Online Identity Assurance National Stakeholder Group

Paper number: OIASG-05

Paper title: Summary of Outputs from the Discovery Exercise

Response: for discussion

Summary of Outputs from the Discovery Exercise

Purpose

1. To provide the National Stakeholder Group with a summary of the outputs of the service design and technical discovery work, undertaken as part of the discovery phase of the Online Identity Assurance Programme, at **Annex A**.

Detail

2. The discovery phase of the Online Identity Assurance Programme ran from January to May 2018.

3. Service design research was conducted by We Are Snook to gather insights about user experiences related to digital identity. This aimed to identify the problem that an online identity assurance solution might address, explore the user journeys, and identify user concerns and needs.

4. Technical discovery research was conducted by ASE Consulting and Consult Hyperion, aimed at identifying the technical options for identity assurance, including fit with the service provider landscape. This initial work explored the technical options, solution characteristics, architecture principles and the preparation for an alpha phase.

5. The full set of discovery outputs will be published on the Scottish Government website and shared with the National Stakeholder Group.

Recommendation

6. That the Group considers the summary of outputs from the discovery exercise, at **Annex A**.

Scottish Government Online Identity Assurance Team
June 2018

Annex A

Online Identity Assurance National Stakeholder Group

Summary of Outputs from the Discovery Exercise

1. The Scottish Government's online identity assurance discovery piece of work ran from January to May 2018. The discovery involved service design user research and technical options appraisal, delivered on behalf of Scottish Government by external consultants. This Annex summarises the outputs from this work.

2. The service design research was conducted by agency We Are Snook to gather insights about user experiences related to digital identity. The aim of the discovery service design was to identify the problem that an online identity assurance programme might address, explore the user journey(s) and identify user concerns and needs.

3. The technical discovery work was conducted by ASE Consulting and Consult Hyperion. The aim of the technical discovery was to identify the technical options for identity assurance, including fit with the service provider landscape. The initial work explored the technical options, solution characteristics, architecture principles and the preparation for an alpha phase.

Service Design Discovery Outputs

4. We Are Snook conducted scoping interviews with key Scottish Government policy teams interested in identity, agencies, local government representatives and UK Government Digital Service. Qualitative research included interviews involving about 30 people in organisations in Falkirk, Glasgow and Dundee; and 17 individual interviews spread across a range of ages. Snook also conducted 2 surveys, asking for opinions and thoughts about online identity: one dedicated to young people (44 responses); and the other aimed at those aged over 25 (40 responses). Snook also were involved in the first National Stakeholder Group meeting, and a discovery 'Show and Tell' session, which enabled some specific stakeholder feedback on the work.

5. Snook identified 3 key recurring themes from the research. The first 2 themes – which were expressed equally across all the groups and ages interviewed – contained these clear and oppositional views:

- 'Convenient' – feedback from people looking for an easier way to transact with public services
- 'Cautious' – feedback focusing on concerns about data privacy and security, above all things

The third theme was about 'barriers to access' – from people who identified the importance of access without barriers, particularly around assisted digital and mobile-first solutions.

6. People in the 'convenient' camp, talked about complex, fragmented services and having to navigate across multiple agencies. For example they spoke about confusion with different online application systems, and forms which asked questions

in different ways, so that people felt they might be 'tricked' into giving a wrong answer. People expressed frustration over the number of paper forms they had to fill in and talked about information given to multiple departments and agencies: perceived as unnecessary, time consuming, and costly. They also spoke about having to send document originals to multiple agencies. Some referenced the ease of creating and authenticating identity for other services, like banking or online shopping. There were clear views that processes for public services could be simplified. And on the whole, people were keen for data to be shared between organisations to avoid them having to provide the same information repeatedly.

7. Those who were much more 'cautious' about digital identity put a great deal of value on their privacy and security above all things. This caution was directed at: those who hold the data and how reliable they are; who can access personal data and who controls this; and how safe data is kept and the risk from hackers. There was a spectrum of opinion on who people trusted to hold their data:

- Some people were comfortable with private sector organisations, such as banks and Google, but were distrustful of government services
- Others were more trustful of government but wary of private organisations holding their data.

Key concerns in the 'cautious' camp were: who would have access to any data stored, and ensuring appropriate and proportionate use and access; clear information about who can access their data and visibility over who is accessing it and why; and some even called to directly control their own data.

8. In terms of 'barriers to access', for some people this was their own lack of digital skills and lack of technology or internet access. Others (specifically those with visual impairments) described the challenges of online and paper forms that were not available in formats suitable for text to speech translation. Other issues raised were around an identity solution being able to accommodate proxy or third party management, on behalf of an individual using the service. In relation to mobile accessibility, the clear recommendation within the report was that an online identity solution must work easily on a mobile phone.

9. Snook's report, made specific recommendations around the path for access to online identity services, aimed at simplification by having a common, consistent approach. This would comply with the 'Digital First Service Standard', which states that when designing new digital services, organisations must "focus on what your users want to do rather than the organisation's objectives or the mechanics of delivering your service." Snook identified '7 easy steps' around access to online identity services. focusing on how we might enable people to move through the journey of creating and using their online identity in the fewest possible steps:

1. Understand – the user gets a clear explanation of what is involved in creating an online identity
2. Create – the user creates a personal profile
3. Gather – the user gathers the documents to establish his or her identity
4. Verify – the user can use a tool to verify that they are this person (e.g. taking a photo or sharing key information)
5. Confirm – the user gets clear confirmation that they have created a verified online profile
6. Expand – the user can save and reuse this profile in future

7. Remember – the user can get reminders from the system about when they might need to update information (e.g. to renew a Blue Badge)

Technical Discovery Outputs

10. ASE Consulting and Consult Hyperion presented technical discovery research outputs covering 4 main areas:

- a technical options appraisal – exploring what models exist and whether they could provide a solution
- identification of the solution characteristics for a Scottish identity solution – identifying the expectations and requirements for identity assurance and how current solutions measure up
- architecture principles – a decision making framework and standards to which the solution should adhere to
- preparation for alpha – advice on the requirements and content of a potential alpha phase

11. Within the technical options appraisal, the consultants presented their considerations around how to potentially leverage existing digital identity services and what the requirements of the online identity solution might be. The technical options report contained the following conclusions:

- One size is unlikely to fit all – that a Scottish system needs an approach that allows multiple digital identity solutions, that allows integration and supports a common user experience
- Existing Scottish identity assets (e.g. the myaccount service) are not sufficient to provide a full solution on their own (although could be part of migration path)
- GOV.UK Verify (run by UK Government Digital Services) should be part of the solution and that this would provide a common approach for existing Verify users, assuming Scotland can simply “plug in” to it (there are around 220,000 people in Scotland who have an existing Verify identity)
- That the digital identity solution should be built around a ‘Personal Data Store’ – a move that might essentially allow a user to have greater control of their own data and who might access it.

12. The solutions characteristics outputs map 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. The advice concluded that:

- From a technical perspective, GOV.UK Verify appears well placed to provide assured digital identity services. However, 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 individual identity providers (operating independently of Verify) and the Fintech (financial technology industry) players.
- That at face value, myaccount (Scotland’s existing secure sign-in service) 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), with low levels of assurance available (i.e. a less thorough checking system to establish that a claimed identity belongs to that user). However, the consultants noted that the Improvement Service (who runs myaccount) is actively exploring potential enhancements to the service.

13. The consultants also considered the reach of existing services available to the Scottish market. In summary, the findings were:

- The number of people in Scotland using GOV.UK Verify today is relatively small, but growing.
- The relevance of individual GOV.UK Verify identity providers to Scotland varies as would their ability to bring scale outside of GOV.UK Verify. This includes individual providers which stand out as having a large number of touch points with individuals which may provide a means to establish digital identities.
- Fintech providers may provide an interesting alternative for some customers, if they reach scale quickly.
- myaccount has a large potential number of users, although with low levels of assurance currently, meaning less value for services requiring assured identities (noting it is possible to add requirements or steps that might increase the level of assurance, as done by some councils currently).

14. The consultants identified that many of the existing digital identity services build digital identities from the same types of sources, such as credit information and official documents like passports. These address the portion of the population that is financially active (e.g. uses credit cards, mobile contracts, mortgages and loans) and that travels. There is clearly a significant section of the population that these sources do not address well, including young people, financially excluded and the elderly. Advice is that Scottish Government should therefore seek to incorporate into its digital identity approach alternative data sources that can address these gaps, such as the National Entitlement Card and local authority data.

15. Advice overall is that Scottish Government should take an approach that provides flexibility to use 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.

16. Outputs from the technical discovery also include a set of architecture principles, to which the online identity assurance programme is proposed to adhere. These are essentially a decision making framework and technical standards for the programme as a whole. The aim is to ensure that whatever product is delivered through the alpha, it should meet the standards contained within the principles.

17. The technical discovery additionally sets out a proposed structure for the delivery of the alpha phase. The proposal is for the alpha to create a prototype of the identity assurance solution to:

- provide confidence that the solution is financially and technically feasible
- demonstrate the technical infrastructure, involving Scottish public service partners and identity provider organisations
- test the (prototype) solution with end-users.

18. The completion of the alpha would aim to:

- provide evidence to help decide if the programme should proceed “as is”, stop, or if it requires re-design or re-structuring
- enable the key strengths, weaknesses and risks of the solution to be identified and/or confirmed
- inform the cost estimates for subsequent stages of the programme
- inform the approach to the beta phase (if any), including which service elements should be the focus

19. Advice is for the alpha to include Scottish public service providers with a recognised need for “real-world” online identity assurance services. Following discussion of the technical outputs at the 21 May 2018 meeting of the Online Identity Assurance Expert Group, the 3 services proposed to participate in the alpha project are:

- Social Security
- eHealth programme
- local government

20. The proposal is that for the alpha phase the programme will work with between 1 and 3 identity providers, and that these identity providers will already be active in the market. This might enable Scottish Government to test the flexible approach to using different identity providers, as recommended in the solutions characteristics report.

21. Given that myaccount is an existing solution that is owned by the public sector in Scotland it may be worth considering inclusion in the alpha phase to determine to what extent it can meet the objectives of the programme: either alone or in conjunction with other solutions; and as is or with enhancements. The inclusion of eHealth and local government within the alpha phase will also provide an opportunity to explore interaction with the existing myaccount service and how a new online identity service might differ from the existing offering.

22. The technical outputs propose a 6 month alpha phase, costing around £700,000.

Scottish Government Online Identity Assurance Team
June 2018