Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

DCMS, Cabinet Office
Digital Identity: Call for Evidence July 2019

This response has been prepared *The Investing and Saving Alliance* (TISA) whose mission is to improve the financial wellbeing of UK consumers by working collectively with the financial services industry. TISA is a rapidly growing body with over 200 members from across the financial services industry.

TISA is wholly supportive of the Government's ambitions to develop a digital identity system that can work for all sectors and which is available widely to all individuals and firms.

TISA looks forward to collaborating further with the Government to enable this to happen and will happily provide further support.

Questions on needs and problems

1. 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?

The strong support from members and stakeholders for TISA's Digital ID scheme provides clear evidence that it will meet the needs of both consumers and organisations..

2. 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?

Economic benefits – the Digital ID is a key / foundational component in the development of:

- The UK digital marketplace and the development of cross border trading post Brexit
- The growing Fintech marketplace
- Ongoing modernisation of UK service businesses that meet the evolving need of consumers
- A UK digital infrastructure that is owned by the UK
- Reduced business costs
- Reduced business risk

Social Benefits – the Digital ID will facilitate:

- The development of improved digital services for all areas of society – for example, TISA has a programme of work focused on vulnerable customers. The Digital ID can help vulnerable and thin file customers to access financial services.
- Improvement in the competitiveness of markets leading to benefits for consumers
- Consumers taking control / ownership of their Digital ID and the benefits in this brings in securing the monetary benefits of this ownership
- Improvements in digital security for consumers

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

No federated identity scheme exists for UK Financial Services. TISA is actively building its scheme with a range of participating firms including banks, insurance companies, pension providers and identity providers.

Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

The current KYC approach for Financial Services is fractured, time consuming, expensive and involves wasteful duplication as the consumer needs to undertake the KYC process each time they apply for a new product or service.

It is frustrating for the consumer, demonstrated by high abandon rates, from difficulties in meeting the Identity Verification process.

This in turn stifles competition with the financial services industry and consumers remain with their existing un-competitive product provider rather than switching to a more competitive and appropriate product.

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

TISA's Digital ID plans to make identity services inclusive, offering different identity validation and verification approaches to open up the scheme to all consumers, particularly vulnerable and thin file customers.

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

The issues pertinent to UK financial services include a current lack of:

- A shared approach for the collection and delivery of re-usable identities and attributes as well as digital access to authoritative sources to validate ID documents (such as the Document Checking Service)
- Acceptance of common standards and policies that underpin and govern a Digital ID scheme operation
- Clarity on the use of Digital ID in the current regulations with AML guidance being a blocker to adoption in the private sector
- A Trust Framework recognising the regulatory requirements for the particular sector and enabling different Financial Services to share Digital ID's and underlying attributes
- A Governance Body to drive adoption and delivery of a Digital ID Scheme for Financial Services and other sectors.
- Solutions tied together to deliver a strong identity system.

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

A federated Digital ID can enable:

- New product development tailored for customers based on their identity profiles
- Frictionless KYC processes that reduce the high abandonment rates in onboarding for new financial products.
- Remove the need to carry documents – driving licence, passport etc.
- Security against fraud - User attributes are held in secure locations, while relying parties know who's authorised to release these attributes.
- Integrated services across many sectors that the consumer interacts with. This could include use cases such as
    a. Incapacity to work following an injury (joining up health services, welfare and the employer);

Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

b. Applying for a mortgage, bank account and other financial products;
c. Changing address/change name by notifying the IDP once who will notify relying parties;
d. Prescription for medicine from the GP which is accessible by the pharmacist.
e. Eligible to claim benefits for a baby with the birth certificate accessible by welfare office.

Questions on criteria for trust

7. 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)?

The critical building blocks are:

- A Trust Framework providing the scheme rules, clear liability and commercial models and a legal framework to allow firms to operate in a trusted environment.
- A Governance Body to administer the Trust Framework and model standards to ensure Trust Schemes are compliant and interoperable. It allows firms to operate in a secure environment and deliver certainty in who each party can trust to deliver verified identity data to an agreed standard. Participating firms will have a single contract to operate in the scheme enabling multiple business relationships to be developed.

  The Governance Body would be responsible for undertaking eligibility checks and on-boarding new firms into the scheme, dealing with disputes between participants and serve the changing needs of the consumer. TISA is planning to set up a Governance Body to administer its Digital ID scheme and would work with bodies that are responsible for other schemes.

- An open and accessible environment for all firms and suppliers, subject to abiding to the scheme rules, policies and relevant regulations. Security is critical and must ensure that the validation and verification processes must be incredibly difficult to fake, but simple to use by consumers.
- Recognition of the Trust Scheme by the relevant regulatory body (such as the FCA) to engender trust and ensure regulatory compliance. Clarity on the provenance of Digital ID in the current AML guidelines is essential.
- Open technology and industry adoption of data standards, along with clear communications to consumers, on the benefits and security within the scheme, to build trust and encourage usage.

8. How does assurance and certification help build trust?

Digital ID certification ensures participating firms can operate in a secure environment and allows relying parties to know they can trust that an ID meets the requisite level of assurance and security.

From a consumer perspective, certified firms can display a Trust Mark to show that the firm is safe to interact with and share their Digital ID.

9. 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)?

Relying parties should only be presented with the data they need and only use it for the permitted purposes. For financial institutions, this means identity systems should be cyber-resilient and meet industry agreed standards for data protection and storage.

Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

TISA's Digital ID scheme has defined a range of principles, regarding consumer privacy including data minimisation and control. These will be detailed in the scheme's privacy policy and will be made available in a Consumer Charter.

The identity solutions in the scheme will operate to high technical standards that can improve the trustworthiness, security, privacy and convenience of identifying consumers in a wide variety of settings.

The technologies in the scheme will be certified, using an agreed framework, and will engender innovation to allow new technical approaches to verify and authenticate identities for financial services. This may include

- Biophysical biometric technology (including fingerprints; facial recognition)
- New approaches to authenticate consumer's identities (such as behavioural biometrics)
- Techniques for verification (such as high-resolution video transmission)
- Artificial intelligence to assess the validity of identity credentials.

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

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

TISA proposes an industry managed not-for profit body to manage its Digital ID scheme and has defined a range of roles and responsibilities, which it is happy to share with Government.

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

Cross sector scheme governance could be managed by a national competent authority (with representation from private and public sector organisations), an Executive Agency or a self-organising cross-industry body that oversees the standards and liability model (such as the Open Identity Exchange).

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

The private sector, the government, the Open Identity Exchange, the different regulators and standards bodies.

Questions on the role of the government

14. 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?

Government-provided evidence of core identifiers or attributes should be made available to enable identity verification and authentication. These should be standardised across all sectors to provide certainty in identity verification.

The government benefits as the veracity of identities can be maintained through regular use of the identity by the private sector.

Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

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

A valid government issued document may be used to verify a consumer's identity and will enable the private sector digital identity market to grow. This could be used for a variety of use cases such as undertaking Customer Due Diligence, renting a property, applying for a mortgage and purchasing age restricted good and services.

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

The government should be responsible for the overarching governance of its data but could use external private sector organisations to broker data distribution. Citizen control and protection would be delivered by scheme rules and associated contracts/service level agreements.

iii) What should the cost model be?

The government could charge a fee for access to this data; however, it would need to be at a reasonable rate to ensure the market can thrive and smaller organisations are not priced out.

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

A variety of use cases would benefit from having government attributes including opening a pension using the National Insurance number; salary data for affordability for loans/mortgages and the right to work in the UK.

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

This could be managed by a new entity or as a Trading Fund (like the National Meteorological Service). Alternatively, this could be governed by a Certification agency that would vet and approve organisations that can use the government data and maintain the certification regime.

iii) What should the cost model be?

It is suggested that this is on a pay per use basis with pricing determined by the market. Volume discounts could be offered for guaranteed use by private sector forms; however, competition issues need to be thoroughly explored.

17. What's the role of legislation and statutory regulation to grow and enforce a secure, privacy-centric and trusted digital identity market?
Regulators can help participating firms to understand what identity data and processes can be trusted. It is recommended that there is clarity on Digital ID in future legislation, regulations and guidance to strengthen the overall compliance process. This should also enable more people to access the regulated financial sector and reinforce safeguards for all citizens including thin-file, vulnerable customers.

Dakota House, 25 Falcon Court,
Preston Farm Business Park,
Stockton-on-Tees. TS18 3TX

t: +44 (0)1642 666999
f: +44 (0)1642 666990
e: enquiries@tisa.uk.com
www.tisa.uk.com

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

Legislation needs to reflect the changing identity marketplace, be flexible to allow the sector to thrive and be technology neutral. As identity is referenced in different legislation (such as AML4/5, Secure Customer Authentication in PSD2 and eIDAS), it is recommended that legislators ensure legislation pertaining to identity, is consistent. AML5 needs to clarify permitted use of digital identity by regulated financial services.

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

- Support through providing a framework to allow Digital ID to be used across different sectors
- Access to the components of Gov.UK Verify scheme (such as sharing its scheme rules, policies and operations manual)
- Open up access to eIDAS for commercial organisations to use the framework across Europe
- Provide funding (in the form of grants, loans) to support industry development.

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

Question on the role of the private sector

21. What is the private sector's role in helping to create a trust model (based on the criteria for trust in section 5), and how should they remain involved in its long-term sustainability (for example funding, helping create the rules of the road)?

The private sector has an active role in creating a Trust Model to be utilised across sectors, including public and private sectors. TISA wishes to avoid disparate initiatives from evolving and is very open to collaborating to ensure interoperability. A body like the Open Identity Exchange could help to ensure standardisation (where possible) and interoperability across different sectors.

Private sector organisations already operate in an environment that requires identity verification and authentication; however, this does not currently extend to reusable Digital Identities. TISA is developing a scheme that will enable this and is actively working with the government, the FCA and FATF.

The TISA project is developing a detailed Trust Framework, which includes the proposed liability model, commercial model and key policies and practices that will ensure it is sustainable in an evolving market. TISA seeks to work more closely with the government to align these rules, policies and practices between the two schemes.

On Funding, it is unclear if this is the government looking for funding from the private sector. If so, why would the private sector pay for something that will be operated by the government. If the government is to fund a Digital Identity Unit to take this initiative forwards, this could be a public/private sector partnership.