Scottish Government

Online Identity Assurance Programme

Technical Discovery

Solution Characteristics

Status:	Baselined
Version:	1.03
Date:	01-Jun-18

Contents

Contents 2
1. Executive Summary 3
2. Introduction 3
3. Considerations 3
3.1. Solution Choice 4
3.2. Segregation Choice 5
3.3. Data Choice 6
3.4. Sources Choice 7
3.5. Attribute Storage Location Choice 8
4. Existing Digital Identity Services 9
4.1. Introduction 9
4.2. Assessment 10
4.3. Summary 13
5. Existing Pools of Digital Identities 14
5.1. Introduction 14
5.2. Identity Accounts 14
5.3. Identity Sources 18
5.4. Summary 19
6. Conceptual Architecture and Integration Solutions 20
6.1. Introduction 20
6.2. Conceptual Architecture 20
6.3. Scenarios 22
6.4. Integration Solutions 23
6.5. Standards 24
6.6. Recommendation 25
Appendix 1 – Version Control 26

1. Executive Summary

The Scottish Government is seeking to provide a common approach to digital identity for both the people of Scotland and the providers of digital public services to those people. ASE Consulting and Consult Hyperion were engaged to undertake a discovery exercise of the potential technical options.

Through our conversations with various stakeholders the following has become clear:

- The needs of individuals vary including accessibility, privacy and user experience needs.
- The requirements of services vary including assurance level requirements as well as information needed to deliver services.
- No single solution or collection of solutions exist in the market today that can immediately address all of these needs and requirements
- There are solutions that already exist, and which some people will be familiar with, that address some of these needs. These would appear to be a good place to start building a common approach.

This document assesses the key characteristics that should be sought from a digital identity solution or solutions for Scotland. Candidate solutions that exist in the market today are examined and an approach suggested that seeks to promote choice to end users, flexibility to service providers and standardisation for providers of identity related services.

The Scottish Government has a real desire and commitment to engage widely with all stakeholders, both end users and service providers, and to develop an approach that respects the privacy of individuals and is inclusive to all members of the population.

2. Introduction

This deliverable maps the expectations and requirements for Online Identity Assurance across the public sector in Scotland against approaches and solutions that are available in the market place and/or used elsewhere. This deliverable also considers how such solutions could, from a technical perspective, be integrated into Scottish public services.

This will contribute to and support preparations for the Alpha Project by helping to distil down the myriad of potential approaches (and combinations of approaches) to a manageable number that can be prioritised by relevance and (expected) suitability.

3. Considerations

As a first step we consider, from the End-User's perspective, the key factors that will influence the choice of solutions in the market. The intention here is to identify some key characteristics that are required of the identity solution. The analysis is done from the perspective of the End-User (the individual wishing to access Scottish public services) as in our discussions with Scottish public sector stakeholders, the importance of placing the user at the centre of digital identity has been very clear.

We consider the following points:

- Solution Choice: Should the user be able to choose between multiple solutions?

- Segregation Choice: Should the user be able to segregate different aspects of their digital life?

- Data Choice: How much control should the user have over the sharing and use of their personal data?

- Sources Choice: How much choice should be given to users about where identity attributes are sourced from?

- Attribute Storage Location Choice: How much control and choice should users have over where their Attribute data is stored?

3.1. Solution Choice

Should End-Users have a choice of solutions and if so could these offer varying functionality?

3.1.1. Why is this significant?

In our discussions with various stakeholders, there appear to be competing requirements that cannot be satisfied through a single solution. These competing requirements include, for example:

- Differing needs of the wide demographic and geographic coverage of individuals: Whilst many people will undoubtedly be ready to embrace digital services, for others there will be barriers. Some people will not have access to the technology, documents and records needed to establish a Digital Identity. A one-size fits all solution is therefore unlikely to work.

- Differing attitudes to privacy (and willingness to trade privacy off against convenience): Some people are particularly concerned about the creation of monolithic identity systems or databases for government that could threaten privacy, civil liberties and personal safety, either now or in the future. This includes the risks arising from honeypots of data. Providing choice can be a transparent way of demonstrating a privacy respecting approach.

- Differing requirements of Relying Parties: The goal is to provide a common approach to Digital Identity across a wide range of services. These will have differing requirements both in terms of the identity data (Attributes) needed and the level of assurance of that data.

Furthermore, not all solutions are equal:

- Some solutions only address part of the problem (Identification or Authentication but not both)

- Some solutions are design for specific channels (mobile only or designed for web, so not optimal UX in mobile)

3.1.2. Basis of Recommendation

The pros and cons for providing solution choice are set out in the following table.

Pros	Cons
Provide solutions that address different user needs	More complex for users to understand
Approach likely to have better privacy properties	Increased solution cost
Encourage suppliers to be competitive	Increased complexity (of solution)

3.1.3. Recommendations

1. For initial stages (including initial "production" use) limit the choice given to users, to simplify the roll out and provide the opportunity to refine the approach. We assume that it will be necessary to continue to support non-digital access to services – these will need to be maintained at a sufficient level until greater choice of Digital Identity solutions is available.
2. Providing multiple solutions for other reasons (e.g. to increase market penetration by providing solutions tailored to user profiles) should not be ruled out.
3. Architect the system such that it can (relatively) easily accommodate provision of additional Digital Identity services in the future.

3.2. Segregation Choice

Should End-Users be able to segregate Digital Identity usage between Relying Parties such as tax, benefits, health and local authorities?

3.2.1. Why is this significant?

The focus of this question is concerned with how far it is appropriate to link services together. In an ideal privacy-respecting solution measures are taken to prevent linkability where this would not be appropriate – even though systems may not be being built to link and share data today. The point is to create a system that protects individuals against the inadvertent or malicious linking of such data in the future. This is in many respects a cultural issue. Germany, Austria and New Zealand, for example, have created Digital Identity solutions that provide strong protections against unintended linking[1]. In Estonia, on the other hand this does not appear to have been a requirement.[2]

Whilst unlinkability can be achieved in various ways, technically, that may not be enough for the End-User (or other stakeholders). The End-User may not have visibility of, and therefore feel able to trust, a purely technical approach. It may therefore be necessary to provide functionality that allows the user to explicitly segregate (or "unlink") various parts of their digital experience. Alternatively, if the user has access to multiple solutions and can choose which to use in each context, that may provide an alternative non-technical solution to segregation, for those users that require it.

3.2.2. Basis of Recommendation

The pros and cons for Digital Identity segregation choice are set out in the following table.

Pros	Cons

[1] Typically achieved by giving the user unlinkable sector specific identifiers
[2] https://www.enisa.europa.eu/publications/eid-cards-en

Stronger privacy	Potentially additional burden on the End-User, depending how implemented.
Lower risk to Relying Parties	May make some legitimate data sharing use cases more complex.

3.2.3. Recommendations

1. Solution should provide a level of technical unlinkability.
2. Provide choice, as per recommendations in section 3.1.3.
3. The architecture should include an abstraction layer or hub that provides a decoupling between all parties: Relying Parties, Identity Providers, other data sources.
4. Make service open to independent scrutiny.
5. Invest in End-User education to build confidence in the approach

3.3. Data Choice

Should End-Users be able to determine and control what Personal Data they share with Relying Parties such as tax, benefits, health and local authorities?

3.3.1. Why is this significant?

The focus of this question is broad, considering the wider range of Attributes that may be needed to deliver services. These additional Attributes (such as residency, entitlement to drive, qualifications and so on) are often only available in the form of paper documents adding friction, inefficiency and risk to both service providers and the End-Users seeking to access those services.

Where Attributes are shared digitally today, it is usually in the background with individuals having limited understanding or visibility of how their information is being shared or used (or even breached). GDPR requires organisations to be much clearer about how information is being used and will drive the implementation of much stronger controls around personal data. It will not, however, result in a fundamental change to the way Attributes are shared.

Digital Identity and Attribute Exchange systems, on the other hand, promise new ways for organisations to share data, placing the individual at the centre and using technology to automate processes that are currently manual.

The promise of Attribute Exchange is yet to be realised, although high profile initiatives such as Verified.me in Canada and the work of the SOVRIN foundation are actively pursuing this area.

3.3.2. Basis of Recommendation

The pros and cons for Personal Data sharing choice are set out in the following table.

Pros	Cons
Empowers individuals	May place more responsibility on the End-User, to manage what is shared when
Discourages exploitation of personal data	Trade-off between data shared and service

	provided may not be clear
Control engenders trust	Requires greater service sophistication, to be able to provide some services where less personal data is shared

3.3.3. Recommendations

1. Adopt an architecture that is Attribute based, to ensure future flexibility
2. Do not replicate Attribute data unnecessarily
3. Where possible[3], provide the End-User with a personal data store (or equivalent) as the means to manage and control aspects of their identity.

3.4. Sources Choice

Should End-Users be able to acquire and assemble Attributes assured by multiple sources (such as Identity Providers, Relying Parties or third parties)?

3.4.1. Why is this significant?

If the Attribute Exchange paradigm were to develop, over time the End-User would find that there are multiple potential sources of the Attributes being requested by a particular Relying Party. At one level this could increase the likelihood of the user being able to assemble the Attributes necessary to access the service in question. It could enable Attributes to be delivered from the source real-time, meaning that changes to Attributes or the status of Attributes will be available to Relying Parties immediately. It may also allow users to demonstrate eligibility to access a service from non-traditional sources, making services more inclusive.

3.4.2. Basis of Recommendation

The pros and cons for supporting multiple sources for Attributes are set out in the following table.

Pros	Cons
Potential to source Attributes from a wide range of sources including non-traditional sources	Potentially complex for the user to understand and manage, especially as the permutations of Attributes that may be acceptable could vary between contexts and become complex to define.
Attributes more current – coming real time from source	Would need to develop standards for fully flexible Attribute Exchange to work.

3.4.3. Recommendations

1. Protect the user from this complexity as far as possible
2. Include in architecture the capability to interrogate whether user has the required Attribute and then request it – to avoid needing the user to make complex decisions.

[3] Insisting on personal data stores will significantly limit the number of providers who can be part of the service. It should however be a desired feature and used as a key differentiator when selecting providers.

3. Consider developing or aligning with standards over time to ensure Attributes are established to meet required levels of assurance

3.5. Attribute Storage Location Choice

Should End-Users be able to choose where Attributes are stored, e.g. by a third party IDP, in a Scottish Government service, at the Relying Party?

3.5.1. Why is this significant?

There are several places one could envisage providing Attribute storage:

- Part of an IDPs service
- Provided centrally by the Scottish Government, perhaps in the form of a personal data store
- Distributed across one or more RPs, if an Attribute Exchange model was adopted

The leading proponents of self-sovereign identity (e.g. the SOVRIN foundation) deliberately leave Attribute storage to the user. This, they argue, is part of the user having true sovereignty over their personal data. In reality, the majority of users will have insufficient expertise to make such decisions and will end up relying on the services of an organisation who they may or may not trust.

3.5.2. Basis of Recommendation

The pros and cons for supporting End-User control over personal data Attributes are set out in the following table.

Pros	Cons
Potentially more privacy, through greater choice.	Places significant responsibility on End-User
Potentially more privacy, through greater transparency.	User will not understand the implications of storing data in different places

3.5.3. Recommendations

1. Make use of Personal Data Stores (PDSs) an optional (but desirable) requirement on IDPs.
2. Consider how to differentiate PDS-based IDP offerings from non-PDS based offerings, e.g. only support PDS-based solutions for broader Attribute Exchange.

4. Existing Digital Identity Services

4.1. Introduction

The market for assured and reusable (or federated) digital identities for citizens and consumers in the UK is immature but evolving. This section assesses at a high level the existing consumer-facing digital identity services in this market that could support the characteristics identified above.

The services assessed are:

- GOV.UK Verify, the scheme as a whole
- GOV.UK Verify Identity Providers, individually separate from the Verify scheme
- Fintech start-ups, with Digital Identity or Know Your Customer (KYC) propositions
- myaccount, the service operated by the Improvement Service providing a Digital Identity service for Scottish Local Authorities

The National Entitlement Card (NEC) is not assessed, as it is not a Digital Identity per se. It does however bring a potentially useful pool of users that could be brought into an identity system (see section 5.3.1).

We have not assessed the potential identity capabilities of banks or mobile operators, as today (for the most part) they do not offer assured digital identity services that the Scottish Government could use. Where bank or operator-led identity schemes have succeeded (e.g. in the Nordics) these have often been driven by the market. In the UK, the open banking initiative is a potential catalyst for federated identity in banking, this however is yet to happen. For mobile operators, GSMA mobile connect is the focus of their identity efforts but in the UK this appears currently to be limited to back-end data (including providing data to the GOV.UK Verify identity providers).

For each service, the following is assessed:

- Level of Identification, does it include strong identity verification to recognised level?
- Level of Authentication, does it include strong authentication, e.g. multi-factor?
- Independently certified, has the service been independently certified, ideally from a Digital Identity perspective?
- Supports unlinkable identifiers, as per the recommendations in section 3.
- Supports flexible Attribute Exchange, as per the recommendations in section 3.
- Includes Personal Data Store, as per the recommendations in section 3.

4.2. Assessment

4.2.1. GOV.UK Verify "as is"

GOV.UK Verify is an established identity scheme that Scottish public services could potentially be integrated with. The following table assesses characteristics of the "as is" scheme, assuming that Scottish services would connect into it via the existing GDS hub.

Characteristic	Assessment	Score
Level of Identification	GOV.UK Verify IDPs required to support LoA 2 Identification as defined in GPG 45, although some users (believed to be a small number currently) will only have been verified to LoA 1	H
Level of Authentication	GOV.UK Verify requires LoA 2 Authentication as defined in GPG 44, for all IDPs, even for LoA 1.	H
Independently certified	All IDPs are assessed and certified by tScheme[4].	H
Supports unlinkable identifiers	The hub creates an "air-gap" between the IDPs and RPs. RPs created internal identifiers that are unlinkable however the Matching Data Set acts as a single identifier across the scheme.	M
Supports flexible Attribute Exchange	Hub architecture technically could support inclusion of Attribute providers, however this has not been done to date and the privacy implications of a much wider set of Attribute data flowing over the hub is not clear.	L
Includes Personal Data Store	Currently it is not believed any of the IDPs include a Personal Data Store component, although some are open to the concept.[5]	L

4.2.2. GOV.UK Verify Identity Providers operating outside of the Verify scheme

The GOV.UK Verify Identity Providers can potentially offer their services independently of the GOV.UK Verify scheme. This may require them to drop the Verify brand for those services. The following table assesses characteristics of the IDPs operating independently.

Characteristic	Assessment	Score
Level of Identification	It is unclear whether the GOV.UK Verify IDPs will be able to access the Document Checking Service[6] when operating outside of GOV.UK Verify. This may reduce the level of identification they can achieve, although as per the Fintech providers below they should still	M

[4] http://www.tscheme.org/
[5] Based on various Consult Hyperion discussions.
[6] Government service provided for checking status of passports and driving licenses.

	be able to satisfy the requirements of the financial services sector.	
Level of Authentication	GOV.UK Verify requires LoA 2 Authentication as defined in GPG 44, for all IDPs, even for LoA 1.	H
Independently certified	All IDPs are assessed and certified by tScheme, although strictly speaking tScheme certification may not apply to non-Verify usage.	M
Supports unlinkable identifiers	Integrating with the IDPs directly (without a hub) would lose the "air-gap" and element of unlinkability that it provides.	L
Supports flexible Attribute Exchange	Potentially some IDPs may be able to support broader Attribute Exchange but this is likely to vary considerably between them.	L
Includes Personal Data Store	Currently it is not believed any of the IDPs include a Personal Data Store component, although some are open to the concept.[7]	L

4.2.3. Fintech Start-ups

There are a number of Fintech start-ups offering Digital Identity or digital AML/KYC (Anti-Money Laundering/Know Your Customer) offerings. Several of them employ mobile technology to read passports or driving licenses and perform facial biometric checks of the user against these documents. The business models vary – some are B2C[8] and some are B2B[9]. The B2C propositions provide individuals with reusable digital identities. The B2B propositions typically facilitate the onboarding of the individual to a service (e.g. financial service, cryptocurrency exchange, gambling site) but do not provide the individual with a reusable Digital Identity per se.

Characteristic	Assessment	Score
Level of Identification	Typically, not formally measured but usually designed to meet AML/KYC needs.	M
Level of Authentication	For B2C propositions, can result in strong mobile Authentication although not formally measured.	M
Independently certified	May have generic certification such as ISO 27000 but unlikely to have specific identity assurance certification.	M
Supports unlinkable identifiers	For B2C propositions, can include relationship specific identifiers.	M
Supports flexible Attribute Exchange	For B2C propositions, can include support for (or have on the roadmap) broader Attribute	M

[7] Based on various Consult Hyperion discussions.
[8] Business-to-consumer
[9] Business-to-business

	Exchange.	
Includes Personal Data Store	For B2C propositions, can include cryptographically secured personal data stores	M

4.2.4. myaccount

myaccount is a Digital Identity service provided by the Improvement Service for local authorities in Scotland.

Characteristic	Assessment	Score
Level of Identification	Not believed to be formally measured. The levels of assurance defined by the Improvement Service[10] suggest the number and type of sources together with the verification of the person is at a level significantly lower that LoA 2 as defined in GPG 45.	M
Level of Authentication	Not believed to be formally measured. Currently appears to be single factor, phone number is collected during registration "to provide enhanced account security in future" [11]	L
Independently certified	Service is "regularly reviewed and audited" but appears not to have specific identity assurance certification.	M
Supports unlinkable identifiers	Supports a mix of linkable (e.g. UCRN[12]) and unlinkable (e.g. SVT[13]) identifiers.	M
Supports flexible Attribute Exchange	Currently limited to core identity Attributes (name, date of birth, gender, postal address, email address and UCRN)	L
Includes Personal Data Store	Does not appear to include Personal Data Store as part of existing design.	L

[10] http://www.improvementservice.org.uk/documents/myaccount/myaccount-information-architecture.pdf

[11] FAQs in https://signin.mygovscot.org/home/

[12] Unique Citizen Reference Number

[13] Secure Visitor Token

4.3. Summary

Characteristic	GOV.UK Verify	GOV.UK Verify IDPs	Fintech	myaccount
Level of Identification	H	M	M	M
Level of Authentication	H	H	M	L
Independently certified	H	M	M	M
Supports unlinkable identifiers	M	L	M	M
Supports flexible Attribute Exchange	L	L	M	L
Includes Personal Data Store	L	L	M	L

From a technical perspective, the GOV.UK Verify appears well placed to provide assured digital identity services. However, as discussed in section 5.3 there are potential issues with its current reach.

There are other players in the market that could provide plausible alternatives. These include the GOV.UK Verify IDPs operating independently of Verify and the Fintech players. In section 6, we propose an approach that will allow the Scottish Government to have some flexibility, supporting alternative identity services as they start to scale and become relevant.

At face value, myaccount does not appear to be as strong technically as the other services assessed. This is because it was built to solve a different problem (providing simple access to local authority and NHS services) and the focus has been on inclusion – getting customers on board at "LoA 0" and then building assurance in them over time. We understand that the Improvement Service is exploring a number of potential enhancements to the service in all of the areas assessed above.

5. Existing Pools of Digital Identities

5.1. Introduction

This section assesses current pools of assured Digital Identities available to the Scottish market for the following reasons:

- They may provide "quick wins" that could be exploited by the programme to get some initial volumes.
- Where these existing pools are expected to grow, the programme may be able to benefit from as well as be a stimulus for this growth.
- For individuals that already have assured Digital Identities, allowing them to use those identities to access Scottish services may provide a simple and straightforward experience, compared to requiring those individuals to establish a different Digital Identity for Scotland.

5.2. Identity Accounts

5.2.1. GOV.UK Verify

GOV.UK Verify is the UK government's flagship Digital Identity programme. Despite the various challenges and hurdles the programme has encountered, the recent reports[14] suggest that role of GDS in digital transformation (which includes GOV.UK Verify) will continue.

Currently there are c.2 million accounts in the GOV.UK Verify scheme (with on average each account having been used twice) and it is supported on 17 services, with HMRC being the biggest Relying Party[15]. There is usually a spike in activity at the end of January each year, which is linked to the deadline for submission of Self Assessment tax returns.

Our research suggests that up to 220K[16] people in Scotland will have GOV.UK Verify accounts and that the majority of these will be of working age, have a good financial footprint and be digitally savvy. This will change over time as the number and type of services grow.

DWP has the potential to drive volumes Digital Identity across a much broader demographic. The roll out of Universal Credit over the next few years should drive this growth.

NHS Digital also has the potential to support the longevity of GOV.UK Verify, although this would not result in a growth in usage of the service in Scotland per se. Specifically, NHS Digital is in the process of developing its own Digital Identity standard as well as trialling various solutions[17]. We would expect this standard to lean heavily on the GPGs, although given the sensitive nature of health data and the importance of ensuring the identity of the patient is correct, it seems likely that NHS Digital will require a

[14] http://central-government.governmentcomputing.com/news/whitehall-sources-reiterate-key-gds-role-in-digital-government-6104239
[15] https://www.gov.uk/performance/govuk-verify
[16] Our research suggests 11% of current Verify accounts have Scottish addresses, which is higher than the percentage of the UK population in Scotland (8%). As individuals are allowed to have accounts with multiple IDPs, the number of people in Scotland using Verify may be less.
[17] https://digital.nhs.uk/about-nhs-digital/our-work/transforming-health-and-care-through-technology/self-care-and-prevention-domain-a/citizen-identity

level of assurance exceeding LoA 2 in some areas. For health, Identification usually includes a physical check of the person. Some of the GOV.UK Verify IDPs have already integrated such capabilities. It therefore seems possible that Verify (or the individual Verify IDPs) may achieve additional volume in England via NHS Digital. No specific timeframes for this have been published however the initiative is linked to the "Personalised Health and Care 2020" framework.

Summary: The number of people in Scotland using GOV.UK Verify today is relatively small but growing. The speed of that growth will be dependent on how quickly GOV.UK Verify itself grows including how well it is able to reach people who are not served by the conventional financial sources.

5.2.2. GOV.UK Verify Identity Providers

GOV.UK Verify Identity Providers are currently contractually prevented from enabling the re-use of digital identities created under the GOV.UK Verify brand. This is expected to change in the near future, in order to provide additional scale from the private sector and to provide additional ways for Identity Providers to recoup their investment.

Aside from the growth in GOV.UK Verify itself, which is considered above, those Identity Providers with consumer brands, that provide non-identity services to consumers, may be able to bring those consumers into their identity service with relative ease (compared to acquiring customers from scratch).

In our view, three of the current GOV.UK Verify Identity Providers have consumer brands and consumer services of sufficient scale to be of interest: Barclays, Experian and the Post Office. These are considered below. All the information used in this analysis has been obtained from public sources.

Barclays

Barclays clearly has retail banking relationships with millions of consumers. A UK government report on the retail banking industry[18] states:

- "In relation to Scotland, while there were some differences in market share in Scotland compared with England and Wales, these were not sufficient to suggest that Scotland should be viewed as a separate geographic market to England and Wales."
- "In Scotland, most Personal Current Accounts were supplied in 2015 by Royal Bank of Scotland Group (through the RBS brand), Lloyds Banking Group (through the Bank of Scotland and Halifax brands), TSB, Clydesdale and Santander"

The number of people in Scotland with Barclays accounts is not completely clear, however their presence in Scotland would appear to be less than that the rest of the UK.

[18] https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

Experian

Experian offers consumer services related to credit scoring including free credit score reports and the paid for Credit Expert product. Using figures from a recent annual report[19] we estimate that Experian has c. 1.4m Credit Expert customers in the UK.

Anecdotal evidence[20] suggests that Experian is used by the financial services industry in Scotland alongside other credit bureaux. This would suggest Experian has c. 110K Credit Expert customers in Scotland. These will of course also be people who are financially active.

The number of customers using the free services could not be found from public sources, so the number of consumer relationships, where the consumer has an account with Experian (albeit a free one), may be significantly higher.

Post Office:

The Post Office provides a wide range of retail services including:

- Retail banking and insurance (operated by the Bank of Ireland) with c. 3m customers[21] in the UK.
- Foreign exchange with c. 9m customers in the UK, although it is unclear if this is the number of individual identifiable customers or the annual volume of transactions. The Post Office will be required to perform AML/KYC steps for some of these.
- The passport "Check and Send" service, which is used by 48% of consumers[22]. We estimate this equates to 2.5m transactions per year across the UK.[23]
- Through their banking framework the Post Office supports 110m in-person transactions per year on behalf of other banks, again across the UK.[24]

In many cases, however, these are not ongoing customer relationships resulting in the establishment of an account or customer relationship per se.

Summary: The relevance of individual GOV.UK Verify IDPs to Scotland varies as would their ability to bring scale outside of GOV.UK Verify. The Post Office stands out as having a large number of touchpoints with individuals which may provide a means to establish digital identities.

[19] https://www.experianplc.com/media/2733/experian-ar2016.pdf
[20] https://www.bankofscotland.co.uk/assets/pdf/HelpCentre/pdf/credit-scoring-guide.pdf
[21] https://postandparcel.info/63849/news/post-office-ltd-rebrands-financial-services-in-bid-for-market-share/
[22] https://www.citizensadvice.org.uk/Global/CitizensAdvice/Post%20and%20Telecoms/The%20state%20of%20the%20post%20office%20network.pdf
[23] Assuming 80% of population have a passport and passports are renewed every 10 years.
[24] https://www.ft.com/content/18035596-e175-11e6-8405-9e5580d6e5fb

5.2.3. Fintech

There are several AML/KYC providers who provide the various combinations of mobile document capture, selfie checks and background checks. Many of these such as Onfido, Mitek, Au10tix and Jumio provide B2B offerings. Two that have a B2C proposition are:

- Yoti, which is focused on providing the End-User with a general purpose mobile-based Digital Identity for use in a wide range of online and offline use case.
- Hooyu, which provides mobile-based identity verification services for peer-to-peer transactions. This does not, however, result in the End-User having a reusable Digital Identity.

At the official launch of Yoti, in November 2017 it was reported[25] that 140,000 people had downloaded the app with about 95,000 of those being UK users. According to the report Yoti is hoping to have 1 million customers "by summer 2018, expanding into India, the US and Europe". Up to date figures were not available for this report, although since the launch there has been a steady stream of press releases suggesting Yoti is aggressively seeking to ramp up.

Summary: Fintech providers, such as Yoti, may provide an interesting alternative to GOV.UK Verify IDPs for some customers if they reach scale quickly.

5.2.4. myaccount

myaccount is a Digital Identity service developed for Local Authorities and the NHS in Scotland. It is integrated with both the NHS Central Register (NHSCR)[26] and the National Entitlement Card[27].

According to mygovscot[28], myaccount is currently supported by 15 local authorities (of the 32 in Scotland). For 12 of these, myaccount is used for general services. Six authorities use myaccount for school payments and 1 for WiFi access.

There are currently approximately 470K myaccount users[29]. The information from mygovscot indicates that all current usage is at level of assurance 0 (as defined by the Improvement Service in their “Scottish Levels of Assurance”.[30]), although we understand that this is done to make the service inclusive. Anyone can open an account and then over time, as the account is used, the level of assurance in the identity can grow.

[25] https://www.zdnet.com/article/yoti-aims-to-provide-everyone-with-a-biometric-digital-identity-that-works-via-a-smartphone-app/
[26] https://www.nrscotland.gov.uk/files//nhscr/governance-board/2016/paper3-nhscr-gb-16-03-mygovscot-myaccount-update.pdf
[27] http://www.improvementservice.org.uk/myaccount.html
[28] https://signin.mygovscot.org/myaccountfaqs/CAS
[29] Number provided by the Improvement Service
[30] Page 31 in http://www.improvementservice.org.uk/documents/myaccount/myaccount-information-architecture.pdf

Summary: myaccount has a large potential number of users. However existing users of this service are currently at LoA 0 (for both identification and authentication), meaning these accounts will be of limited immediate value for services requiring assured Digital Identities. RPs can of course undertake their own identification of the myaccount holder directly (e.g. by requiring them to visit the RP or by performing knowledge-based verification) as is done by two Councils currently. Improving the user authentication would also create a basis on which assured identities could be built using conventional sources or leveraging the checks performed by RPs.

5.3. Identity Sources

Many of the digital identity services highlighted build digital identities from the same types of sources. These include credit bureau data and official documents such as passports. These address the portion of the population that is financially active (using credit cards, post-paid mobile contracts, mortgages and loans) and that travels. There is a significant section of the population that these sources do not address well, including young people, financially excluded and the elderly.

The SG should therefore seek to incorporate into its Digital Identity approach alternative sources that can address these gaps, such as:

5.3.1. National Entitlement Card (NEC)

The National Entitlement Card (NEC) is a multi-purpose card that provides concessionary travel (via an ITSO application on the card which is owned by Transport Scotland) as well as access to various local authority services (via information printed on the card and stored in the chip).

NEC cannot be considered as a Digital Identity per se, as it is unlikely to be practical to integrate it directly with digital services, due to the need for card readers for access from a PC, limitations with Apple devices[31] and because the cards do not include cardholder authentication, such as a PIN. However, to get a NEC the person has to undergo a level of identity checking, to confirm entitlement to receive the card. This is performed by the local authority and often involves face-to-face checks. This verified identity data has the potential to be the foundation of an assured digital identity.

There are around 2.1m people with a NEC[32] including young people (the Young Scot card) and others entitled to concessionary travel.

5.3.2. Local Authority Data

The recent OIX discovery project assessing "microsources of data"[33] and the subsequent ongoing alpha project[34] ask whether the user can present data from organisations such as local authorities as part of the

[31] The NFC interface on Apple devices is tightly controlled by Apple, preventing performing a transaction with the ITSO application on the NEC.
[32] http://www.improvementservice.org.uk/national-entitlement-card.html

process of establishing an assured verified digital identity. The particular example of housing is explored, as local authorities will have verified the identity of people claiming housing benefit or living in social housing. This identity source is potentially valuable in filling the gaps in the conventional sources based on financial activity.

5.3.3. Schools Data

Schools potentially provide a way to corroborate the identity of a young person. To get a place in school in the first place some checks will be done to confirm the identity and address of the pupil. More importantly the school (and by implication the Scottish schools management systems) will often know the young person over a period of years.

5.3.4. In Person Contact

Scottish public services will have in person contact with end users at various points, for example in the delivery of health care. For some end users this may be an appropriate place to perform identity verification steps. This does not necessarily imply that health care professionals need to become experts in identity proofing. For example, if a health visitor was able to use their work mobile device to scan a code produced from an identity app running on the patient's mobile device, this would provide a means to form connection between the known customer and their digital identity without any special training or expertise required.

5.4. Summary

Today there is no single pool of digital identities that the Scottish Government can leverage to address a significant proportion of the Scottish population. However, it is an evolving situation. Some of the existing pools are expected to grow. Scottish public services will help to drive growth bringing new customers into those identity services.

The Scottish Government should seek to measure the reliability of alternative data sources and integrate them into the approach, to provide routes for as many people as possible to obtain assured digital identities.

The Scottish Government should take an approach that provides flexibility to support different Identity Providers, as the landscape evolves. Which Identity Providers and Data Sources it makes sense to start with will depend on the services that are to be supported first.

[33] http://oixuk.org/micro-sources-of-data/

[34] http://oixuk.org/using-verify-for-local-authority-multi-service-portals-alpha-project/

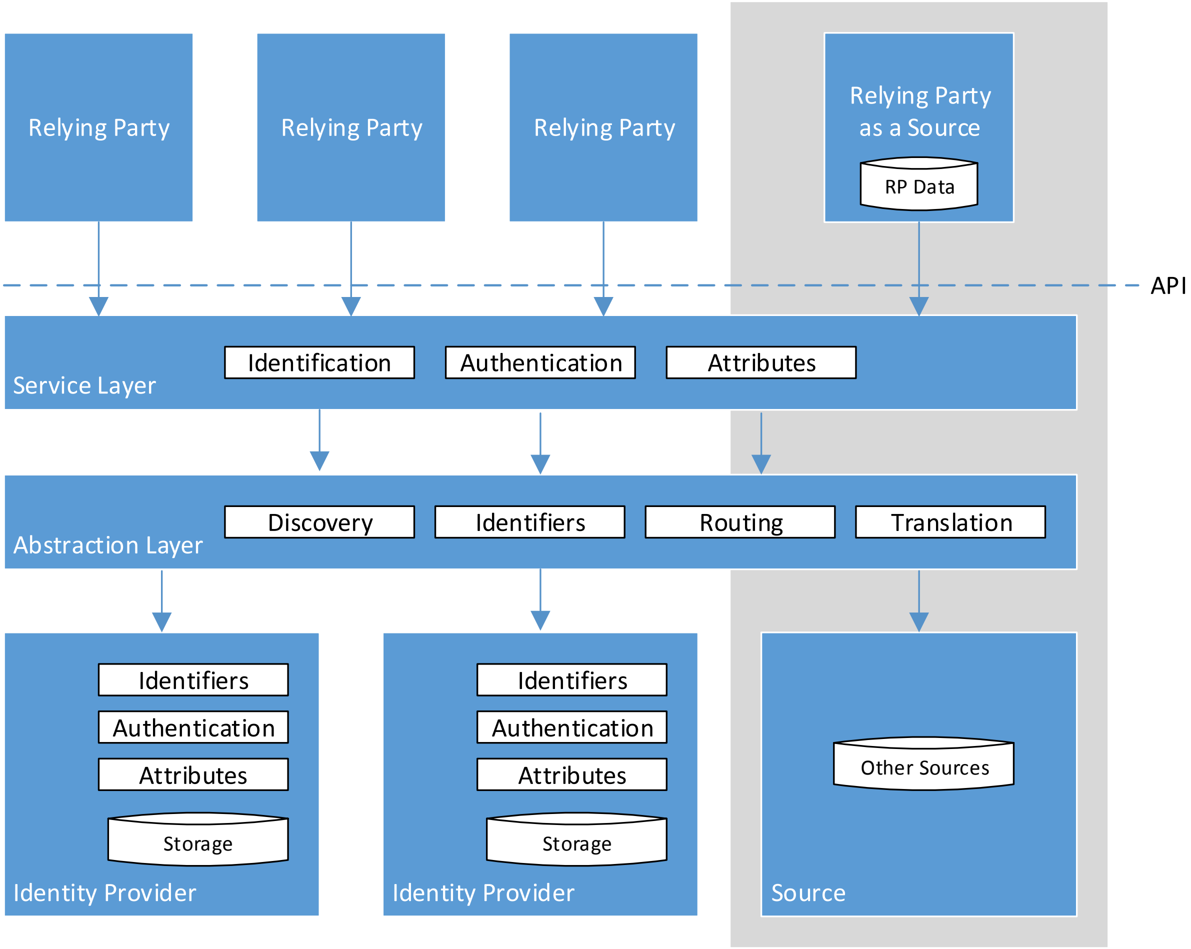
6. Conceptual Architecture and Integration Solutions

6.1. Introduction

This section proposes a conceptual architecture for the Scottish Government, derived from the analysis above. The aim is to consider, at a high-level, the overall shape the architecture could take, in order to inform the next steps that the Scottish Government should take.

A key component of the architecture is the need for integration services that would be sourced by the Scottish Government. Options for these are also considered.

6.2. Conceptual Architecture



The proposed technical approach to Digital Identity, as illustrated in the above diagram, is as follows:

6.2.1. API

Relying Parties would integrate with the Digital Identity service via a flexible API that has the following characteristics:

- Positions Digital Identity as a service Relying Parties can use, extent of use will be determined by the Relying Party

- Minimises the deep integration and avoids tight coupling with the Relying Parties
- Can provide a flexible set of services that Relying Parties can use in a way tailored to their own needs
- Does not attempt to align all Relying Parties systems, recognising that across the many Scottish public services this would be difficult to achieve
- Does not solve Relying Parties internal data quality issues but provides a tool that will help as they address these issues

The following types of (high-level) operation are anticipated to be offered via the API:

- Identification
    - Discover if IDP can do ID&V on user
    - Ask for ID&V
- Authentication
    - Get authenticated identifier
    - Request Authentication for user with specified identifier
    - Discover if IDP can step-up user
    - Ask user to step-up
- Attribute Request
    - Discover if Authenticated user has required Attribute
    - Ask for Attribute (once discovered)
- Attribute storage
    - Discover if IDP can store Attribute for user
    - Ask user if they want to store Attribute
    - Store Attribute

The aim is to provide straightforward Identification, Authentication and Attribute services that allow Relying Parties to discover whether a user has the relevant Digital Identity before asking them to present it. This should enable the user experience to be simplified, with users only being asked to do things they can actually complete.

The APIs should allow Authentication to be done without Identification where the Relying Party either doesn’t need it or has other means to determine who the user is. When the Relying Party is performing its own identification steps, the APIs could provide a means for that evidence to be shared with the external IDP.Inevitably the first time the user accesses the service, there will be a need to present the user with a choice of IDPs – this could implemented by the RP (if API calls allowed them to interrogate the service for available IDPs), or by the Scottish Government as part of the Service and Abstraction Layers.

6.2.2. Service and Abstraction Layers

The Scottish Government would source an integration layer to connect the API to the supported Identity Providers. For the purposes of the conceptual architecture this is split into two parts:

- A service layer that provides the consistent and standardised API to Relying Parties

- An abstraction layer that isolates the service layer from the specific integration to each IDP, mapping identifiers and allowing IDPs to be added without impacting the service layer.

A key consideration will be whether the Scottish Government defines a standardised interface (API) for IDPs, requiring them to support that "as is" as a condition of entry or whether (as the above suggests) the abstraction layer provides integration specific to the needs of each IDP. There are pros and cons to each approach.

6.2.3. Identity Providers

The aim of the conceptual architecture is to provide a flexible way to support identity providers in the market today (mainly GOV.UK Verify), new identity providers that could emerge (such as GOV.UK Verify Identity Providers operated outside of Verify and Fintech identity providers) and potentially a Scottish Government sourced identity provider (such as myaccount or a replacement for it).

6.2.4. Sources

As discussed in section 5.3, the Scottish Government should seek to incorporate alternative sources to ensure that the Digital Identity service can be used by all sections of the population. Two types of source are envisaged:

- Relying Parties themselves can be sources of verified identity data, acquired as a result of the services offer by the Relying Party to users. Relying Parties may wish to offer their customers the ability to upload the identity data that they have verified into their identity account – provided the digital identity service ensures all necessary data protection measures are in place. This would allow those Relying Parties to assist their customers in establishing assured Digital Identities, which in turn will provide them greater access to digital services.

- Some sources (such as schools data) will be background sources, similar to credit bureaux, without a direct relationship with End-Users. These can potentially be made available to the Identity Providers through the Abstraction Layer, although care will be needed to ensure that appropriate data protection controls are in place.

6.3. Scenarios

The conceptual architecture, and in particular the API approach, allows for a number of scenarios including, but not limited to:

- Migration of known user to new authentication credential: the user presents or uses their new authentication credential (provided by an Identity Provider) in the context of an existing service (in-person or digital) which allows them to then assert their identity digitally to that service provider (Relying Party) in the future.

- Growing identity assurance over time: the user signs up for a Digital Identity at the point they first access a digital service. Initially only limited checks are performed and so the Digital Identity is only viewed as low assurance. As the user continues to use the service at various points events occur that corroborate the users identity (e.g. the user replies digitally to a letter sent in the post). This enables the user's identity assurance to be increased.

- Risk based approach: the user presents a Digital Identity to the Relying Party that does not meet all of their normal identity assurance requirements. The Relying Party takes a risk-based decision on whether to provide the service based on the type and context of the service request. If the Relying Party decides to offer the service, this can be monitored over time to gain confidence in the Digital Identity.

- Assured identity from day one: the user signs up for a Digital Identity at the point they first access a digital service and is able to complete the checks to obtain an assured digital identity on day one. This enables the user to start using a wide range of services immediately.

6.4. Integration Solutions

This section assesses integration middleware and hub solutions (both identity focused and more general purpose) available from the market that could potentially support the rapid and agile development of a flexible and extensible infrastructure for the “common approach” to Digital Identity.

As suggested in the conceptual architecture above, it is likely that some form of integration middleware will be required as part of the solution to enable Relying Parties and Identity Providers (each typically with pre-existing and disparate systems and services) to consume and/or provide online identity assurance services securely, reliably and with a minimum of effort.

Middleware will also support a migration towards open standards (such as OIDC and SAML) which should provide greater flexibility moving forwards. This is especially important given the rapidly evolving nature of the Digital Identity space.

There are broadly speaking two types of middleware that the Scottish Government could consider:

6.4.1. Middleware Type A – Identity Focused Hub

Several existing Digital Identity schemes (such as GOV.UK Verify and the eHerkenning scheme in the Netherlands) used hub-based architectures, with multiple IDPs being accessible via one or more hubs. This model has also been discussed extensively within the OIX, with several OIX members having hub offerings.

Examples providers include (in alphabetical order):

- Digidentity, who provide a hub as part of the eHerkenning scheme[35] and part of OIX

- MVine, who provide a portal and identity middleware platform. Active in OIX and GSMA Mobile Connect.

- Microsoft, who offer a “Citizen Identity Hub” solution running on top of their Azure Active Directory B2C platform.

- SecureKey, who provide an Authentication hub in Canada and have collaborated with Idemia on OIX projects.[36]

[35] https://nl.wikipedia.org/wiki/EHerkenning

- Signicat, provider of identity integration services based in Norway but with a presence in several European countries.

Pros	Cons
Hub Providers will understand the identity use case	Unclear how much flexibility hub providers would have for alternative or variant architectures.
Specialist players will be more amenable to making enhancements to platforms, especially when potential for reuse in other contexts	Capacity to make enhancement in a timely manner may be an issue, depending on nature of change.
Likely to support OIDC and SAML "out of the box"	

6.4.2. Middleware Type B – Generic Middleware

Large technology firms such as IBM, Oracle and Microsoft provide, amongst other things, general purpose middleware capable of being deployed across a range of applications and services. Being general purpose, it is likely that these middleware solutions will require significant development work to provide the specific integration layers required by Scottish Government. On the other hand they will be flexible.

Pros	Cons
Sourcing expertise in the middleware should be straightforward.	Technology providers may not have a strong or specialised knowledge of Digital Identity.
Highly flexible	Level of support for identity specific standards and protocols will vary.
	Likely to require significantly higher capital expenditure due to need for significant design and build effort (compared with using a hub tailored for identity) including potentially significant customisation / configuration costs.

6.5. Standards

The Scottish Government should envisage appointing a Digital Identity standards owner.

Relying Parties will ultimately be responsible for determining the level of assurance needed by their services. In order to do this, Relying Parties will need to be able to assess the quality of Digital Identities presented, including the sources and processes employed to establish those Digital Identities.

It will not be practical for every Relying Party to audit every Identity Provider and Identity Source. Standards should be developed that allow Relying Parties to make their Identity Assurance decisions.

Identity Assurance standards provide a means for assessing the technologies and processes employed in digital including any requirements for audit or certification. We envisage that where appropriate these

[36] E.g. http://oixuk.org/wp-content/uploads/2017/06/OIX-White-Paper-Digital-ID-for-Pensions-Dashboard-Final.pdf

standards will be aligned with existing standards such as the UK Governments Good Practice Guides (GPGs) and the European eIDAS regulation.

6.6. Recommendation

As a next step we recommend seeking to conduct one or more alpha projects to test the above approach. We recommend seeking to establish a minimum viable product involving at least 2 Identity Providers, with the aim of demonstrating some straightforward Identification and Authentication solutions.

For the alpha projects, we recommend working with one or more Middleware Type A (Identity Focused Hub) providers for the service and abstractions layers. This should not require a significant build activity, as these providers specialise in identity they should be able to provide a working platform very quickly and it will be a good test of their flexibility.

The choice of Relying Parties and services will be important. For the project to be successful the Relying Party will need to be agile, able to provide functioning test instance of a digital service with the necessary test data. Test data will need to be realistic to ensure that the alpha project is a true test of feasibility, in particular exploring the issues that often arise as a result of data quality issues.

Appendix 1 – Version Control

Version	Date	Summary of Changes
0.06	01-May-18	First draft for internal review (only)
1.00	08-May-18	Initial Baseline – addressing review comments
1.01	12-May-18	Not issued
1.02	14-May-18	Minor changes following review by Scottish Government
1.03	01-Jun-18	Executive Summary Added