ANNEX A

Online Identity Assurance National Stakeholder Group

Outputs from First meeting Workshop Discussion

1. The outputs from the workshop discussion within this Annex are grouped according to the key themes that emerged.

Role and Remit of the National Stakeholder Group and how the Group should work together

2. Comments on the Group's remit:

- The National Stakeholder Group should provide an advisory role and not be a decision making body.
- The full National Stakeholder Group should meet on a 3 monthly basis, but consideration should be given to more frequent involvement, for example invitations to show and tell events, opportunities to be kept informed of progress and by exploring other opportunities for providing input.

3. Comments on the Group's membership:

- Additional thought should be given to the Group's membership to ensure that it includes a wide range of organisations whose interest and influence would be helpful in developing this work.

4. Communications with the National Stakeholder Group:

- Consideration should be given to establishing an online forum for the National Stakeholder Group and the Programme Team, to facilitate and encourage the sharing of ideas, information and discussion.

5. Frequency and Location of Meetings

- Full meetings of the National Stakeholder Group should be as inclusive as possible and, as such, should take place in a space that is accessible to the majority (with the option of videoing in for those unable to make it to the venue), which supports good acoustics and where everyone's physical comfort is catered for.

6. Other Ways of Working

- The Programme Team should continue to publish blogs, papers and other information. However, we cannot assume that people external to the Group will find and access these and so other communications strategies and channels should be employed.

Online Identity Assurance Programme Considerations

7. The needs of the individual user should be at the heart of what we do. We should ensure a Person Centred Approach by:

- Accommodating individual preferences and designing an approach which offers multiple levels of authentication, to enable citizens to choose whether they sign-up to a single or multiple providers or services.
- Providing individuals with the opportunity to prove their identity by non-online methods, such as in person, to access public services.
- Designing the approach in collaboration with users to ensure it meets their needs and, in particular, is easy to use whilst at the same time ensuring that security of information is guaranteed.

8. The design and implementation of the approach should be underpinned by set guiding principles which should:

- Be compliant with the General Data Protection Regulation (GDPR), any other principles agreed upon as part of the programme, or Information Commissioner's Office codes aimed at protection the citizen's privacy and rights.
- Incorporate safeguards to ensure that minimum data sharing between providers is standard.
- Involve a mechanism to regulate against the need for either the service user or provider to duplicate effort.
- These guiding principles should relate to the Scottish Government's Identity Management and Privacy Principles, and consideration should be given to updating these in line with the emerging programme.

9. In designing the new approach we should be mindful of the existing landscape and of future changes in technology by:

- Considering the various organisations that are already assuring their customers identity online and take account of this when developing the new system to prevent unnecessary migration costs or unraveling of what is already in place.
- Developing an approach that is flexible enough to keep pace with changing behaviors and technological and social obsolescence.
- Recognising that separate organisations may wish to assure citizens in different ways.

10. We want service users and providers to be able to use the approach with confidence and will build citizen trust by:

- Listening to citizen needs and taking them into account at all stages of the process.
- Clearly communicating details of the emerging system.

- Providing citizens with reassurance about who will be able to access the system, what data will and won't be needed, what data will be held about individuals, and by delivering choice and control.
- Ensuring the approach is proportionate and offers various levels of assurance appropriate to the service a citizen wishes to access.
- Supporting fraud reduction, securing people's data, improving privacy and by communicating a non-technical narrative of what the approach is.