

Kantara is pleased to provide responses to the questions posed the UK DCMS in their open consultation on digital identity and attributes.

Kantara is the leading global consortium whose mission is to grow and fulfill the market for trustworthy use of identity and personal data. To fulfill this mission Kantara operates an independent third-party conformity assessment program for the digital identity and personal data ecosystems. In addition to this Kantara has, since its inception in 2009, provided real-world innovation through its development of specifications, such as UMA 2.0, Consent Receipt, applied R&D, and its Identity Assurance (Trust) Framework (IAF). More information is available at <https://kantarainitiative.org/trustoperations/> or contact us at staff@KantaraInitiative.org.

This submission was developed by participants in Kantara’s Identity Assurance Work Group (IAWG). The IAWG consists of individuals from both the public and private sectors with extensive experience in the identity industry including assessing identity services for conformance to established requirements, developing requirements for identity services, and implementing and providing identity related products and services.

Kantara continues to invite the United Kingdom team to keep Kantara apprised of its progress.

## Overall Comments

Kantara has the following overall comments on the information presented by the DCMS.

1. Change the concept from “providing and using Digital Identity” to “enabling Digital Identification”.

This changes puts the focus on why digital attributes are being checked or used. It will also change the perception of Government becoming “big brother” and holding the digital identity of citizens. Rather, it changes the perception to the Government using the information it already has collected about citizens for other purposes to enable other organizations to identify a citizen in order to provide them with a service.

As an example of this subtle switch in concept, the following two paragraphs were reworded:

Online authentication, identity and eligibility solutions can increase security, ease of use and accessibility to public services. They are central to transforming the delivery and efficiency of public services and people’s ability to operate confidently in an increasingly digital economy. It is estimated that widespread use of digital identity products would be worth around £800m per year to the UK economy. Widespread use of digital identity products could also help to reduce the record levels of abuse of personal data and impersonation to commit fraud in the UK, with over 220,000 cases reported in 2019.

The government is committed to realising the benefits of digital identity, without creating ID cards. Earlier this year we published a draft of the [UK digital identity and attributes trust framework](https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework). This document sets out what rules and standards are needed to protect people’s sensitive identity data when used digitally. We will put in place the necessary framework and tools so that digital identity products enhance privacy, transparency, confidence and inclusion, and that users are able to control their data, in line with the principles published in the [2019 Call for Evidence response](https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response). We are also developing and piloting a new ‘One Login for Government’ system that will make it easier for everyone to access government services, with users only having to provide data to prove their identity once, and protecting privacy throughout.

BECOMES

Online authentication, identification and eligibility solutions can increase security, ease of use and accessibility to public services. They are central to transforming the delivery and efficiency of public services and people’s ability to operate confidently in an increasingly digital economy. It is estimated that widespread use of digital identification products would be worth around £800m per year to the UK economy. Widespread use of digital identification products could also help to reduce the record levels of abuse of personal data and impersonation to commit fraud in the UK, with over 220,000 cases reported in 2019.

The government is committed to realising the benefits of digital identification, without creating ID cards. Earlier this year we published a draft of the [UK digital identity and attributes trust framework](https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework). This document sets out what rules and standards are needed to protect people’s sensitive personal data when used digitally. We will put in place the necessary framework and tools so that digital identification products enhance privacy, transparency, confidence and inclusion, and that users are able to control their data, in line with the principles published in the [2019 Call for Evidence response](https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response). We are also developing and piloting a new ‘One Login for Government’ system that will make it easier for everyone to access government services, with users only having to provide data to prove who they are once, and protecting privacy throughout.

The switch, in Kantara’s opinion, does not change the meaning of the paragraphs but does change the focus from attributes being held to attributes being used.

1. The document makes no mention of allowing international participants to participate in the UK federation. Kantara recommends that international participation be allowed by organizations that are service providers or as perform eligibility or identity checks. These organizations will need to be certified as meeting the requirements established by the UK. The inclusion of international participants could increase competition in the Identification ecosphere.

## Responses to Individual Questions

1. Do you agree an existing regulator is best placed to house digital identity governance, or should a new body be created?

**Kantara Response**: Kantara suggests that, for the reasons stated, an existing Pan-Economy regulator should be used.

1. Which regulator do you think should house digital identity governance?

**Kantara Response**: Kantara, as it does not have intimate knowledge of the workings of the UK Government, cannot make a recommendation. As stated in the document, the chosen regulator needs to have the ability to perform the governing functions (i.e., monitoring) as well as setting the rules that need to followed.

1. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

**Kantara Response**: No additional functions required.

1. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

**Kantara Response**: Kantara does not oppose the governing body owning the trust framework. However, Kantara believes that certification that participating organizations comply with the commitments required by the trust framework should be an independent function.

1. Is there any other guidance that you propose could be incorporated into the trust framework?
2. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

**Kantara Response**: The approach identified in the document appears to be adequate.

1. Are there any other advisory groups that should be set up in addition to those suggested?
2. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

**Kantara Response**: The question of fees, as the document identifies, is delicate. The cost to an organization to use digital identification should not exceed the savings the organization will receive from using it. This approach will put the onus on the organization to understand how it will use digital identification and what savings it will realize from its use (i.e., will the organization realize savings over the use of document-based identification). The organization will also need to understand its customer base’s desire to use digital, rather than document-based, identification. Kantara suggests that the governing body provide a business-case template to help organizations make their decision. Kantara recommends that the fees an organization pays cover the cost of operating the service. However, the fees an organization pays should be seen as providing the organization with something tangible rather than just an annual subscription fee. For example, a fee to be certified and recertified on a periodic basis.

1. Do you agree with this two-layered approach to oversight where oversight is provided by the governing body and scheme owners?

**Kantara Response**: Yes.

1. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?

**Kantara Response**: Yes. However, Kantara recommends an independent Ombudsman role or other low-cost dispute resolution mechanism be specified in the Framework agreement to handle complaints not directly against the policies and rules of the governing body.

1. Do you think there needs to be additional redress routes for consumers using products under the trust framework?

**Kantara Response**: Yes. However, the additional redress routes should be available to organizations as well as consumers.

1. Do you see any challenges to this approach of signposting to existing redress pathways?

**Kantara Response**: No. However, memoranda of understanding will need to ensure that the identification needs of organizations and consumers are considered in existing redress pathways.

1. How should we enhance the ‘right to rectification’ for trust framework products and services?
2. Should the governing body be granted any of the following additional enforcement powers where there is non-compliance to trust framework requirements?
* Monetary fines
* Enforced compensation payments to affected consumers
* Restricting processing and/or provision of digital identity services
* Issue reprimand notices for minor offences with persistent reprimands requiring further investigation

**Kantara Response**: Yes. Kantara suggests that joining the service be in the form of a contract so that violations can be a matter of contract law enforcement.

1. Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?

**Kantara Response**: Kantara is a proponent of transparency.

1. What framework-level fraud and security management initiatives should be put in place?
2. How else can we encourage more inclusive digital identities?
3. What are the advantages and disadvantages with this exclusion report approach?

**Kantara Response**: While the document states that the production of the Exclusion Report should not create overhead for the organization, the mere fact of having to create a report, for many small to medium sized organizations, will create an overhead. As such, Kantara recommends that the requirement for producing an Exclusion Report be carefully considered.

1. What would you expect the exclusion report to include?
2. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

**Kantara Response**: Yes. As was identified in the response to Question 8, the cost of membership should include the cost of certification or recertification. It also needs to be measured against the savings an organization will realize from using digital identification.

1. Should a requirement to allow an alternative pathway for those who fail a digital check be set out in legislation or by the governing body in standards?

**Kantara Response**: Kantara recommends that it be set out in legislation as the path for non compliance to legislation is already well established.

1. Should disclosure be restricted to a “yes/no’’ answer or should we allow more detailed responses if appropriate?

**Kantara Response**: Kantara would recommend that more detailed responses be allowed to accommodate future, yet unknown, requirements to be accommodated.

1. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

**Kantara Response**: Yes.

1. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

**Kantara Response**: the number of confirmations performed by a government department would be lower. As is said in the document, the onus is on the user of the confirmation, based on their risk analysis, to determine the period of time they will allow a confirmation to be valid.

1. Would it be helpful to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

**Kantara Response**: While affirmation in legislation would be helpful, Kantara believes that strong and persistent communication of the equivalence would be more effective. It could also be effective for the government to underwrite the cost of misidentification when digital identification is used.