Department of Culture, Media and Sport

100 Parliament Street

London

SW1A 2BQ

13th September 2019

LCCC and ESC Response to DCMS' Call for Evidence on Digital Identity

Introduction

Please treat as non-confidential

The Low Carbon Contracts Company (LCCC) and The Electricity Settlements Company (ESC) are private companies wholly owned by the Secretary of State for Business, Energy and Industrial Strategy (BEIS). They perform central functions in the operation of the Contracts for Difference (CfD) and Capacity Market (CM) schemes. LCCC carries out the functions of its sister company ESC, via a cost-sharing arrangement.

We welcome the opportunity to respond to the Call for Evidence on Digital Identity, and LCCC & ESC wish to draw your attention to certain areas of our response that we believe to be most pertinent:

- Trust would be enabled in digital identity by ensuring that players in the system are subject to robust consequences for inaction, for knowingly providing false information or for interfering with others' information;
- It would be a sensible approach when designing an effective digital identity system to replicate elements of other governmental organisations' digital identification systems, such as the passport office, HMRC and DWP; and,
- The passport office has introduced a digital access portal, and this could be used as an exemplar for a future digital identity portal.

Yours sincerely,

Omer Ahmad

Policy and Regulation Manager
Low Carbon Contracts Company
Electricity Settlements Company

Consultation questions and responses

Needs and problems

Q1. Do you think digital identity checking will be a way to help meet the common needs of individuals and organisations referenced above? What other ideas or options would help?

We do believe that digital identity could help meet the common needs of the individuals and organisations referenced. However, we require a more detailed explanation of what it entails before we could give a more definitive answer.

Q2. What are the economic or social benefits or costs from developing a digital identity system in the UK which meets these needs? Can you provide examples?

No comment.

Q3. What are the costs and burdens of current identity verification processes?

Our organisation's costs and burdens are caused by the need to provide resource to verify the data provided by external parties. We employ a member of staff that completes our due diligence checks on both new and ongoing contracts where identities of directors need to be verified. Our Human Resources team need to use resource to verify the identity of new members of staff and security checks for government access passes.

Q4. How should we ensure inclusion, especially for individuals with thin files?

As an organisation we rarely deal with "thin file" individuals however a face to face access point for those in this situation would be beneficial. Examples of which can be found within the state benefits and HMRC process.

Q5. What currently prevents organisations from meeting the needs stated above?

Our organisation has no other access to verify identity other than the documents provided by the individuals themselves which are detailed on the Government acceptable documents list.

Q6. Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples?

If new company directors were required to create a digital identity and also legally required to keep the details up to date it would provide a reusable asset to our company process.

Q7. What are the building blocks essential to creating this trust? How should the environment be created to enable this trust – for example, what is the role of open standards (identity, technical, operational, business implementation, design requirements for consumer privacy and protection)?

We believe, that open standards applied to the process would create a confidence in the process, cyber security and Legal consequences for misuse.

Regarding DP, the biggest and essential 'building block' to create trust would be for the government to provide full and comprehensive answers to all the questions asked in above answer to Question 1, ensuring the complete transparency of the project.

Organisations would need assurance of the accuracy, up-to-date and relevance of the data held, as well as the pertinent validation measures put in place for this purpose.

Individuals would need assurance that their privacy, their personal data and their rights and freedoms under current DP legislation are guaranteed through the relevant measures and mechanisms put in place for this project.

Also, if it is to be compulsory, how does the project address the 'right to be forgotten'?

To build trust all of these questions must be fully considered and answered.

Q8. How does assurance and certification help build trust?

As a minimum, the level of assurance and certification should provide at least a common level of understanding of the power of the data.

Q9. How do we ensure an approach that protects the privacy of users, and is able to cover a range of technologies and respond appropriately to innovation (such as biometrics)?

As an organisation we do not use biometrics partly because of the higher level of process required by the Data Protection Act (2018). Introducing additional functionality with smart phone usage may introduce more cyber security risks. The passport office have introduced digital access, so this could be a model to follow across other parts of the government.

Q10. How do we ensure digital identities comply with the Human Rights Act and ensure people with protected characteristics are able to participate equally?

From an organisational perspective allowing access by the individual in a face-to-face process whilst still creating a digital identity would be useful.

Q11. How should the roles, responsibilities and liabilities of players in the digital identity market be governed and framed to enable trust?

We believe there should be robust consequences for inaction, for knowingly providing false information or for interfering with others' information.

Q12. What's the best model to set the "rules of the road" to ensure creation of this trusted market?

The government has made large advances into digital identity in the passport office, social benefits and HMRC. The best model for the "rules of the road" should take the lessons learned and applied from these and consider implementing them for the purposes outlined in this consultation.

Q13. Who do you think should be involved in setting these rules?

We believe this should be a cross government process led by the Cabinet Office.

Q14. Do you think government should make government documents and/or their associated attributes available in a digital form, which could be used to help assure identity?

Yes, digital documents remain available even when the hard copies are lost or destroyed. It is a practical application which will need to be safeguarded with adequate cyber security.

Q15. i) For what purposes should government seek to further open up the validity checking of government-issued documents such as passports?

Some examples of where this could be more widely applied include, for the purpose of undertaking Human Resourcing checks and to prevent identity theft.

Q16. i) For what purposes should government seek to further open up the attributes (such as age of citizens) that it holds for verification?

It should be open to all, birth to death and any associated reference numbers should become inactive with death of an individual but remain searchable for digital identify checks.

ii) How should this be governed to ensure protection and citizen control of data?

The data should be open to all who can provide a business need to use it.

iii) What should the cost model be?

The cost model should take account of the reduction in resource by using a centralised service however making it too expensive will limit the take up of the service.

Q17. What's the role of legislation and statutory regulation to grow and enforce a secure, privacy-centric and trusted digital identity market?

We believe, the role of legislation and statutory regulation in this context is to build trust and promote the responsible use of this data in a secure and privacy-centric digital identity market.

Q18. What legislation and guidance requires updating to enable greater use of digital identities?

Consideration should be given to the following legislation:

- Data Protection Act (2018)
- Company Legislation
- Tax Legislation
- Social Benefits legislation
- Employment legislation

Q19. What else should government do to enable the wider use of digital identity?

No comment.

Q20. How could digital identity support the provision of local government services (including library cards and concessionary travel)?

No comment.