Digital Identity, Verification and the UK Trust Framework

Richard Johnstone – February 2021

Digital Identity

Your identity is what you are. When you meet someone, you typically give your name. On more formal meetings you may show a business card, a driving licence or a passport. Your doctor may display a professional certificate on his/her wall. On occasions you may need to present copies of a recent bank statement or utility bill. These documents show **attributes** of a person's identity in face-to-face environments.

In today's world with widespread use of computers, smartphones and the internet, we increasingly communicate remotely. When you want to identify yourself, and prove your identity, you must communicate digitally. If you buy something over the internet you will need to provide your name, delivery address, e-mail address, and payment card details. These attributes form part of your **digital identity**. For different tasks and transactions different sets of attributes are required, depending on the level of authentication needed.

Many of the attributes need to be presented repeatedly for multiple transactions. This data can be stored and presented when needed, which makes transactions easier for the user.

This digital data is currently stored and maintained in multiple databases, which results in inconsistencies and extra work for all parties. As a result there are moves to pool some of this data where it can be maintained and verified securely, and used for most transactions and by multiple organisations.

Identity Verification

Identity verification means proving that you are who you claim to be. For physical identity verification this often means showing a photo-ID card, or signing your name. At a POS or ATM terminal a PIN may be entered. For an online transaction often a sign-on or login process is required, typically requiring a password or a random number returned to the user's smartphone.

Criminals are keen to misuse your data (identity theft) for their own ends. They also create fictitious digital identities. For more security you will need to **authenticate** your identity, for example online banking and online government services, where a sign-in process with authentication data is needed – passwords, date of birth, answers to agreed questions or biometric data via a smartphone.

UK Digital Identity and Attributes Trust Framework

Countries around the world are now in the process of setting up national Digital Identity systems in light of the growing need for easier, more efficient and safer use of digital identities. In the UK the government has recently (2019-2021) consulted with public, private & consumer organisations on the establishment of a UK digital identity framework that would enable individual users, government departments and private organisations to have secure access to proven digital identity attributes.

A first draft was circulated in February 2021*. The responses to the consultation and the first draft have been largely positive. A similar approach is being followed in Canada, Australia, Sweden and New Zealand. The approach does **not** require a national identity card.

The trust framework will provide a set of rules and standards that all connected organisations must follow. The organisations in the framework may be from the public or private sector. International standards and practices will be followed in order to maximise future international interoperability. Individual users must be confident that their digital identity data will be handled securely, providing privacy protection for all. For individual users, establishing a digital identity will be **voluntary**. Users will also be in control of which attributes are provided, to whom and when.

The framework will be owned and run by a governing body, established by the government, which will ensure that all connected organisations are accredited and follow the rules. Where necessary the government will remove any legislative blockers to the use of the framework.

Users may decide to use their identity attributes to purchase a product online, apply for a job, open a bank account, buy a house, obtain a visa, rent a car or apply for a loan.

Organisations may be individual Government Departments, Public Organisations, Banks, Retailers, Airlines, or sector-based groups or schemes. They may join as Identity Service Providers, Attribute Service Providers or "Relying Parties" who source products or services from other participants in the framework. Organisations can join by themselves, or as a member of a "scheme". The scheme's rules will need to meet the requirements of the trust network.

The government seems to have learned lessons from the previous (failed) digital identity scheme – "Verify", which was viewed as too prescriptive and centralised. The current proposal is for a user-centric, open, decentralised and universal framework with safeguards for user rights and privacy.
The current government systems – Verify, Government Gateway (HMRC), ConfirmYourIdentity (DWP/Universal Credit) and Login (NHS) will be migrated to a single sign-on and identity assurance system.

In terms of the implementation of this framework, public-facing government departments look likely to lead the way. They are being pressed to migrate from their current systems to the new UK trust framework. These departments are also the depositories for most of our digital identity information – birth certificates, passports, driving licences, addresses, electoral roll data, tax information etc.

Although the early signs are encouraging, much further work is needed to fill in the details and, as we know, the devil is often in the detail.

Richard Johnstone – February 2021

---

* "The UK Digital Identity and Attributes Trust Framework" – a Government Policy Paper published on 11 February 2021 by the Department for Digital, Culture, Media & Sport