Next steps to DCMS Digital Identity policy development

Thank you for agreeing to participate in one of our engagement sessions on digital identity for the UK economy. In advance of your session, we'd be grateful if you would complete the following questionnaire to help ensure your valuable contribution and expertise is fed into the development of the appropriate session, and that where possible, you are allocated the session that is of interest to you.

The questionnaire is broken down into six sections, covering the development of a digital identity Trust Framework, legislation, governance and oversight, attribute checking of government data, international interoperability, and inclusion and privacy. Please don't feel obliged to complete the entire questionnaire if you feel particular sections are not relevant to your interest or specialism. We'd be grateful if you could complete the questionnaire by Monday 12th October.

What is your name? *

Colin Wallis

What organisation do you work for? *

Kantara Inititiative

What is your email address? *

.....@kantaraInitiative.org

Trust Framework development

In response to the Call for Evidence, the general consensus was that government should take the lead in setting the rules and building public trust. Other countries and markets have developed a trust framework to address these challenges.

A trust framework is a set of rules and standards governing the use of digital identity. All organisations that are part of the trust framework will create products and services, check identities and share attributes in a consistent way, enabling interoperability and increasing public confidence.

What thematic areas should be considered in the development of a trust framework and why?

1.Scope of application and phasing; public central? public county/local? private? NGO sectors? Timeframes are important because the uses cases with the most frequent use drive higher adoption rates.
2. Only 1 TF with multiple schemes? Or multiple TFs? Because this decision has a knock-on effect on federation, interoperability and potentially liability.
3. Only 1 Level of Assurance? Or Multiple? Or none? Similar knock-on effects as above.
4. Agree on the actors and roles active in a/the TF.
5. Business model /sustainability (mixtures of taxpayer funded, subscription, per transaction etc), because without these being structured there is too much risk, insufficient incentive to invest. Decide on policy baselines e.g. that if a service or RP mandates the need for the use of the Trust Framework, it should be free to the end user, but if an individual chooses opts-in to use a service the individual pays for it.
6. Liability because without this being structured there is too much risk, insufficient incentive to invest.
7. "... will create products and services, check identities and share attributes in a consistent way, enabling interoperability and increasing public confidence"..may not be actually a correct statement depending on what is meant by 'creating products and services, since assessor and certifiers of the parties and their solutions may not have been envisaged as being included.
8. Establishing trustworthiness is useful but not sufficient. Once trust is established, the greater need is not building trust but not losing it. So consideration of edge cases, failure cases, account recovery early on is essential.

Which existing standards or guidance do you think should be referenced?

ISO standards/specs such as 24760, 29003, 29115 and its new PWI, ISO 17065 (and applicable 17000 series standards); IETF RFC 8485; NIST SP 800-63-3, NIST SP 800-53; GPG 44 & 45, Australia's TDIF, Canada's PCTF, NZ's Identity standards suite (in draft), eIDAS, BSI PAS 499, BS 8626; UNCITRAL WG IV Draft Provisions on the use and recognition of cross border identity management and trust services; W3C Verifiable Credentials Implementation Guidance, W3C Web Authentication: An API for accessing Public Key Credentials; FIDO 2 (CTAP), Kantara Identity Assurance Framework, ISO 29184 online privacy notices and consent, NIST Privacy Framework, Kantara Consent receipt Specification, GDPR, UK Data Protection Act. User Experience guidance and best practice (standards if there are any) is critical to test applying services against.

Thinking about UK legislation, international legislation and/or technological developments, what dependencies do you think should be considered in the development of the trust framework?

1.A single trust framework needs a single central agency lead. A policy split between Cabinet Office and DCMS should be avoided. Previous industry-led efforts, e.g. the British Business Federation Association, floundered because the timescale for commitment by each separate government department was unworkable.
2. Consider UK new or amended legislation in the context of legislation in other countries and states (The Commonwealth of Virginia Digital Identity Act is a good beacon). Policy instruments in other countries as well, such as OMB M1917 in the US.
3. Consider Schemes and related Trust Framework operations in other countries that undertake assessment and assurance activities to support Schemes.

Legislation

Legislation for digital identity is needed to provide a basis of national and international confidence in digital identities. This legislation will be the subject of a formal public consultation, as mentioned in the Call for Evidence response published on 1 September. Detailed proposals are being developed and may cover the rules and standards that will be part of the Trust Framework, an oversight function for this enabling framework, and the removal of legal barriers to the use of digital identity.

What legislative changes and data do you need to enable the use of digital identity tools within your business?

1. Legislation to enable (and progressively mandate) public sector registers being available – including postcodes.
2. Sundry provisions for existing legislation including
   - Immigration Act, 2014
   - Immigration, Asylum and Nationality Act 2006
   - Power of Attorney Act 1971
   - Law of Property (Miscellaneous Provisions) Act 1989.
   - Licensing Act 2003 (Mandatory Licensing Conditions) (Amendment) Order 2014.
   - The Fraud Act 2006
   - The Identity Documents Act 2010
   - The Forgery and Counterfeiting Act 1981
   - The Money Laundering Regulations 2017
   - Protection of Freedoms Act 2012 (Chapter 3)
   - The Offensive Weapons Act 2019.
3. The above is English legislation. A review of Scottish legislation will be needed too.
4. Identity related attribute data is needed from its authoritative source, or at a lower level of confidence derived data and individually claimed data.

Where should we prioritise our efforts, and what benefits can we expect to see for people and the economy?

1. Enabling Authoritative sources of data held in central and local government registers to be exposed as yes/no zero knowledge proofs because this will allow 'quick wins' for existing service providers while the TF begins to take more formal shape over time.
2. Making changes to the most critical legislation roadblocks e.g. Alcohol Licencing, Identity Documents..
3. Decide on the suite of standards in light of what is operational, assessed and assured overseas, so that at least mutual recognition might be possible nearer tem if interoperability/convergence is not.
4. Operating a digital identity scheme and associated TF/s is significantly Business Process Re-engineering to enable it to operate omni-channel. Within the system, the failure of a yes/no attribute claim for example, should kick off a process to determine if it is attempted fraud.
5. Business model - policies around who pays for what and in what use case/circumstance, so that providers have the leadtime to plan to engage (or not).

Governance and oversight

A governance and oversight function will be helpful to enable the safe creation and use of digital identities across the economy, and provide guidance if something goes wrong.

What should be the tools available to an oversight body to ensure adherence to the Trust Framework?

1. Assessment and certification of conformance
2. Authority to operate, restricted or revoked.
3. Censure and fines
4. Appeals process
5. Ombudsman
6. Fidelity fund

What should be the consequences for infringements of the agreed Trust Framework?

1. Authority to operate, restricted or revoked.
2. Civil/common law action for negligence and/or breach of contract
2. Censure and fines from the TF
3. Payment to the harmed party from the provider's E&O and public liability insurance
4. Stand down period before re-application

How should redress be handled for organisations that consume digital identity, and for people if something goes wrong?

1. Civil/common law action for negligence and/or breach of contract.
2. Censure and fines from the TF.
3. Payment to the harmed party from the provider's E&O and public liability insurance.
4. Payments from the fidelity fund in the case of for example, a provider has gone bankrupt.

What existing bodies or groups may be well placed to provide oversight?

A mix of skills needed - into a dedicated specialist body drawn from experts for example from the Law Society, Chartered in institute of Accountants (auditors), a mix of central and local government agency reps as Relying Parties, a Consumer advocacy rep, also reps from the other the TF other Schemes and TF operators from other countries such as DG Connect (eIDAS), GSA, DTA, tScheme, Kantara etc... dynamically structured and resourced to avoid conflicts of interest.

It is envisaged that an advisory group will be created to provide viewpoints from industry and privacy groups - how could this be best enabled?

It could be a combination of the following;
1. Consider the lessons learned from what did not work in the Verify project would be one of several ways. An example of what did not work in that project was the PCAG, where its recommendations and outputs could be ignored in the interests of expediency.
2. The advisory group should always have representation on the oversight group - perhaps 2 voting reps cycling annually and elected from the wider advisory group.
3. The advisory group should have observation rights on oversight group meetings, with perhaps 3 meetings per year specifically dedicated to discussing various issues. The oversight group in effect gives problems to the advisory group that it needs help to solve, and visa versa. These become projects that cannot be stalled and are subject to agreed defined timelines.
4. Both the oversight group and the advisory group should itself have maximum periods of rotating on and off.
5. Some roles should have a permanent position even if the people revolve, for example law enforcement.
6. Both the oversight group and the advisory group need to engage in established processes for all aspects of standards life-cycle, not just development or parachuting.

Attribute checking of government data

Respondents felt strongly that the government should unlock additional data sets. Government data was seen as essential for meeting digital identity needs and could be woven with other data sets if the individual chose.

What attribute datasets would be useful for your organisation (beyond passports and driving licences)?

Not applicable for a TF operator such as Kantara.

How likely is it that your organisation will invest to enable checks against government identity data when it is available?

Not applicable for a TF operator such as Kantara.

What is the commercially viable price point for your organisation to make a single check against an attribute dataset?

Not applicable for a TF operator such as Kantara.

Which type of digital identity checks would be most useful to your service model? E.g. are 'yes/no' validity checks relating to data inputted by your customer sufficient? Are photo or fuzzy matching essential components?

As certifiers, we expect fuzzy matching that is context-dependent, with variants on addresses different from that on names, nicknames and variations on transliterations.

International interoperability

The Call for Evidence restated the importance of the UK taking an international approach to digital identity. Respondents see the UK as having the experience to lead the development of international best practice.

How important to you is international interoperability?

	1	2	3	4	5	
Not important	○	○	○	○	◉	Very important

With which markets is it particularly important for the UK to achieve interoperability?

Those with the most frequent population level interactions... US and the EU are the primary ones, with perhaps Canada and Australia next.
Financial Services, Payments, Health,

Privacy and inclusion

Respondents have highlighted privacy, inclusivity, and proportionality as three of the key principles underpinning the development of digital identity for the economy.

What are your concerns about consumer protection and privacy in developing a new digital identity trust framework?

Obviously considerable concern since transparent and trustworthy digital identification is dependent on strong data protection and privacy. However, there is a tension between them and a balance needs to be struck, which may move over time, to reflect consumer feedback (not just relying on advocacy group feedback)

Do you already have practices implemented into your service that focus on diversity, inclusion and safeguarding (e.g. in policies or embedded into technology)? If yes, please provide examples. If not, have you encountered any barriers in trying to do so?

Kantara has such policy broadly reflected in its contracts for its contractors.

What could government do to help ensure digital identity is as inclusive as possible?

Tackle the issue from a business process re-engineering standpoint so it can be delivered omni-channel. Prioritise a process for enabling agents/powers of attorney etc. Establish a consistent policy for bringing illegal immigrants, asylum seekers and thin file residents on the digital identity journey, progressively building their digital identification confidence level over time.

What are your key accessibility concerns in the area of digital identity?

Added costs (time and money) for those unable to use services as a result of disability. That is why the programme needs to be tackled from a business process re-engineering standpoint so it can be delivered omni-channel.

We anticipate that the engagement sessions will commence from 21st October. Please indicate below the topics that are of most interest to you. Please tick all that apply.

What topics are you most interested in exploring during the listening sessions? *

- [x] Trust Framework development
- [ ] Legislation
- [x] Governance and oversight
- [x] Attribute checking of government data
- [x] International interoperability
- [x] Privacy and inclusion