers (assuming the negotiations are successful), it is likely to be an involved process and could lead to an unpredictable business model. The cost to the SG of externally sourced identity services would depend on the provider selected by the individual at the point they signed up for the service, or when they choose to switch to another provider.

### 5.3.2 Standardised pricing

DIS could seek to establish a standard contract, with standardised terms and pricing and require each private sector provider to adopt them. This would provide a more predictable business model and should simplify negotiations with providers. They would be required to “take it or leave it”.

Care would be needed in setting the standard terms and pricing to ensure that private sector IDPs are incentivised to support DIS.

The pricing itself could be either:

- **Outcome based pricing**: where IDPs are paid for achieving a result, e.g. completing identification of a customer to Level of Identification of “Medium” (see section 6.2.6).

- **Componentised pricing**: where IDPs are paid a set amount for each of the tasks they may undertake, e.g. checking a passport, calling a credit bureau, etc.

In general, we believe outcome based pricing is better. It would be less complex to administer but more importantly incentivise providers to be creative. Of course, the SG would want to incentivise providers to be creative in developing solutions that work for everyone, as opposed to focusing on individuals that are easier and cheaper to serve. This would likely mean that a single flat price would not be sufficient. Instead, the SG would need to develop an outcome-based pricing model that takes into account the additional costs of identifying some individuals, whilst ensuring competitive, commodity pricing for the rest.

Getting the pricing and tiers right may take time, especially as the market develops. However, we believe that participation in DIS should be of value to all IDPs, adding increased utility to their identity services and helping them achieve the critical mass they will need to ensure the ongoing commercial viability of their services. We believe it is essential that the market focuses growth towards critical mass rather than being encumbered by short term revenue concerns. To be successful the digital identity market must achieve scale, with the volumes ensuring that services are financially sustainable.

### 5.3.3 Recommendation

Finding the optimal commercial model and pricing for DIS will require careful consideration. IDPs must be incentivised to behave in a way that supports the objectives of DIS. For example, if IDPs were to provide solutions that catered for individuals who can be identified at low cost, in order to maximize profits, this would potentially leave significant numbers of individuals not catered for.

Furthermore, the optimal pricing will likely change as the service grows and develops. The optimal pricing when volumes are low, to provide the right incentives, may not be optimal when the service has grown. The prices that DIS can achieve will also be dependent on the development of the wider digital identity market.

Nonetheless, based on the consultation with OIX members we believe DIS should pursue standardised pricing that is outcome based with defined tiers for different groups of individuals. This will make the business case for DIS more predictable and simplify negotiations with IDPs.

DIS should seek to align with other public sector organisations who are buying digital identity services both in terms of commercial model and pricing. As the market grows, it will be important to align with other RPs to ensure that DIS benefits from commodity pricing.

## 5.4 Leveraging Scottish public sector identity evidence sources

As discussed below (in section 7.2), the DIS may be able to provide private sector IDPs with access to specific identity evidence sources that will help them create digital identities for individuals.

For example, in-person identity verification is already performed by the public sector for access to certain services. Allowing those checks to be accurately reflected in an individual's chosen IDP may provide those individuals to obtain verified digital identities more easily.

Where such sources are made available, they will reduce the cost to private sector IDPs of performing identification of individuals. This saving should of course be passed back to DIS (e.g. via a recharging arrangement). The value of the publicly provided identification assets to the IDP will depend on how the private sector IDP is permitted to leverage them.

There are two basic approaches:

### 5.4.1 Do not allow re-use of public sector evidence sources in the private sector

One approach could be that these sources can only be used for identification of individuals when accessing public services. This however is likely to be difficult to implement, requiring IDPs to ignore the fact that certain checks have been performed in certain situations. If the SG chooses to share fraud data with the IDPs it could create the nonsensical situation where an IDP knows that an identity is compromised but has to pretend it isn't.

It could also be confusing for individuals, in that they would have an identity account that works for some services (i.e. Scottish public sector) but not for others (i.e. private sector).

Perhaps most important is the fact that the public sector needs to play a role in enabling individuals to create secure digital identities as a public good. The same argument would apply to other UK identity evidence sources such as the Document Checking Service currently provided as part of the GOV.UK Verify scheme but which may be opened up in the future.

### 5.4.2 Allow re-use of public sector evidence sources in private sector

The alternative is of course to allow IDPs to re-use the evidence obtained from these sources in other contexts, such as in the private sector. This will provide flexibility to providers and convenience to individuals. Of course, depending on the use case the IDP may choose not to use the results from these assets or combine them with other identification processes in order to meet their requirements.

The commercial arrangements will need to reflect the additional benefits provided to IDPs and any liabilities that may arise, as well as protecting the interests of the individual in relation to their identity.

### 5.4.3 Recommendation

We recommend that evidence obtained from public sector identification sources should be reusable by IDPs in other contexts, with the individual's consent. This will provide the most benefit to individuals, providing them with portable digital identities that provide utility, convenience and security across all digital services. The goal should of course be to ensure that fair and reasonable commercial arrangements are in place for the re-use of those assets, which will likely include some kind of recharge arrangement.

## 5.5 Support for future roadmap

As discussed above, the digital identity market is evolving and the services offered by DIS itself will likely evolve as the service grows. In particular, giving individuals portable digital identities is likely to involve establishing ways for customers to also make their attributes portable. The provision of these attribute services may over time transform the role of the IDP, requiring the development or acquisition of new capabilities.

Whilst it is critical that DIS engage providers who can meet the requirements of early use cases, providers should be sought who can move with the market providing richer privacy-respecting attribute-based services in due course.

## 5.6 Summary

In summary then the following approach is recommended:

- DIS operates as a “Master RP” seeking to integrate with any appropriate schemes that develop in the market.
- DIS seeks to use multiple private sector providers but complements these with a SG operated IDP focused on, but not exclusively for, individuals who would find it more difficult to obtain a digital identity from a private sector provider.
- DIS sets a standardised pricing model for commercial providers, recognising that this will need to be tuned as the market develops.
- The standard pricing model should include recharge arrangements where identity evidence sources from the public sector are used.
- DIS should continue to engage with the market to promote the development of privacy respecting attribute services.

# 6 IMPACT ON STANDARDS

**QUICK READ:**

Standards play a vital role in making digital identity services interoperable. This includes ensuring that the services provided by multiple providers are equally secure and robust. They also ensure that the processes employed in establishing and maintaining a digital identity are clear, measurable and auditable.

DIS expects to align with standards in the market as far as possible. In particular, they expect to align with the standards used in other parts of the UK public sector (namely the GPGs). These standards are however not static. GPG 45 was recently reviewed and updated (in April 2019), GPG 44 is due to be updated and the UK government is actively working on standards for attributes. This section discusses the current state of these standards and considers what DIS should do to meet its needs.

## 6.1 Why are standards needed?

Standards are needed to ensure equivalence and interoperability across the identity service envisioned by the SG, and in the market more generally.

If the individual is able to choose an IDP, the RP needs to know the level of assurance that can be placed in the services provided (whether identification, authentication or attribute services) even though they may not have direct visibility or control of the processes employed by the IDP. Similarly, the citizen should not need to worry about whether the IDP they choose will be good enough for the service they are attempting to access.

It is essential that the standards used are pragmatic and based around the needs of RPs and the types of identity evidence individuals commonly hold.

## 6.2 Which standards should be used?

### 6.2.1 Digital identity standards in the UK

Digital identity standards are being developed by several groups in the UK:

- Good Practice Guide (GPG) 45 and GPG 44, published by the UK government have been central to the GOV.UK Verify scheme as well as having been adopted (or adapted) in various parts of government. These guidelines are intended to be applicable in the private sector and work is underway to show how they align with the requirements of financial services, for example.
- BSI is developing an umbrella national standard.

The SG intends to align with the standards developed by the UK government for several reasons:

- The needs of public services in Scotland are the same as the needs of public services across the rest of the UK.
- Scottish public services do not operate in isolation. Sometimes services will interoperate with UK public services that use the UK governments digital identity standards.

- By adopting the same standards the SG will be able to benefit from the standards expertise built up in GDS and avoid duplicating effort.

- Scottish citizens will interact with both Scottish and UK government departments, depending on whether powers are reserved or devolved.

### 6.2.2 GPG 45 (Identification)

GPG 45 (Identification) v3.0 was published by the UK Government Digital Service (GDS) in the context of GOV.UK Verify. Originally it defined 4 levels of assurance. To date most citizen facing services have required a level of assurance of 2 or less.

In April 2019, GPG 45 underwent a substantial revision - published as v4.1. This included writing the guidance in language that can be understood by both technical and non-technical audiences, providing requirements for remote physical comparison and the use of biometrics, and defining four new levels (low, medium, high and very high). The guidance breaks down the individual components of identification allowing each to be given a score. These scores can be combined together in different ways (“profiles”) to achieve the required level.

The result of the revision is:

- standardisation in the way the elements of identification are scored.

- flexibility in the definition of profiles, allowing for example, financial services organisations to define profiles relevant to them but based on standardised and measurable underlying capabilities.

The levels of assurance from the earlier GPG 45 map onto profiles within the new GPG. Level of Assurance 2, for example, maps onto two of the Medium profiles.

### 6.2.3 GPG 44 (Authentication)

GPG 44 (Authentication) v2.0 was also published (October 2014) by the UK Government Digital Service (GDS) in the context of GOV.UK Verify. It defines 3 levels of authentication. To date most citizen facing services have required a level of authentication of 2 or less.

### 6.2.4 Attributes standards

Standards for attributes are less mature. This sub-section 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**

The term attribute is used to refer to any quality or characteristic ascribed to an individual. Attributes will typically be established or 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 and make them available in 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 still to be determined and not the focus of this document. Instead this document is concerned with what a RP needs to know in order to be able to rely on an attribute for the purposes of granting access to a service. This will be RP and context specific. Attribute standards will help RPs determine that the attributes they receive meet their criteria.

**What attribute 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 attribute types.
    - Defining and describing metadata (data that describes attributes).
    - Defining formatting rules and encoding schemes for data and metadata.
- Provenance
    - Source of the data.
    - Whether the source is authoritative or not.
    - Process undertaken by the source to establish the data and whether that is auditable / audited.
    - Creation date and expiry or 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 RP.
    - Authentication of the individual at the point of attribute sharing.

**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, including:
    - **NIST SP 800-63C**: Provides guidance to the US government on integrity and binding in the context of federated identity. NIST has also published a proposed metadata schema for attributes (**NIST IR 8112**) which covers language and provenance.
    - **GDS Attribute Guidance**: Draft document providing outline guidance on provenance, integrity and binding, that is expected to develop into formally published guidance. This is likely to be a key input to DIS.

- **Industry standards**: The following are examples of industry developments related to attributes:
    - **W3C Verifiable Credentials**: Candidate recommendation covering integrity and binding and several aspects of language and provenance.
    - **OASIS COEL**: The “Classification of Everyday Living”[6] covers language providing a taxonomy of human behaviour events.
    - **Kantara Blinding Identity Taxonomy**: An initiative[7] to classify attributes that can be used to identify a person and therefore require “cryptographic encoding”.
- **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. Examples from the OIX membership include:
    - **Factern**: Seeking to develop a universal standard for metadata management primarily focused on language and provenance[8].
    - **Mydex**: Has defined numerous datasets covering a range of applications that define a language for attributes[9].
    - **Meeco**: Has published white papers describing their personal data ecosystem service that includes examples of language, provenance, integrity and binding[10].
    - **Etive**: As part of their digital logbook work have explored potential attribute sources in local authorities (so called “micro sources”) with a specific focus on obtaining data for identity verification[11].

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 all of the processes employed by attribute providers are sufficiently robust and where necessary, auditable?

**Developing attribute services in the short term**

The evolving state of attributes standards will be a challenge to the SG in the short term. The SG should, of course, seek to develop services that align with open standards to ensure maximum scalability and interoperability. Until standards reach a sufficient level of maturity and are adopted by providers in the market, the SG may be constrained in the attribute services it can build.

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. Work undertaken by Mydex, for example, suggests that there can often be local clusters of personal data. Where attributes are shared between public sector organisations that trust each other liability is arguably shared. It may therefore be possible, for example, to assume the provenance and integrity of attributes.

[6] https://docs.oasis-open.org/coel/COEL/v1.0/COEL-v1.0.html
[7] https://kantarainitiative.org/confluence/display/infosharing/Blinding+Identity+Taxonomy
[8] https://next.factern.com/project/protocol
[9] https://dev.mydex.org/data-schema/datasets.html
[10] E.g. https://www.meeco.me/whitepaper.html
[11] https://www.digitallogbook.org/what-is-digital-log-book/

Importantly, a closed system does not necessarily mean a proprietary system. Closed systems may help the SG to make early use of attributes, whilst waiting for the market to achieve a sufficient level of maturity both in terms of standardisation and available services. The SG should still seek to align with open standards wherever possible.

### 6.2.5 Consent Standards

Standards for consent management are being developed including by ISO[12] and Kantara[13]. The SG should seek to align with such standards in order that the consent processes presented to individuals are clear, understandable and consistent with how those processes work elsewhere.

### 6.2.6 Levels of Assurance

DIS will need to define the levels of assurance it uses, even if just to align with existing levels or standards in the market.

To provide sufficient flexibility for the range of services DIS is intended to support, DIS expects to define separate levels of assurance for identification, authentication and attributes. These can be referred to as:

- **Level of identification** – the strength of processes employed to ensure that an individual represented by an identifier being presented is real, unique and identifiable. DIS expects to align with the levels in GPG 45. In addition, a level of identification of "None" where the individual claims to be real but no validation or verification of the individual's identity has occurred.
- **Level of authentication** – the strength of authentication credential employed at the point an individual is attempting to access a service. DIS expects to align with the levels in GPG 44.
- **Level of attribute assurance** - the confidence that can be put in an attribute associated with an identifier, based on the originator of the attribute and the processes they employ. DIS expects to align with the levels defined by GDS as they become available.

For the Alpha PoC we used a simplified version aligned with the level of assurance construct currently employed within GOV.UK Verify, to make it easy to leverage solutions provided by OIX members for the PoC with minimal changes, as follows:

- LoA0 (Level of Assurance 0) which corresponded to a level of identification of "None" and a level of authentication of 2 (i.e. the customer has an account with an IDP with associated authentication credentials but no specific information about the customer has been validated or verified yet).
- LoA1 (Level of Assurance 1) which corresponded to a level of identification of "Low" and a level of authentication of 2.
- LoA2 (Level of Assurance 2) which corresponded to a level of identification of "Medium" and a level of authentication of 2.

[12] https://www.iso.org/standard/70331.html

[13] https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/ and https://kantarainitiative.org/confluence/display/uma/Home

### 6.2.7 Scottish requirements

The identity assurance requirements will vary between digital services and RPs. However, it has been confirmed that Social Security will need to align with “Medium” as defined in GPG 45 v4.1 (or LoA2 in the GPG 45 v3.0), so that is a useful benchmark against which to assess potential services and explore where issues may exist.

Achieving Medium is more straightforward for some people than others. The goal is to be able to:

- achieve Medium for all people that wish to access services requiring this level.
- do so in a way that is not burdensome or difficult.

### 6.2.8 Extending the standards

GPG 45 is already flexible in supporting several different approaches to ID&V. Aligning with standards will help the SG to obtain identity services at standard market (hopefully commodity) pricing.

If the SG wishes to provide or endorse alternatives that do not fit with the GPGs as currently written, a pragmatic approach would be to publish an addendum to the standards allowing alternatives to be used until such time as the standards can be updated to include the alternative methods – assuming they are acceptable.

# 7 MEETING THE STANDARDS

**QUICK READ:**

DIS needs the market to be able meet its standards in a way that provides sufficient reach, so that there are solutions that work for all individuals that may be need to access Scottish public services.

As it stands there are several gaps in the market. For example, providers may be able to achieve level of identification of “Medium” for a subset of the population, but could leave sections of the population not catered for.

DIS may be able to help bridge some of these gaps with identity evidence sources available within the Scottish public services. Ensuring that these evidence sources are aligned with standards will help to ensure that the digital identities that individuals obtain are both portable and reusable.

## 7.1 Why are standards needed?

The GOV.UK Verify IDPs by definition already achieve Medium for the services that they offer. However, based on the experience of GOV.UK Verify, these IDPs may not be able to reach Medium for all individuals.

There are other IDPs in the market who are not currently part of the GOV.UK Verify scheme. Gaps may exist for these too – both in terms of the Level of Identification, Level of Authentication and reach.

The following specific gaps are considered:

### 7.1.1 Availability of the Suitable Sources

While the GPG45 identity proofing process is well structured and based around widely available evidence sources, these sources may not be available to a sufficient proportion of the population to meet the needs of the SG. Common evidence sources such as financial credit history and passport information may not work for the financially excluded, retired and other groups. This has the potential to affect existing GOV.UK Verify providers, as well as other IDPs.

### 7.1.2 Availability of the Document Checking Service

To facilitate the delivery of GOV.UK Verify, the UK government made the Document Checking Service available. This however is not currently available to non-Verify providers – something which has sometimes been viewed as a barrier to achieving GPG45 LoA2/Medium. Although GPG 45[14] does not stipulate that DCS, is required to meet LoA2/Medium, lack of access to it will limit the options for non-Verify providers. DIS is therefore supportive of DCS being opened up to these providers, as this will provide greater choice to individuals.

## 7.2 Bridging the gaps

There is the potential to bridge these gaps, extending the reach of all providers, through the use of certain Scottish public sector data and services.

[14] Neither v3.0 or v4.1

### 7.2.1 In-Person Checking

The provision of a standardised and auditable in-person checking service would appear to be a pragmatic solution to bridge the gaps that exist with both Verify and non-Verify providers. This would provide a context within which verification could take place through a guided process, with the necessary audit trail. It could be used to support different organisations in the checking process and enable RPs to make better informed decisions on the data gathered during this process.

The same capability could also be used to provide an assisted digital process, supporting individuals for whom technology is a barrier to access services.

Potential sources of in-person identity verification services include locals authorities, who conduct identity checks for certain services (such as housing benefit), and the Post Office.

As part of the Alpha project, DIS prepared outline requirements for an in-person identity verification service. The aim was to distil from GPG 45 a set of capabilities that would need to be delivered by an in-person identity verification service, in order that such capabilities could be compared.

### 7.2.2 Scottish Identity Evidence Sources

Some public sector services in Scotland may be able to provide identity evidence sources, in addition to those IDPs can already access. These additional sources, which could potentially be provided via DIS, would enable IDPs to support a wider range of individuals. This will make DIS more inclusive and provide greater choice to individuals.

Examples of these are considered in section 7.4 below.

## 7.3 Other approaches

DIS aims to deliver digital identity services that work for a high proportion of individuals. It is likely however that there will be some individuals who are unable to obtain a digital identity with a sufficient level of assurance for the service they wish to access. Two alternative approaches that should be considered in these circumstances are vouching and waivers. Ultimately it will be down to the RP to decide when these approaches can be used.

### 7.3.1 Vouching

Where individuals have an ongoing relationship with a service provider, such as a local authority, it may be possible for a trustworthy worker at the service provider to vouch for the individual's identity. This already happens today for certain services. For example, social services will often know personally individuals accessing their services including hard to reach individuals such as those who are homeless.

GPG 45 does not explicitly support vouching. DIS should consider whether vouching can be codified in a way that allows it to be used for individuals who cannot provide standard forms of identity evidence. This could include:

- Defining the qualifications or role of the person permitted to vouch for another's identity.
- Defining acceptable relationships where vouching may and may not occur.
- Limiting the use of vouching, so that it is a last resort.

### 7.3.2 Waivers

When an individual is unable to obtain a digital identity with sufficient assurance there could be an impact on both the individual and the service requested:

- Impact on individual - this could vary from not being able to access the service at all to being required to access the service in a different way (e.g. over-the-counter instead of digital) or experiencing a significant delay.
- Impact on service - the service provider could suffer reputational risk if they have been deemed to let individuals down. Depending on the process followed the service provider could also be exposed to other risks, such as financial risks.

There may be occasions when access to a service can be given even though the usual identification (or authentication) has not been achieved.

For example:

- Lower risk services - the RP may be able to make a risk-based decision and allow services to be accessed even though the usual assurance requirements have not been satisfied. The RP may decide to restrict the level of access or monitor the access given.
- Risk to life - where a situation is life threatening (such as a call to emergency services) the usual checks may be bypassed. Today of course digital identity is not used for such services. In the future, any integration of digital identity would need to account for such requirements.

For high value services, such as those where there is a high risk of fraud, it is unlikely identity processes can be waived.

DIS should provide guidance to RPs that enables them to design service that make the optimal use of the DIS service, minimising the need for waivers but ensuring appropriate measures are employed when they are necessary.

## 7.4 Overview of specific Scottish public sector evidence sources

There are a number of assets in Scotland that could potentially help IDPs achieve the reach required by Scottish public services, as outlined below.

### 7.4.1 National Entitlement Card

The National Entitlement Card (NEC) supports access to a range of national and local public services. Certain services, such as Scotland-wide concessionary travel, are only available to qualifying holders of the NEC. Other services such as library or leisure memberships may offer a choice of using the NEC or not; it is up to the provider to decide what can be used to access the service.

The NEC is most widely held by older (60+) and disabled people and young people.

For older and disabled people, cards are issued by local authorities on receipt of a valid application for a service that uses the NEC. The process involves checking the identity of the applicant. Anecdotally, there is significant variation in these processes both in terms of the document combinations that are acceptable (as proofs of identity and residence) and the auditability of the processes themselves. As it stands today then we assume that the basic NEC would achieve a score of 1, as an evidence source in GPG 45.

### 7.4.2 National Entitlement Card – Young Scot

The Young Scot version of the National Entitlement Card complies with the requirements of the PASS[15] scheme for proof of age. The card is available to 11 - 25 year olds with 675,000 cards in circulation. The majority of cards[16] are issued via schools and involve the school vouching for their students. These follow strict audited processes to comply with the PASS requirements. Additional arrangements allow young people, who did not receive a card via their school, to apply for a card directly. The processes employed still have to comply with PASS. The Young Scot version of the National Entitlement Card, therefore appears to provide a strong evidence of identity.

On this basis, it appears that the Young Scot card could be a valuable evidence source in meeting the requirements of GPG 45. If combined with an API call to the NEC database, a cryptographic challenge-response to the card and / or inspection of the security features of the physical card, it would provide a valuable asset in identification and onboarding of young people into a digital identity system. Furthermore, transactional records such as use of public transport and payment for school dinners may provide activity history for the individual.

### 7.4.3 Identification Performed by Local Authorities

Local authorities are legally required to perform identification for claimants of Housing Benefit and Council Tax Benefit. From examining the particular processes employed at one local authority, the identification processes appear to be of high quality. Anecdotal evidence suggests that processes are not, however, standardised across local authorities. Detailed analysis would be required to assess whether the processes employed by local authorities are equivalent and to determine any gaps in meeting a medium level of assurance, as defined in GPG 45.

Standardising these processes across Scottish local authorities would be of value in itself, ensuring that systems are robust and create the potential for re-use and interoperability. A standardised approach would then also enable this capability to be leveraged in a common approach to digital identity in Scotland.

### 7.4.4 MyDiabetesMyWay

MyDiabetesMyWay (MDMW) is an online service provided by NHS Scotland to help support people who have diabetes and their family and friends. Enrolment to this service uses a vouching service in combination with a trusted data source. During an appointment at a diabetes clinic or at a GP surgery, the healthcare professional enters the patient's email address (if not already present on SCI-Diabetes) and clicks a button to verify the patient's identity and trigger the sending of an email to the patient's email address. On receipt of the email, the patient clicks a link to take them to an online web form. This verifies their email address, before they are asked to confirm their basic demographic details. The patient demographics entered are then checked against those held on SCI-Diabetes. This ensures that the email has been sent to the correct individual.

Today authentication to MDMW is performed using myaccount. As part of the enrolment the myaccount service performs an additional check against an extract of NHSCR[17] data. There are currently legal restrictions on this process, which will need to be resolved before it can be used to "seed" a digital identity.

[15] http://www.pass-scheme.org.uk/

[16] 80-90%

[17] NHS Central Register, access to which is governed by the Local Electoral Administration and Registration Services (Scotland) Act 2006 (LEARS Act).

# 8 IMPACT ON CERTIFICATION

**QUICK READ:**

Certification complements standards. Standards specify what an IDP needs to do. Certification demonstrates that they do it. To date the tScheme certification programme established for GOV.UK Verify is the prime example of certification of IDPs in the UK. There are examples elsewhere (e.g. Kantara).

Reuse of existing certification results would appear to be a pragmatic and low cost approach for DIS and in keeping with the way certification should work in an open market. There are specific additional steps that may need to be taken to have capabilities delivered for DIS that are not in scope of existing certifications.

## 8.1 Purpose of certification

In any collaborative scheme, participants are required to comply with specifications that ensure that the scheme functions correctly and reliably. Independent certification is often used to ensure compliance with those specifications. In a digital identity scheme this could include assessing the security of the scheme, the correct implementation of technical standards as well as assessing the processes employed for identification and authentication.

As discussed above DIS should not be viewed as a new scheme per se, with its own standards and certification arrangements. Instead the desire is to adopt appropriate standards and certification arrangements from the market. This should reduce the burden on the SG and market alike, allowing the re-use, where appropriate of standards and certification work already undertaken.

The SG may however have requirements that are not yet satisfied by the market and so some additional certification may be necessary to bridge any gaps.

This section provides an overview of digital identity certification arrangements today and considers specific additional steps the SG may need to take.

## 8.2 Digital identity certification today

GOV.UK Verify requires that IDPs are assessed by tScheme.

In simple terms, a successful tScheme assessment certifies that an organisation is doing what they claim to be doing. This does not in any way imply that the certification is sufficient for an organisation’s particular needs.

The tScheme process is managed in Stages:

- Stage 1 – Agree that an IDP’s policies are auditable and appropriate.
- Stage 2 – Audit the processes against the policies.
- Ongoing – Regular repeat audits (at least annually often six-monthly).

For GOV.UK Verify, GPG 44, GPG 45 and the Ops Manual act as a standard set of requirements against which all providers can be audited. In the event that an IDP wishes to do something non-standard (e.g. employ an identity evidence source not recognised by the GPG 45) then they will request a waiver from GOV.UK Verify. The basis of the assessment for a waiver is a risk assessment that the IDP will have undertaken to justify why their approach is sufficient to meet the requirements.

Other digital identity certification programmes, such as the Kantara Identity Framework[18], exist. As with the tScheme arrangements for GOV.UK Verify, these focus on identification and authentication as opposed to the broader assessment of attribute exchange.

## 8.3 Digital identity certification gaps

The following gaps will exist in the coverage of DIS requirements by existing certification arrangements:

- **IDPs who are not certified by tScheme**: This is likely to be the case for IDPs that are not currently part of the GOV.UK Verify scheme, including any SG provided IDP. The most straightforward approach for DIS to take here is to make tScheme certification against GPG 44 and 45 (and potentially the IPV Operations Manual[19]) a requirement. This would allow DIS to benefit from certification work already undertaken whilst bringing all IDPs up to the same level.

- **Recognition of identity assets provided by the SG**: For DIS provided identity assets (such as access to the NEC or a DIS sourced in-person identity verification service), the IDPs would need to know what value can be applied to those assets. DIS should consider how best to establish and convey the assurance that can be placed on these assets.

- **Extending GPG 45**: There may be additional identification capabilities (such as allowing vouching of identity) that are not covered by GPG 45. The simplest way to handle these would be for DIS to describe the capabilities in an addendum to GPG 45 or a DIS Operations Manual and work with tScheme to enable a “delta” certification that extends existing certifications to support DIS specific capabilities.

- **Attribute exchange**: Until attribute standards are better defined, defining a certification approach will be difficult. However, given the wide range of potential attributes it is possible that the current certification approach will not scale effectively to support all possible attribute needs. An alternative is to focus on the standardisation of metadata and providing a robust means to determine the source of an attribute (but not necessarily the process undertaken to establish the attribute). This appears to be the current direction of the nascent decentralised identity initiatives. A RP then would need to determine how much trust they place in the source. DIS should seek to play an active role in developments in this area.

[18] https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework

[19] This may require GDS to release the full IPV Operations Manual to those IDPs. Currently only a redacted version is available in the public domain: https://www.gov.uk/government/publications/govuk-verify-ipv-operations-manual-redacted

# 9 SUMMARY AND CONCLUSIONS

The OIX Alpha project undertaken by the SG with the support of several OIX members has covered much ground. The primary objective was to analyse in more detail the findings from the Discovery project undertaken by the SG in 2018 on the need for and possible approaches to digital identity.

The Alpha project has provided valuable insights that will help the SG as it moves to the next stages of the DIS programme. It is hoped that the findings will also be of benefit to the OIX community as it considers the future of the digital identity market in the UK and elsewhere.

The SG, through the DIS programme, wishes to develop a common approach to digital identity for access to public services in Scotland. The Alpha project has shown that this will entail taking:

- **A Flexible Approach**: Catering for the differing needs of individuals and the public services they wish to access will be complex and these needs vary considerably. A key recommendation of the report is that the SG creates a publicly owned identity provider (IDP) alongside private sector IDPs. This will ensure that the common approach includes sufficient choice to meet the range of needs of individuals wishing to access public services in Scotland. The recommendation includes ensuring that there are still sufficient incentives for private sector IDPs to participate.

- **A Standards Based Approach**: A flexible approach will require the adoption of appropriate standards - both technical standards and identity assurance standards. This, in conjunction with appropriate governance arrangements, is the best way to ensure that services are interoperable, future proofed and to avoid DIS building expensive proprietary solutions.

- **A Phased Approach**: The vision of DIS is to support a wide range of digital identity uses, enabling all kinds of public service. To achieve this vision, DIS will be dependent on the digital identity industry to develop standards-based services that support the full range of capabilities that DIS will need. Existing digital identity services are often focused on identification and authentication. DIS will need to work with providers to ensure that there is a route to the wider support of attributes, which will unlock many valuable use cases and support the concept of "tell us once".

# APPENDIX A PROOF OF CONCEPT

A key activity in the Alpha Project was prototyping a proof of concept (PoC) digital identity system. This appendix provides more detail on the proof of concept exercise, its achievements and findings.

**Scope**

The PoC was the DIS Programme's opportunity to explore the proposed approach and architecture for providing a digital identity solution that would meet the identified needs and constraints. It was important that we were able to understand the scale of the delivery challenges in real terms. We wanted to be able to say not only what would and would not work but also the degree of difficulty (effectively the time, cost and risk) of creating the required end-to-end system. For example a solution that required each Relying Party to undertake a significant amount of work just to be able to make use of the service would not be well received.

An important aspect of the PoC was to learn lessons from working with a range of organisations and roles that, as in production, would not be co-located. We entered PoC with a well-defined conceptual architecture and high-level roles for RPs, the integration layer and IDPs but without a detailed specification of the technical interfaces between those elements. The aim was to determine if the various PoC participants involved could implement a working system on the basis of a common standard (namely OIDC), in a collaborative manner. This approach enabled us to explore:

- what information needs to specified up-front;
- what misunderstandings can occur; and
- how best to structure collaborative development.

The organisations involved supported the PoC voluntarily, undertaking the work alongside their other commitments.

We set out to demonstrate the following scenarios in the PoC:

- **Scenario 1** - New customer wants to apply for a Social Security allowance online and is able to obtain the required level of assurance
- **Scenario 2** - New customer wants to apply for a Social Security allowance online but is not able to obtain the required level of assurance
- **Scenario 3** - Existing customer wants to apply for a Social Security allowance online and already has the required level of assurance with an IDP
- **Scenario 4** - Existing customer wants to apply for a Social Security allowance online and needs to uplift their current level of assurance with an IDP
- **Scenario 5** - Existing customer wants to request a service from their Local Authority and already has the required level of assurance with an IDP
- **Scenario 6** - Existing customer wants to request a service from their Local Authority and already has the required level of assurance with a different IDP
- **Scenario 7** - Existing customer wants to apply for a Social Security allowance (with vouching)

The focus of the scenarios was on the likely requirements of DIS in the first stage of the service (see section 3.2.1). The scenarios also tested DIS working with different types of IDP and different types of RP, as this is central to the flexible approach that DIS has in mind.

**Achievements**

The PoC work demonstrated that building an integrated digital identity service based on OIDC is relatively straightforward. Whilst we were not successful demonstrating all of the scenarios above, this was primarily down to scheduling challenges rather than technical issues.

The PoC was successful in achieving the following:

- Basic registration and login functionality for a single RP and a single IDP was achieved within c. 3 days of all the necessary individuals having been identified and made available across the parties. This was at the low end of our predicted timescale.
- Over time, following a phased approach and allowing for the availability of the necessary resources (given that contribution to the PoC was generally a background task for most participants) the PoC integration layer was:
    - successful in fully onboarding 2 RPs (as intended)
    - successful in fully onboarding 1 IDP (of the 2 intended)
    - partially successful in onboarding the second IDP.  Full onboarding was prevented by an identified and understood technical issue (at the time of writing it is hoped that the onboarding of the second IDP will be completed following the implementation of a change request to address that technical issue)

**Findings**

The high level findings for the DIS programme arising from PoC work include:

- the conceptual architecture appears technically sound with no serious issues having arisen within the specific scope and activities of the PoC.
- available open standards are supported by vendors and broadly suitable for DIS purposes
- the OIDC standard may not “as is” support all features of every use case - requiring some domain specific extensions.
- a phased (and Agile) approach to delivery is feasible and would be expected to reduce technical risk and time to market for prioritised functionality.
- RPs, integration layer providers and IDPs are readily capable of relatively quickly implementing a working system.
- RPs and IDPs do not need to have knowledge of each other’s detailed implementation - use of an integration layer and the use of open standards enables the necessary isolation (decoupling) of these roles logically and physically.
- Progress was affected by the need to coordinate multiple organisations who were supporting the PoC voluntarily. Whilst the challenges and risks of delivering a multi-stakeholder service must not be underestimated, we believe that these can be managed and mitigated.

The following table discusses more detailed findings:

**Exploring properties of technical standards**

For PoC we had a stated preference to use OIDC as the protocol for exchanges between RPs and the integration layer and between IDPs and the integration layer.  During PoC we wanted to explore whether this would be straightforward or, at the other end of the scale, it would be impractical, for example because of radically different interpretations of the way the standard is implemented in practice.  Whilst OIDC as a protocol is clearly well established and widely used particularly in consumer markets such as social media it is less well established in more stringently regulated markets such as government.

This objective was largely achieved during PoC.  It was established that different implementations do realise the standard in different ways. In most cases this caused initial challenges in establishing interoperation that were overcome through a positive collaborative and active process of looking at diagnostic data, investigating system behaviour and expectations and identifying corrective actions.  In most cases this process was accomplished within one elapsed day but with the actual active time across all parties being considerably less, generally estimated at 1 to 2 hours.

One particular issue (concerning the use HTTP GET versus HTTP POST commands) highlighted an incomplete implementation of the mandatory parts of the OIDC specification in the system used by one party. Whilst anecdotal, it does illustrate that DIS should expect to encounter such issues when working with multiple suppliers.

**Understanding capabilities of solutions and technologies**

In addition to being able to interoperate with other elements of the solution by use of a shared, standard protocol it is also important that each element of the solution is able to provide the necessary functionality within its own boundary to support its role in the end-to-end system.

This objective was partially met during PoC.  For the use cases that we were able to exercise all necessary functionality was available and sufficient to support the use case, and further no use case was unable to be exercised due to a lack of (or deficiency of) expected functionality in any element.

However there were use cases that we were not able to attempt due to other constraints. One example that we were unable to attempt is demonstrating that when multiple RPs and multiple IDPs are in play that identities can be isolated, e.g. a RP is unable to determine other RPs that use that identity and an IDP is unable to determine which RP is requesting an identity.

**Detailed findings regarding the use of OIDC**

The PoC afforded an opportunity for the programme to explore the features, usage and applicability of the OIDC standard leading to the following conclusions:

- Only the OIDC core specification appears to be mature enough to base an implementation on at present. Various extensions are being developed but are either no standardised or widely adopted, meaning bespoke work would be required to utilise them.
- OIDC implementations vary sufficiently between vendors such that we can’t assume 100% “plug and play” interoperability yet – though our experience from PoC is that they are reasonably close.
- OIDC vendor implementations are generally not as mature (stable) as SAML; during PoC some participants had to raise support calls which required code fixes to addresses even for fairly basic authorisation use cases.
- For the majority of public sector use cases, the OIDC core specification level of functionality will probably suffice (assuming best practice security procedures are followed when implementing it). The basic OIDC authorisation code flow was sufficient for the scenarios in the PoC.
- Different vendors have implemented custom mechanisms to increase the flexibility or ease of use of their solutions. The most common approach appears to be to define “custom scopes”. The approach seems to offer a good balance of remaining close to the core specification whilst providing additional flexibility.
- Custom mechanisms to convey levels of assurance typically do not provide the level of flexibility that DIS would ultimately wish to support (see section 6.2.6).
- Most providers have an ability to apply procedural logic to OIDC “Claims” before returning to the RP or to augment them with additional headers etc. It therefore it appears viable to present a common API to RPs, which can standardise (to a degree) the data retrieved from IdPs. This capability should likely be able to provide for future desired advanced functionality around step-up authentication and more granular Level of Authentication/Level of Assurance requirements (this was discussed with vendors during PoC - but not tested).
- For a production-scale implementation of the conceptual architecture, cryptographic agility will be vital. To enable this efficiently, it is important that vendors support OIDC Discovery 1.0, allowing OIDC clients to reach out and discover the current signing keys.
- Most suppliers support Bearer tokens as JWT (JSON Web Tokens) as a de facto standard
- The PoC participants agreed that cascading logout should not be supported (i.e. when one RP issues a logout (end session) request to the integration layer, that logout should not then end the session at the IDP or with any other RPs).
- Notwithstanding the above, instantaneous token revocation may be desired in some edge-case circumstances (such as fraud on high-value transactions). Having said that, support for instantaneous token revocation appears to be limited in some

vendor implementations. Therefore setting a short-but-sensible token expiry seemed to be the best compromise between security and convenience.

- Support for the “prompt” parameter is a desired capability, especially in an accessibility scenario, where a user may need additional time to complete a form. Vendor support for this appears limited at present.
- For the conceptual architecture to maintain a privacy barrier, it should ensure identifiers used by IDPs and RPs are different. For the purposes of the PoC, we simply relayed the IdP identifier “as-is” to the RP. To meet the programme’s privacy goals a production solution would need to transform these identifiers in a secure and consistent manner.

**Other Outcomes**

Throughout the PoC many valuable lessons were learned in areas such as:

- approaches to management, scheduling and prioritisation across collaborating organisations.
- communication methods to support asynchronous and remote working.
- configuration and development diagnostic and debugging approaches and techniques.

These will be taken forward by the DIS as it moves into the next stage of the programme.

# APPENDIX B GLOSSARY

The following table provides working definitions of terms. In the future these will be aligned with an appropriate standard.

| Term | Meaning |
|---|---|
| Alpha Delivery Partner | means an organisation providing services to the DIS Programme in relation to the Alpha Phase. |
| Alpha Development System | means the technical infrastructure (physical and or virtual) implemented and assessed during the Alpha Phase - expected to be a subset of the full DIS Solution. |
| Alpha Phase | means a programme or project stage undertaken to demonstrate some of the key concepts of one or more potential solutions where concepts can be substantiated or rejected quickly and at low cost. |
| AML | abbreviates Anti-Money Laundering. |
| Attribute | means a quality or characteristic ascribed to an individual. |
| Attribute Exchange | means a system for individual-controlled sharing of attributes between organisations. |
| Authentication | means confirming the identity of the individual in the context of a transaction. |
| Authorisation | means the process of the individual allowing (or “authorising”) attributes to be processed or used by a relying party. |
| Digital Identity | means the digital representation of an individual. |
| Digital Identity Scotland | means the Scottish Government programme to develop a common approach to digital identity for digital public services in Scotland |
| DIS | abbreviates Digital Identity Scotland. |
| DIS Ecosystem | means the complete logical system implemented to deliver the objectives of the DIS Programme including people, processes and technology across all participants. |
| GPG 44 | means Good Practice Guide 44 available at:<br>https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services |
| GPG 45 | means Good Practice Guide 45 available at:<br>https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual |
| Identification | means verifying the identity of an individual, typically during onboarding, or of an attribute pertaining to that individual. |
| Identifier | means a persistent reference to the individual. |

| | |
|---|---|
| | Note that DIS intends for identifiers to be specific to RPs or IDPs, to avoid the privacy concerns associated with all parties referring to the individual by the same identifier. |
| Identity | means a set of information sufficient to distinguish a real, identifiable and unique individual. |
| Identity Provider or IDP | means an organisation that provides services to an individual to manage their Digital Identity. |
| In-Person Identification | means performing identity checks in-person. This may be necessary for individuals who are unable to complete an identification process digitally, e.g. because the individual concerned does not have an existing digital footprint (e.g. financial history) or to support cases where the individual needs assistance in completing the process. |
| Individual | means a person accessing Scottish Public Services on behalf of themself of another person.<br>This is in contrast to an Officer (see below) where an individual is acting on behalf of an organisation. |
| Integration Solution | means middleware used by the DIS Solution to enable many-to-many inter-operation between IDPs and RPs and potentially providing additional functionality at the core of the DIS Solution. |
| Integration Solution Provider | means an organisation providing an Integration Solution. |
| KYC | abbreviates Know Your Customer. |
| Level of Assurance or LoA | means a measure of the quality and robustness of technologies, processes and checks employed for identification, authentication or attribute assurance. |
| linkability | means the ability for organisations to determine (independently of the individual) that two records or accounts correspond to the same individual. |
| Middleware | means a layer of software intended to enable other (heterogeneous) software or systems to interoperate. |
| Officer | means an individual acting on behalf of an organisation |
| OIDC | OpenID Connect |
| Personal Data | means personally identifiable data, as defined in the General Data Protection Regulation (GDPR). |
| Personal Data Store | means a protected repository and data exchange system for attributes and other personal data that is controlled by the individual to whom that personal data relates. |
| PoC | Proof of Concept |

| | |
|---|---|
| Product Backlog | means the set of things deliverables that are not yet delivered by an project following an Agile approach<br>(see: https://www.scrum-institute.org). |
| Programme Alpha Lead | means a member of the DIS Programme team who will provide strategy, direction and leadership for the alpha phase including, but not limited to, liaising with the alpha delivery partner. |
| Relying Party or RP | means an organisation relying on an IDP to determine the identity or attributes of an individual. |
| unlinkability | means a feature of privacy enhancing technologies and systems that prevent unauthorised linkability. |
| User Experience or UX | means an individual's response to using (or anticipating using) a product or service (see: https://en.wikipedia.org/). |

# APPENDIX C ACKNOWLEDGEMENTS

The Scottish Government is grateful to support received from many individuals and organisations throughout the Alpha Project, including:

- Avoco Secure
- Argyll and Bute Council
- Department of Work and Pensions
- Digidentity
- Dundee City Council
- Experian
- Factern
- Government Digital Service
- Idemia
- Improvement Service
- Kantara Initiative
- Meeco
- Mydex
- Mvine
- Nature Scotland
- NHS24
- North Lanarkshire Council
- MyDiabetesMyWay
- New Zealand Government
- Post Office
- Scottish Social Security
- Sitekit
- TISA
- tScheme
- Verisec
- Yoti

We are also grateful to the DIS Expert Group[20] for their insight and guidance.

[20] https://www.gov.scot/groups/online-identity-assurance-expert-group/