Policy area: Personal Data and Identity Management for citizen interaction with the digital economy

Relevant Government Department: Cabinet Office and DCMS lead and relevant to all Government Departments, Local Government and devolved administrations

Minister/Shadow Minister: Secretary of State at the Cabinet Office

1. **Background** – explain the context of the topic in straight forward terms. What is the problem and why does it exist?

The Government is seeking to move to “digital by default” for delivering Government services. The desire is to simplify and provide the public with a one stop shop for Government services. Digital is the direction that all service delivery is moving in the both the private and public sectors. Many members of the British public have shown themselves happy to engage online (Britain has a larger percentage of online commerce than any other country (ONS) and some Government services, such as annual vehicle registration renewal are already predominantly done on line (DVLA)). Digital services are significantly cheaper than physical correspondence, phone or face to face services. This is a major element of the Government efficiency and cost reduction programme. In order for digital service provision to become universal, the management of identity attributes and personal data must be secure and trusted by the public. The Government is seeking to achieve effective identity management to access digital services, including payments, through a service co-ordinated by the Cabinet Office called Gov.UK Verify, which is currently in beta test.

The British public are sceptical about the privacy and security aspects of Government Identity Schemes. The UK does not have an identity card system in place (as almost all other European Countries do). The attempt to produce an identity card, based on the creation of an identity data base for the whole population was abandoned by the incoming Coalition Government in 2010 under public pressure to do so. The BCS agreed with this decision and that the current approach was the best one.

The UK is required under EU legislation to have an identity assurance scheme in place by 2016 to facilitate cross border trade. Gov.UK Verify is intended to provide such a scheme by enabling private sector identity providers (IDPs) to assure the identity of all UK citizens by cross referencing a variety of private sector data bases (such as those held by Credit Reference Agencies) with a variety of Government databases (such as the Passport and Driving License systems) through a secure hub for one time verification, without holding a large national identity data base. The BCS supports this concept (which is the same concept as is being introduced in the USA). However, for operational implementation, the “devil is in the detail”. Progress over the last five years has been slow, as many problems have arisen and many have been overcome. A consequence of the slow progress has been that many potential IDPs in the private sector have baulked at the costs and liabilities involved.

Gov.UK Verify is the only possible route to a Government backed identity scheme by 2016. However, there are many issues that still require resolution for the scheme to “take off” in Government, and also become the default identity assurance scheme for use in online commerce. The use of the scheme outside access to Government services is necessary
because that is the route for private sector providers to recover their costs of becoming Government approved IDPs.

2. **Factual evidence** – provide facts/figures to demonstrate. Ensure sources are correctly referenced

See sections above and below.

3. **Key issues** – why does government need to address it? What are the consequences and the impact?

Modern society depends on electronic information to function. Citizens and consumers assume information held by Government and other organisations will be secure, the privacy of their personal data will be maintained, and the systems they access will be both available and usable.

**Security, identity theft and crime** - Any ability of organised crime or others to commit mass identity theft, misuse identity or defraud Government services will have a massive impact. The security placed on different data bases and elements in the overall systems of storage and access are not standardised (and are unlikely ever to be standardised). This makes guaranteeing security extremely complex (see Mobile access). Pressure to cut costs could lead to the ineffective initial registration of identities and weak credentials for future verification, that could be cloned and misused (identity assertion at different levels of security are required in the IDP scheme depending on the service to be accessed, e.g. renewal of a driving license or payment to the citizen of a high value on-going benefit).

**Trust and Privacy** – A lot of people feel insecure online. Their privacy is threatened online by everyone including: Government; marketing companies; organisations offering “free” services in exchange for personal data; organised crime. Identity theft is a growing problem as criminals and advertisers follow the money online. Privacy, and the ability to be anonymous in some situations, are becoming much more important to regular users of the Internet. The Cabinet Office has appointed a Privacy and Consumer Advisory Group (PCAG) (on which BCS has a representative) to look at the privacy aspects of Gov.UK Verify. The Group has produced a set of Principles for the scheme available at: [https://www.gov.uk/government/consultations/draft-identity-assurance-principles](https://www.gov.uk/government/consultations/draft-identity-assurance-principles). It is essential for long term trust in the scheme that these principles are incorporated into the contracts of all IDPs and audited for compliance. There also needs to be an adjudicator appointed, who the public can appeal to and get redress through if things go wrong and their personal data is not protected or they are defrauded.

**Usability** – One of the major problems revealed in both the alpha and beta tests of the Gov.UK Verify scheme is the time and effort required to register with an IDP. Many people do not possess the required matching information in the data sets being used. There are a variety of reasons for this, such as: not being in possession of a passport or driving license; married women having data in some data bases used for cross referencing in their maiden names and others in their married names (this also applies to all other people choosing to use more than one name, such as actors); having no credit reference status; having a bank account opened prior to 2007 (when the ICO ruled that banks could not share data with credit reference agencies without express permission from individuals, and to default to “no permission granted” on existing accounts); or people moving house between data being collected for the different data bases being cross-referenced. In addition, many users of the beta tests gave up because of the time involved and the need to have all the complex data
required to hand at registration. Constant requirements to correct data and re-register on multiple services wastes money and frustrates users.

**Economic impact** - The UK needs simple, secure and compatible identity management systems, trusted across organisational boundaries, if Government is to achieve serious savings in the cost of delivering public services. These same systems are needed for all national and global e-commerce.

**Mobile access** – There is a fast growing trend for people to access services on mobile devices. This is going to be hard for initial registration (see usability). In addition, if services are accessed on mobile devices post registration, it is likely that apps will be developed to help them. The security of Mobile Access to Services (MAS) is very complex as there are many parties involved: phone companies, Internet Service Providers, App suppliers, Credit Card companies, etc. Each have their own secure elements (or not) and these are not standardised (see Security). The chain of responsibility and liability for personal data and systems failures when using MAS is totally unclear (see Figure below and Privacy and Trust and Governance).

**Communicating a complex system to the public** – There needs to be a professional communications campaign to the public to persuade them that it is worth registering with an IDP for the longer term advantage of not having to re-register for other Government services, and the ability to use their asserted identity for non-Government services (the one-stop shop element). Given the time and effort involved for an individual to register (often at first registration for a services they only expect to access infrequently) the critical mass needed for a robust and useful ID eco-system to evolve that is used by all members of the public is unlikely to be achieved without an economic incentive. Such an incentive could be a small discount awarded for the services used (such as payment for vehicle registration renewal) that reflects a percentage of the reduced costs of those services when they are digital.

**Initial registration and data accuracy at the outset and over time** - Registration reference data are stored in fragmented bespoke systems, with limited on-going maintenance, resulting in attributes such as "address" becoming increasingly inaccurate over time. In addition, human error and deliberate attack result in information being lost,
stolen, corrupted or abused. Rules for the protection and use of information are proving hard to enforce due to poor identity management, including by those with access to the systems. 

**Governance structures** – Gov.UK Verify needs robust common governance structures, for the secure sharing and exchange of identity between Central Government systems, Local Government systems, devolved administrations, IDP systems and other related systems including those of all EU countries (as required in the EU legislation) and globally if the UK identity scheme is to be usable for all e-commerce. Such governance systems have not yet been devised or put in place.

4. **EU aspects** – is the issue national or EU level? Is there a relevant comparison with other EU countries? How does being in or out of the EU affect this?

The timing for the implementation of Gov.UK Verify in the UK is dictated by EU legislation. However, the UK scheme is significantly different to all other EU national schemes and there are likely to be significant problems over cross border use of the UK scheme in the rest of the EU and vice versa (see Key issues - Security and Governance). These issues have yet to be addressed.

5. **Local/ devolved government aspect** – what are the considerations for local government and devolved administrations?

Local Government and devolved administrations are all expected and expecting to use Gov.UK Verify (see Key issues - Security and Governance)

6. **BCS advice (including EU/local recommendation)** – what do BCS want government to do?

The UK is lagging internationally on identity management for the digital economy. Electronic identity within the UK is fragmented and immature, with inadequate understanding of shared information-centric risks. Organisations such as Facebook, Google and Microsoft are building commercially based identity systems, but these have serious privacy issues. The public sector lags behind, but industry is unwilling to invest in public sector systems due to a lack of clarity of objectives and lack of a working commercial model for Gov.UK Verify. Both the public sector and citizens need to know that only authorised individuals have access to their information in data bases and that it is accurate and protected against fraud. Such fraud is said (by the National Fraud Authority) to cost the UK £30bn/year, over half of this is fraud against Government. This adds to an international perception that the UK is not a leader in the protection of sensitive information – which also has wider economic impacts.

Controlling who can access what information across organisational boundaries requires identity management based on common policies and collaborative identity governance within and across three main user domains – public sector, private sector and citizen. Together, they should focus on common trust policies, procedures and mechanisms for sharing electronic information to answer four key questions:

1. Can you prove that you are who you claim to be beyond reasonable doubt? Registration & Authentication
2. Do you or your organisation have permission to access information, entitlements or services? Authorisation
3. Can every action be traced to the individual or organisation and can they be held accountable for unauthorised actions? Accountability & Audit
4. Is there an independent arbiter to resolve issues of redress? Governance

The basis of any Identity management system is the initial registration. If this can be conducted less often and to higher standards, for re-use by other verification systems,
significant savings can be made by removing duplication, security can be increased and fraud reduced. The credentials issued can then be used for authentication by a variety of organisations, including after checking with the issuer that they are still valid when higher assurance is needed. This is similar in concept to an online passport. Credit cards also operate this way as do the consumer credit industry and the trust services based on the Laws of Contract that underpin global trade.

Everyone cares about their identity and privacy even if some users of social media may not realise this initially. This is an issue that requires Government led communication and education.

The UK Government needs to work with industry to develop and implement standards based identity management frameworks that provide usable trust models, possibly based on the banking liability models. When public sector organisations believe they can trust identities registered by others, they no longer feel compelled to re-register those with whom they deal. This could potentially save billions in duplicated cost and fraud reduction.

However, if systems such as Gov.UK Verify do not instil a sense of trust or are even openly compromised it could have devastating results as the public moves back to paper forms.
Suggested topics to cover

**Digital Skills/Future of the Workforce** - implication of creative disruption (eg autonomous vehicles, IoT, wearables) innovation & growth  
**Authors:** Adam Thilthorpe, Tom Crick (liaise with Paul Martynenko, Paul Excell)  
**Target:** BIS, DCMS, DfE  
**Ministers and Shadows:**

**Personal Data** - ID assurance and citizen interaction in the digital economy (including with government digital services)  
**Authors:** Louise Bennett, Phillip Webb  
**Target:** DCMS, Cabinet Office  
**Ministers and Shadows:**

**Communications & Infrastructure** – Broadband and mobile coverage, scope for doing business outside of urban clusters  
**Authors:** Roger Marshall, Selwyn Castleden  
**Target:** DCMS, BIS, Communities & Local Govt  
**MPs and Shadows:**

**Health** – Reducing inequalities through personalised healthcare, informaticians on a level with clinicians (handling data), protecting the public on use of information, integration of health and social care.  
**Authors:** Tom Denwood, BCS Health  
**Target:** DoH  
**Ministers and Shadows:**

**Online Government Services & Citizen Interaction** – eGovernment, ‘digital by default’ and digital inclusion/skills  
**Authors:** Yvonne Gallagher? Lesley Cowley?  
**Target:** Cabinet Office  
**Ministers and Shadows:**