The Scottish Government
Riaghaltas na h-Alba

# Technical Options

## Scottish Government
## Online Identity Assurance

consult hyperion

ase
consulting with clarity

# Objectives of Digital Identity

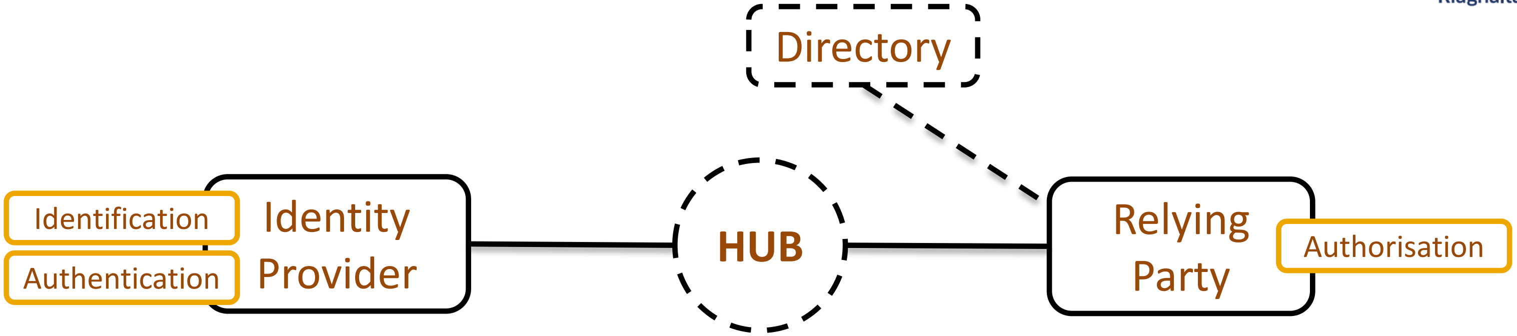
The Scottish Government
Riaghaltas na h-Alba

1. **Common Approach**: 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. **Designed for citizens**: To develop a solution that is designed with and for members of the public (service users) and that stakeholders can support.
3. **Appropriate to task**: 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. **Privacy protecting**: To develop a solution where members of the public can be confident that their privacy is being protected.
5. **Economic**: To develop a solution that brings value for money and efficiencies in the delivery of digital public services
6. **Future proofed**: 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

# Scope of Digital Identity

- Narrow identity requirements
  - Establishing you are dealing with the correct individual with a sufficient level of assurance for the service in question (e.g. core attributes)
  - Knowing it is the same customer in order to provide a consistent and tailored user experience (e.g. authenticated identifiers that allow recognition of the same customer)
- Broader attribute exchange requirements
  - Allowing the individual to see and control the sharing of a wide range of attributes (verifiable personal data) beyond narrow identity data.
  - Allowing the individual to permit or deny the sharing of attributes between organisations for clearly defined and beneficial reasons.

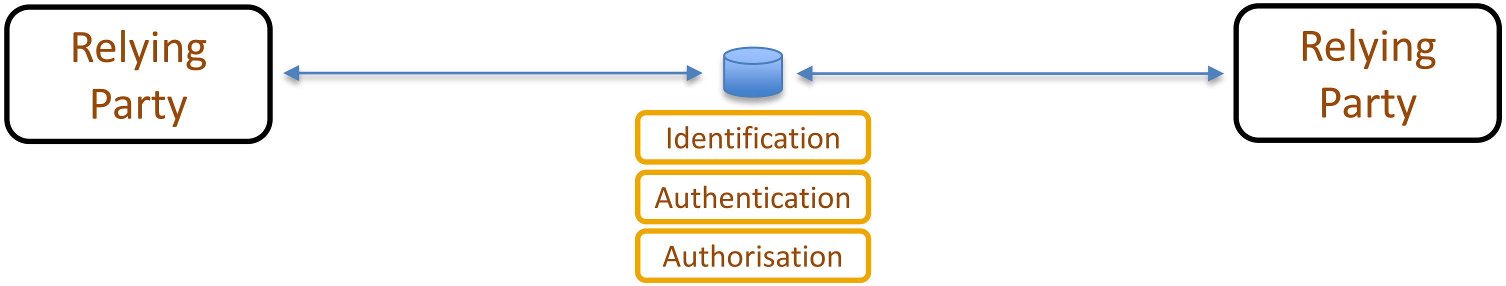
# Examples: Identity Focused



| Model | Example | Privacy |
|---|---|---|
| 1. Multiple IDPs with Hub | GOV.UK Verify, BankID Schemes | Hub provides blinding |
| 2. Multiple IDPs without Hub | Mobile Connect | IDP choice but limited blinding |
| 3. Single IDP with Hub | New Zealand RealMe | Hub provides air gap |
| 4. Single IDP without Hub | Social Logon, Fintech Identity Providers | Significant variance between providers |

- Multi-party schemes will be expensive and slow to market
  - GOV.UK Verify has been through a lot of that pain already
- Single party schemes likely to be cheaper and quick to market
  - Privacy and perception implications need to be considered.

# Examples: Attribute Focused



| Model | Example | Privacy |
|---|---|---|
| 5. Personal Data Stores | Various personal data ecosystem start-ups | Usually strong privacy focus |
| 6. Distributed Ledger Technology | Various DLT identity start-ups | Some have strong privacy focus |

- Aligns with putting the customer at the centre
- No examples at scale to date
- Potentially puts too much burden and responsibility on the customer
- Could however be positive architectural component of more conventional digital identity solution

# Evaluation

| Priority Requirement | Rationale |
|---|---|
| Identity Functionality | Utility functions to enable many services |
| Demographic Coverage | Customer base includes harder to reach |
| Ease of use | Simple trusted services key to adoption |
| Privacy protecting | Customer must be put at centre |
| Time to market | Easy to lose momentum |
| Public perception | Solution must be transparently good |

| Additional Requirement | Rationale |
|---|---|
| Attribute Exchange Functionality | Longer term future value |
| Channel Coverage | Primary need is to support digital* |
| Level of Assurance | Do not want to limit solutions |
| Commercially attractive | Likely to become more important later |
| Maturity | Do not want to limit solutions |

| Option | Score |
|---|---|
| 5. Personal Data Store | 47 |
| 4. Single IDP without Hub | 47 |
| 3. Single IDP with Hub | 43 |
| 1. Multiple IDPs with Hub | 38 |
| 2. Multiple IDPs without Hub | 37 |
| 6. Distributed Ledger Technology | 35 |

Each option is scored against the requirements with the “priority” given double weighting of the “additional requirements”

*Service design project suggests support for mobile critical for inclusion. This is likely to be implementation dependent.

# Existing Digital Identities

- Many customers already have digital identities:

**National Entitlement Card**

- 1.5m contactless cards (ITSO CMD2)
- ID&V done at card issuance. Verified data stored by NEC and uploaded to MyAcccount
- Potential to use cards as cryptographic token to provision mobile identity (would require cooperation of Transport Scotland and access to ISAMs)

**MyAccount**

- 2m dormant accounts as a result of NEC issuance
- 500K active accounts
- Checks done against NHSCR data (within constraints of LEARS Act)
- Proposal to replace / update. Focus on more flexible ID&V.

**GOV.UK Verify**

- Number of Scottish customers with Verify account unclear (pro rata figure would be 165K)
- Different possible approaches:
  - GOV.UK Verify as a “pattern” for a new scheme – identities not re-used
  - Re-use following whichever model is adopted for private sector re-use
  - Scottish Government becomes RP(s) in the current Verify scheme via GDS hub

# Existing Digital Identities

- Many customers already have digital identities :

GSMA Mobile Connect

- Published Mobile figures are not real.
- UK operators are focusing on back-end attribute sharing
- Other markets, especially developing, focus is not logon
- Potential additional source, which is the role played in GOV.UK Verify

PSD2 / Open Banking

- PSD2 mandates banks to provide APIs to TPPs for account information and payment initiation
- Identity providers could become TPPs and leverage those APIs as an additional source. Data is account & transaction related rather than identity per se.

# Key Considerations

- Is it necessary or desirable to allow same digital identity to be used for central and local government?

| For | Against |
|---|---|
| • "Common approach"<br>• Digital identity with greater utility<br>• Familiarity with increased frequency of use | • Wider range of requirements<br>• Variability of LoA for LA services<br>• Local government more fragmented<br>• Privacy concerns with joining up central and local government? |

- Could the government be a digital identity provider?

| When possible? | When not possible? |
|---|---|
| • Demonstrable separation from and between service delivery organisations<br>• Digital identity not compulsory | • If solution does not engender separation<br>• If mandatory or becomes only route to access some services. |

# Key Considerations

- How can we achieve a separation between identity providers and relying parties (to maintain acceptable levels of privacy)?

| How? | Example |
|---|---|
| Hub providing air gap between IDPs and RPs | GOV.UK Verify |
| Personal Data Store | MyDex, Meeco, SOVRIN (DLT) |
| Smart card eID (depending how integrated) | Austrian eID |
| Vendor providing identity services only | RealMe, Yoti, itsme, Miicard |

- Are precise levels of assurance too restrictive?

| For | Against |
|---|---|
| • Drives standardisation<br>• Good for regulatory compliance (e.g. AML/KYC) | • Could exclude innovative solutions<br>• RPs may not agree on levels<br>• Ultimately it is an RP risk decision |

# Key Considerations

- How to best serve geographically remote citizens

| What will not work? | What could work? |
|---|---|
| • Rely on commercial IDPs, where hard to reach groups may not be commercially viable. | • Create specific identification pathways, e.g. leverage on Social Security home visits, work with local authorities, Post Office and utilities<br>• Risk based approach, accept lower LoA |

- How to best serve excluded (e.g. thin file, disabled)

| What will not work? | What could work? |
|---|---|
| • Fully digital solutions where data and documents may not be available for conventional identification, or ergonomic issues. | • Local authority offices<br>• Alternative data sources<br>• Post Office branch network<br>• Risk based approach |

# Conclusions

- One size unlikely to fit all:
  - Need approach that allows multiple digital identity solutions*
  - Could take a catalogue or portal approach
  - Should allow common integration and common UX
- Existing Scottish identity assets not sufficient to provide full solution
  - Although could be part of migration path
  - Should be prepared to build support for hard to reach groups
- GOV.UK Verify should be part of the solution
  - Assuming Scotland can simply “plug in” to it
  - Provide a common approach for existing Verify users
- Should solicit digital identity solutions built around a Personal Data Store
  - To address both identity and personal data requirements
  - Supports future migration to DLT / Blockchain

*Note, this is the approach taken by the Canadian Government – logon via bank plus government built alternative.

# Next Steps

- Focus on Target Architecture ahead of Outline Business Case
  - Need greater clarity on recommended approach for business case
- Target architecture will
  - Be high level / conceptual
  - Focus on how to achieve common approach for:
    - Relying parties through common integration
    - Citizens by defining common identity services, that can be packaged up by “identity providers”
    - Consider inclusion of supporting capabilities to be delivered by Scottish Government to support hard to reach customers
    - Consider options for interoperation with GOV.UK Verify
    - Consider potential roadmap towards new DLT architectures