The case for Government-managed Digital Identities

Frederic Trojani, Chairman of the Board from the Secure Identity Alliance analyses today's proliferating digital identities market, and argues that only governments can deliver the trusted environment that enable digital identities and digital economies to thrive.

Today there are millions of bytes of data being collected, by thousands of organisations, about billions people. In fact, anyone engaging with private firms and governments online, or making any form of virtual transaction is being tracked, analysed and targeted.

Depending on your point of view, it's not necessarily a bad thing. Often, it can be very good indeed. For most, sharing personal information in exchange for online services they regard as valuable is a natural extension of their physical lives; from a social network to an e-commerce portal or a branded website. As more data is shared, a more detailed picture of the individual emerges. And the digital identity is born.

Digital identities create wealth

Leveraging these digital identities offers huge opportunity; for individuals, commercial organisations and governments. Towards the end of 2012, the Boston Consulting Group (BCG) added some numbers to the rhetoric. The value created through digital identity, it said, could deliver annual economic benefits for organisations across Europe of €330 billion by 2020, growing to €670 billion for consumers.

For governments a digital identity gives citizens access to a host of new eGovernment services. Individuals can pay their taxes online, monitor their health, apply for state social security payments, register births and more besides.

Governments can save billions of dollars in provisioning and administering these services.

Added to this, governments benefit from an injection of wealth as commercial organisations build new services, which consumers buy, and digital economies are created.

Starts with trust

The success of any digital economy is inexorably tied to the success of managing and leveraging the digital identities of today's connected citizens. But there are challenges.

At the most fundamental level, digital identities are not built on the millions of bytes of user data currently being extracted, analysed and used by public and private organisations. They are built on trust.

This may seem like a semantic discussion because identities in the digital world are, of course, data-driven. But it's not. Without the underlying principle of trust users won't willingly expose the data needed to create these identities, and initiatives and economies will fail.

The next point is convenience. Locking away an identity behind multiple authentication systems may very well offer the kind of information security that will instantly guarantee trust. But if users aren't able to easily use these digital IDs to gain fast access to, for example, an online gaming portal, or an e-commerce site, a banking application or an eGoverment service then they'll rapidly become redundant.

Then there's security. Where are identities stored? How easily can they be compromised? Who has access? What level of personal data exposure is likely in any one system? Can snippets of data be pieced together and used for malicious purposes? The security issues are immense.

Protection is needed

Protecting personal data is therefore critical. An environment where digital identities are protected and instantly accessible must be created. I'd strongly argue that the responsibility, and the opportunity, lies with governments.

It is also logical. Today governments are managing identities in the real world; from birth, marriage and death certificates, through passports to driving licenses. It therefore makes perfect sense that they play a key role in managing citizen identities in the digital world.

Not only that. Governments are answerable to citizens in a way that commercial organizations are not. They are, or at least should be, altruistic organisations run for the good of the populace, and more trusted because of it.

Creating secure digital identities

It's important, right up front, to deal with the ownership issue. While governments may manage and secure digital identities, they do not own them. That is the preserve of the individual, and the individual alone.

Conventional methods of accessing online services have tended to revolve around user name and password systems. These have been proven to be ineffective against increasingly sophisticated attacks.

In February 2013 over a quarter of a million Twitter users had their accounts hacked, potentially exposing usernames, email addresses and password. More recently online note-taking service, Evernote, issued an advisory informing its 50 million users of a security breach that saw hackers steal usernames, associated email addresses and encrypted passwords. These are not isolated incidents, and now we're seeing threats migrate to smartphone, through app-borne malware, mobile payments fraud and more.

Privacy best practices in terms of service design should therefore deliver digital certificates that include just a snapshot of the identity of the individual, rather all the user's information.

For example, an eGovernment services platform with an over 18 year old policy could authenticate a citizen using a digital certificate that exposes none of their personal data whatsoever. The certificate would come from a trusted source and simply confirm the user is indeed over 18, and a citizen of the country. No other personal information would be shared, and access would be granted.

Technology and policy

Creating that protected environment, where trust, security and convenience are delivered has as much to do with policies and principles as it does with technology. But there's no doubt it's a complex task.

Citizens are already well used to interacting with government through online eGovernment portals and self-service kiosks. Also, as we have seen in the Nordic countries and in the Middle East, channel preferences rapidly shift from PCs and laptops to smartphones and tablets as government websites become easier to use on the move.

The result will be more and more new government applications targeting mobile platforms. Many of these applications will be supported by secure technologies and authentication services.

There are multiple options for storing identity credentials in mobile devices. One such way is through the embedded Secure Element in the device within the Universal Integrated Circuit Card (UICC) or Subscriber Identity Module (SIM) card, or within an external MicroSD card. A UICC can readily be transferred from one device to another.

Other options include a combination of the UICC, which provides a tamper-proof container for credentials, with a standardized trusted execution environment in the mobile device, enabling credentials to be securely used with multiple apps.

But there are more.

Establishing secure partnerships

Helping to address all these issues, the Secure Identity Alliance has been created to offer leadership and advisory services to governments, agencies and other public bodies.

Formed by four of the leading eDocument providers in the world (Gemalto, Morpho (Safran), Oberthur Technologies, and 3M) and opened to other members, the not for profit Alliance uniquely delivers support throughput the digital lifecycle; from enrolment, personalization, application & verification, through OS development to secure printing capabilities and security certifications.

In essence, the Secure Identity Alliance offers a trusted partner for governments when defining their eDocument strategies and implementing associated eGovernment services.

Ultimately, whoever governments partner with, the creation and management of digital identities is not an opportunity they can, or should, ignore. Only governments can provide the level of oversight needed to protect identities. And only governments are in a position to provide that trusted environment where digital identities, and digital economies, can thrive.

Meet the Secure Identity Alliance at Security Document World 2013 on 23 May 2013:

First Secure Identity Alliance Members Information (Recruitment) Meeting at Security Document World 2013 in London on 23rd May from 12:40 to 13:40 - main Conference Room. (Buffet Lunch served)

To register, go to www.secureidentityalliance.org or send an email to info@secureidentityalliance.org