Whether we’re logging into eServices to perform healthcare claims, to vote or sign a digital transaction, pay taxes, book or buy goods or services, our digital identity will become ever more significant in the years to come. This is especially true when it comes to accessing a vast range of public and government services.

Indeed, a major new study from the Secure Identity Alliance (SIA) reveals that the two – eServices rollout and a trusted digital identity – are intrinsically linked. It is impossible for the former to be successful without the development of the latter.

However the creation of a trusted framework to underpin identity is no small task, bringing together governance, standards, business processes, technical capabilities and more. But, according to the Secure Identity Alliance’ survey, it’s a task that would allow governments around the world are to realize some $50bn annual savings through effective eServices provision by 2020.

And while we’ll see multiple identity providers emerging in the coming years, the root identity – the one trusted digital identity upon which all are based – must start with Government.

Mobile devices, social media and other technology innovations are changing citizens’ way of life, and governments need to raise their game to deliver cutting-edge e-services that match the consumer expectations. But the shift to digital services stands and falls on whether governments can deliver trusted transactional eServices and manage the digital identity lifecycle.

In response to growing citizen demand for convenient and modern public eServices, today’s governments need to unlock a better and more harmonised service delivery that also generates significant savings for
the public purse. Fast-tracking this risk-free shift to digital service provision is dependent on public bodies addressing core issues such as data security, citizen privacy, identity and authentication.

It also depends on the emergence of a context sensitive and fully interoperable ecosystem in which citizens can use their trusted digital identity to securely access both public and private services.

**Imagining the World in 2020**

In 2020 trusted digital identity will become a ubiquitous part of our everyday lives. We’ll use it every time we engage with our national governments – when we apply for benefits or pay our taxes. And when we vote online in national or municipal elections, our trusted digital identity will give us the permissions to do so. These eServices have the potential to return around $80bn according to research conducted by Secure Identity Alliance in association with the Boston Consulting Group (BCG).

We’ll see our trusted digital identity become a key enabler of everyday life. Using a secure digital mailbox we’ll be able to communicate with government bodies, view and edit tax returns and submit clarifying questions to tax inspectors. We’ll even be able to use our identity to participate into a secure video chat with our doctor, or to collect a medical prescription.

Not only that, we’ll also use our digital identity or a derivation of this root identity in a host of time-saving lifestyle applications. Everything from accessing tailored promotions and special offers at the point of purchase, to signing digital contracts online. We’ll even be able to use our mobile devices to unlock a rental car booked in our name or drive a shared car pool vehicle. These new services will drive wealth creation across economies as well as seeing new identity providers emerge to push the boundaries of what is possible today.

Ultimately, our trusted identities will give us access to an exciting world of new on-line experiences, and provide the foundation for an explosion in the development and adoption of next-generation government eServices.

There’s already a pent-up demand and appetite for both public and private eServices, fuelled by today’s digitally confident citizens who expect services to be available across all channels, the instant they need them. From simple identification processes like the electronic submission of photos to renew a driving license or passport to registering the birth of a child, there’s a growing public willingness to replace in-person procedures with online engagement and to give – or receive – information electronically.
That’s good news for governments looking to consolidate and migrate information delivery and transactions online, enabling self-service for citizens. While eGovernment services are projected to deliver significant financial returns in 2020, the opportunities for increasing convenience, trust and citizen satisfaction and stimulating the wider digital economy are just as significant.

For citizens the benefits include 24/7 service access, from anywhere, eradicating the cost and time involved in travelling or waiting in line to undertake in-person transactions. Alongside this, citizens gain faster and more transparent processing, improved transactional security and access to innovative new service delivery models. ehealth services, walk-in health clinics and personalised medicine are all perceived as key pay offs.

The wider benefits of the trusted digital identity framework as a key enabler of the wider digital economy should not be underestimated. As providers of essential online services to the whole population, governments can take the lead in promoting high value trust-based economic and social interactions online, establishing a clear national policy strategy for digital identity management that benefits all and enables the creation of innovative online public and private services. And by acting as the national validation gateway for ID service providers, governments can help accelerate the wider digital economy.

From Vision to Reality

From a citizen/consumer acceptance perspective, the take up of digital identity applications is heavily dependent on trust. How digital identity develops is an important concern; but if privacy controls and benefits are calibrated appropriately, people will be ready and willing to share personal data. So what does it take to turn the eGovernment – and wider digital economy – vision into a reality? The first step is to understand and follow the four guiding principles that underpin digital identity value creation, and then apply these to technology solutions:
Guiding principles for digital identity value creation ...

- **Privacy**
  - Provide options for control regarding data sharing

- **Transparency**
  - Take accountability for a trusted flow of data

- **Responsibility**
  - Increase data security in order to safeguard digital identity
  - Communicate benefits and engage users for sustainable data usage

- **Benefits**

February 6, 2014  •  S2A eGov: Study Feb 10 2013.pptx
Source: S2A Liberty Global and BCD 'The Value of Our Digital Identity' (2012)

benefits of any secure identification solution needs to be communicated clearly to users in order to assure sustainable data usage.

Until now the authentication of identity has proved a major bottleneck to the widespread realisation of trusted digital identity. But a number of high profile eGovernment implementations across the world means that growing numbers of citizens are now able to create an online government account, populating their profile with preferences and consents. Providing the ideal conditions for governments to initiate better harmonised service delivery across all agencies – and unlock the full value of digital identity in a sustainable, citizen-centric way.

But if citizens are to benefit comprehensively from a trusted digital identity that can be used to securely access public and private services, then a fully interoperable ecosystem needs to evolve to support secure and transparent data exchange between all parties – citizens, public and private sectors.

- **protecting citizens/consumers** - building in ‘privacy by design’ to give citizens/consumers privacy controls and options that including the ability to change access rights.

- **transparency** - organisations must be fully accountable for a trusted flow of data, adhering to clearly defined codes on how they work with and use personal data

- **responsibility** - organisations are responsible for safeguarding data relating to digital identity

- **communication** - the
Enabling this will require a trust framework that encompasses ID technology, authentication, application and interoperability alongside accountability, privacy and transparency and ID supply. All of which will be essential to generating citizen trust and a positive perception of the benefit/risk ratio to assure take-up. Many of these elements are already in place. Today’s card-reader based solutions are evolving towards smartcard-based secure electronic ID verification, and smartphones can now deliver electronic ID via standard contactless interfaces such as NFC (near field communications) and Bluetooth.

Meanwhile authentication technologies already support multi factor authentication processes such as PINS, usernames, passwords and/or OTA tokens – and biometrics will deliver a further authentication layer.

As we evolve towards the 2020 vision, context aware authentication will be required to determine the identification method(s) most appropriate to the user case in hand; for example multi-factor authentication involving biometrics can be added if required.
The question of where these identities are stored is crucial for obvious security reasons and tamper resistance. The form factor of the electronic identity may vary but shall be stored or accessible using a secure element such as a smart card, a mobile UICC (SIM card), an embedded secure element in the mobile, or a microSD card for example. eDocuments are able to authenticate the user based on access to appropriate levels of the root identity – offering only enough information to authenticate the transaction without revealing the details on which that identity is built. In this way privacy is served, and a greater level of user trust assured.
From a technical standpoint the trust framework will require policies and standards that establish what user information is accessible which entity provide it and gives citizens a degree of control over what data they make available and the option of surrendering additional data for non-core services. It will also require an infrastructure that facilitates and enables trust and confidence between all members, and delivers streamlined identity and data verification based on summary digital credentials.

Ultimately, enabling the kinds of eService returns that are projected is dependent on establishing the accountability and responsibilities of all who operate within the digital economy as well as enabling full interoperability across the framework, in contrast to the limited scope of the services that operate today.
Bringing it all Together

The eGovernment experience is already proving its worth and a number of high profile implementations around the globe are showcasing what’s possible.

Since 2001 the United Arab Emirates (UAE) has been engaged in building a competitive and resilient economy and today is acknowledged as having one of the most advanced eGovernments in the world. The ultimate objective of Emirates’ eGovernment strategy is to provide innovative channels in a time and cost effective manner – through the Internet, fixed and mobile phones and kiosks alongside traditional service centres. Citizens reap the benefits of efficient connectedness in their digital lives while UAE businesses can network, transact and interact to share knowledge and innovation.

In South Korea, 90 per cent of all government interactions can now be performed online. As one of the most comprehensive, mature and high performance eGovernment programmes in Asia, if not the world, Korea’s strategy integrates and coordinates responsive, efficient customer services, governance and policy making. Customised services for individuals and corporates, available via the Internet and mobile devices, have successfully eliminated 70 percent of all document requests.

Meanwhile, the tiny state of Estonia – one of Europe’s smallest countries – has become an eGovernment role model with over 400 government services now fully integrated online. Full transparency has seen widespread positive acceptance of the eGovernment agenda by citizens. State issued ID smart cards unlock all the government’s eServices and allow Estonians to send and receive encrypted emails. In Estonia you can register your tax, vote in national elections, access e-health records or school reports – and even register your newborn child – online.

It is possible to find examples of these best practices right across the world. Each is extremely valuable, adding to the weight of knowledge that will ultimately define the shape and success of eGovernment services as we move forward.
Indeed, sharing these best practices is one of the key objectives of the Secure Identity Alliance. It’s why we have, for example, recently launched an initiative to track live government eServices projects across the world. Similarly, it’s the reason why we are working with public bodies across the world to develop a self-assessment tool that allows governments to benchmark and plan eID programs against proven best practices and real-world global deployments.

For more information download the full report at www.secureidentityalliance.org