Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity

A research report and position paper by the Secure Identity Alliance

March 2014

Table of Contents

1. Executive Summary

In response to growing citizen demand for convenient and modern public eServices, today's governments are looking to unlock a better and more harmonized approach to service delivery that generates significant savings for the public purse.

This paper identifies the cost-saving potential of smarter, better and faster eGovernment through a cost-benefit analysis jointly undertaken between the Secure Identity Alliance and the Boston Consulting Group – a potential global public administration saving of $50 billion per annum by 2020.

Cost and citizen experience drivers means governments around the world are pursuing an e-agenda that will enable the introduction of an open and relationship-based government model in which citizens can access and take advantage of a host of government services with both speed and convenience.

But our research indicates the 'top down' benefits of eGovernment extend well beyond the cost-effective delivery of convenient and 'joined up' public administration. High profile implementations around the world are demonstrating powerful knock-on effects for the wider digital economy – stimulating new business models and services that generate employment opportunities and pave the way for greater social inclusion.

One thing is clear. Whether citizens are logging into eServices to perform healthcare claims, to vote, pay taxes, book or buy goods or services, digital identity is set to become critical in years to come.

The findings of the eGovernment services study demonstrate the central role trusted digital identity will play in fast-tracking a risk-free shift to digital service provision. Despite the emergence of multiple identities from multiple providers, the root identity – the one trusted digital identity upon which all are based – will begin with Government.

The creation of a trusted framework to underpin identity is no small task that requires public bodies address the core issues of data security, citizen privacy, identity and authentication. But the benefits of the trusted digital identity framework as an enabler of the wider digital economy will also be dependent on the emergence of a context sensitive and fully interoperable environment in which citizens use their trusted digital identity to securely access both public and private services.

The Secure Identity Alliance is dedicated to supporting sustainable worldwide economic growth and prosperity by enabling government agencies around the world develop the trust frameworks – combining governance, standards, business processes and technical capabilities – necessary to support the successful introduction of eGovernment services.

This report evaluates the benefits eGovernment can deliver, assessing the opportunities for citizens and public bodies alike. The document also clarifies the critical elements that need to be in place to enable governments and public agencies realize the opportunities and address risk issues as they transition to digital service provision.

2. Introduction

Mobile devices, social media and other technology innovations are raising citizen expectations of customer service in a range of contexts – including interactions with government.

Around the globe governments and public bodies are looking to information and communication technologies to improve information and service delivery, encourage citizen participation in the decision-making process and make government more accountable, transparent and effective. These programs look to engage, enable and empower citizens through the provision of:

- eServices – the direct provision of online services to users (citizens, businesses, non-profit organizations) to improve quality, quantity and outreach
- eDemocracy – improving the participation of citizens and businesses in decision-making by facilitating access to information and enabling public discourse
- eAdministration –the exchange of information and knowledge within the public sector.

These eGovernment initiatives are being driven by a universal desire to evolve and transform government, creating a public sector that is:

- open, transparent and accountable to citizens
- user-centered, excludes no one and provides personalized services
- productive and delivers maximum value for taxpayers' money – less time wasted in queues, fewer errors, more time for professional advice and guidance
- transactional – supports 24x7 access to online services for paying taxes, applying for ID cards, birth certificates, passports, license renewals
- connected – enables inter-agency, central and local government connections and wider connectivity to other stakeholders (private sector, academic institutions, NGOs, civil society).

Ultimately, the end goal for government organizations is the achievement of a government 2020 vision in which trusted digital identity becomes a ubiquitous part of people's everyday lives. Enabling permissions that allow people to engage with their national government and apply for benefits, pay taxes, vote online, or register a birth or death.

But in time these trusted identities – or derivations of the root identity - could become the basis for a host of time-saving lifestyle applications that extend beyond government and into the wider economy. This would make it possible for people to transact widely; signing digital contracts, accessing tailored promotions and offers at the point of purchase, using permissions received via a mobile phone to unlock a rental car or access personalized eHealth services.

The case for eGovernment services

The Alliance plays a key role in sharing best practice and uncovering the new generation of eIdentity and eDocument technologies crucial to building the trusted framework on which to drive eGovernment, and global economic growth, forward.
To support the goals of governments striving to make their eGovernment 2020 vision a reality, the Secure Identity Alliance, in conjunction with the Boston Consulting Group, embarked on a research project to:

- evaluate the scope and scale of the potential gains of eGovernment enablement delivers
- benchmark the current state-of-play in terms of the technologies and frameworks currently in place
- define the guiding principles and evolutionary path for digital identity value creation
- characterize the components of a trust framework that will enable the broadest adoption of a trusted digital identity.

This report details the opportunities and challenges of this rapidly expanding marketplace. It is our hope that these insights and guidelines will act as a catalyst to making the eGovernment 2020 vision a reality.

3. eGovernment Value

The findings of the Secure Identity Alliance joint research undertaken with the Boston Consulting Group indicate that eGovernment services, enabled by trusted digital identity, are set to yield $50 billion annual global savings by 2020.

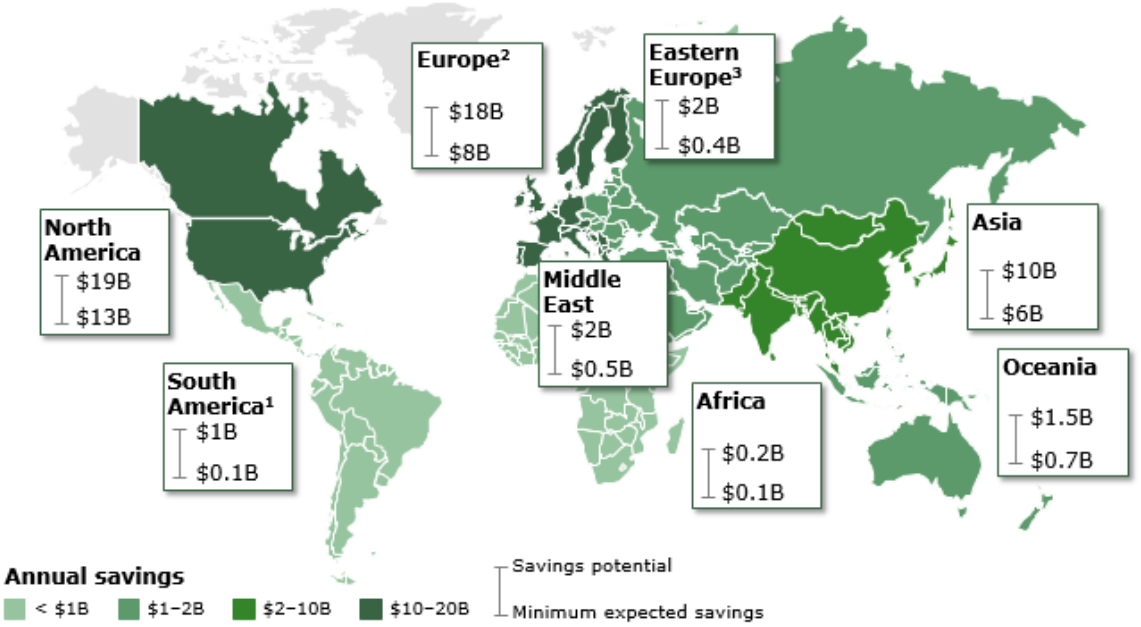
In quantifying the worldwide/regional administration cost-saving figures, a cost/volume benchmark of all global analog and digital interactions between government and citizens (excluding businesses) undertaken in 2011 was established on a country/region basis. Transaction data included in the modelling process included all interactions with government authorities (tax collection, advice, registrations etc).

For the purposes of the analysis model digital transactions were defined as internet, email, SMS and electronic transfers, while onsite visits and phone calls (including call centers and automated interactive systems) were designated as analog.

Using this data a projection model was created, utilizing country-by-country data alongside an analysis of reference countries digital transaction maturity and growth rates to establish a global/regional digitization growth curve to 2020; digitization figures per country were calculated using the eGov index and clustering method and include an 80 per cent cap to reflect the fact that some transactions cannot be digitized.

The differential in cost between digitized and analog transactions was next established and this figure was utilized to calculate the cost saving potential generated by the projected growth in digital transactional share; projections reveal the share of digital transactions is set to grow worldwide by 30 per cent by 2020.

Chart 1: eGovernment yields $30–50B annual savings by 2020—enabled by trusted digital identity



Research methodology

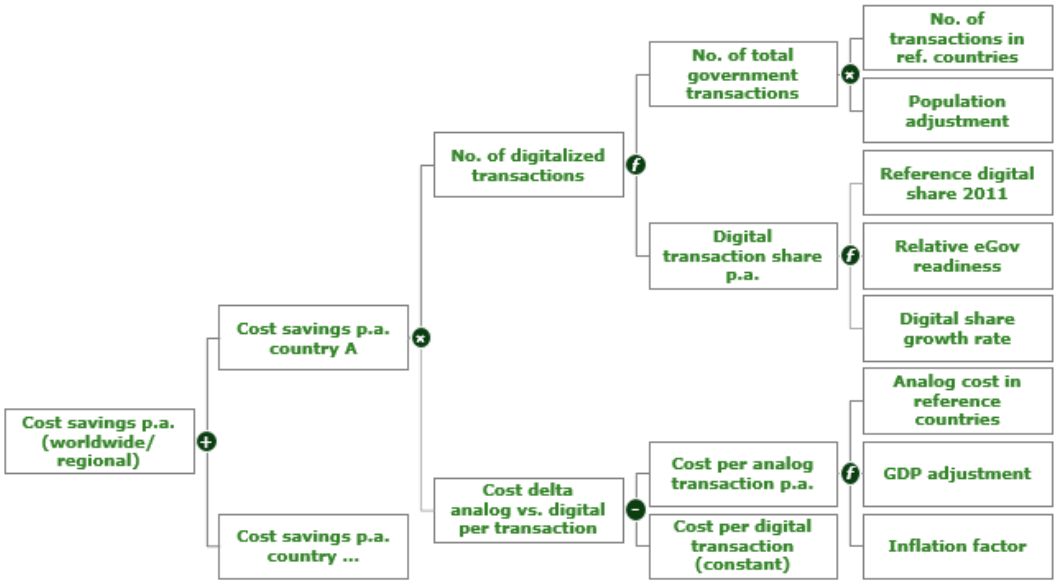
A global market model (Chart 2) was developed to quantify the potential administrative savings generated by eGovernment from on a worldwide basis. To achieve this, deep analysis was conducted to establish:

- the total number of government/citizen transactions in 2011 (baseline)
- digital transactional share in 2011 and the digital share growth rate curve to 2020
- comparison of cost per analog transaction (adjusted by country-specific GDP/inflation figures) versus digital transaction cost figures to establish a regional/global differential cost-saving number (between $2.80 and $3.50 per transaction)
- the relative eGovernment readiness of reference countries to identify an appropriate digital transaction growth projection to 2020
- an S-curve function to calculate digital transaction share growth to 2020, utilizing the UN eGovernment Readiness Index (see chart 2.1)

A complete breakdown of the criteria used to build this model is available at www.secureidentityalliance.org.

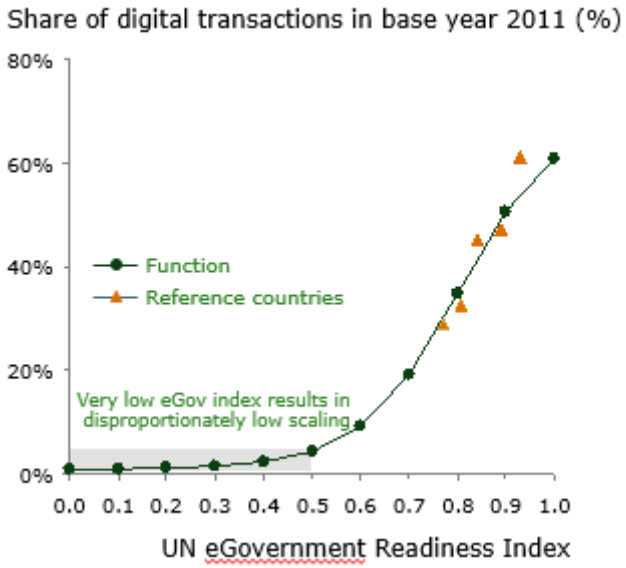
Total projected transaction volumes for 2020 were established by capping the number of transactions per capita before utilizing population scaling to determine country/region/global figures.

Chart 2: Market model developed to quantify the potential administrative savings due to eGov



Understanding the s-curve

Chart 2.1: S-curve function approximates the 2011 digitization share per country

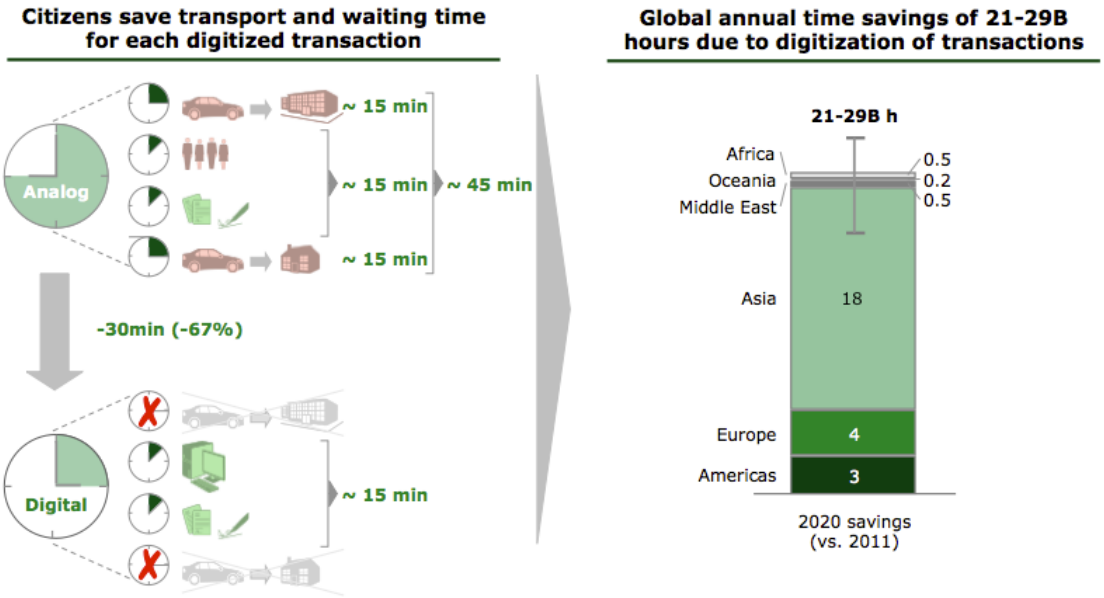


Utilizing the UN eGovernment "Readiness Index" to calculate the share of digital transactions, an S-curve scaling model has been used to present the growth in the number of digital transactions worldwide. This is based on data received from reference countries, and classifies transactions into analog and digital. Internet, e-mail, SMS, electronic transfers are categorized as "digital" with onsite visits and phone calls (call center or automated/interactive system) designated as "analog". This data was then used as part of the wider model we see in chart 2.

Constant digital cost vs. increasing analog cost

- Digital transaction costs, comprising of IT/engineer labor, were assumed equal for all countries and kept constant at $0.5-0.7 to 2020 to reflect inflation (energy/labor) is neutralized by hardware price decreases
- Analog processing costs, comprising primarily labor, were based on the projected 2011-2020 CAGR of individual reference country GDP

Chart 3: Estimated time savings worldwide through digitization



The model was also applied to quantify the time-saving potential generated by digital transactions for citizens by 2020. These calculations evaluated average transport and waiting times to establish an average time saving of 30 minutes per transaction. Utilizing the projected uplift in digitized transactions, this equated to a global annual time saving of 29 billion hours for citizens resulting from the digitization of transactions.

Benefits for citizens

Access to 24/7 services from anywhere eradicates the cost and time burden involved in travelling or waiting in line to make in-person transactions. The time-saving benefits for citizens alone are significant; our model indicates a 65 per cent time reduction per digitized transaction.

Alongside time and cost saving advantages, citizens will also gain faster and more transparent processing, improved transactional security and the opportunity to tap into innovative new service delivery models that include eHealth services, walk-in clinics and personalized medicine.

Benefits for governments

While eGovernment services are projected to deliver significant financial returns by 2020, the opportunities for increasing convenience, trust and citizen satisfaction and stimulating the wider digital economy are just as significant.

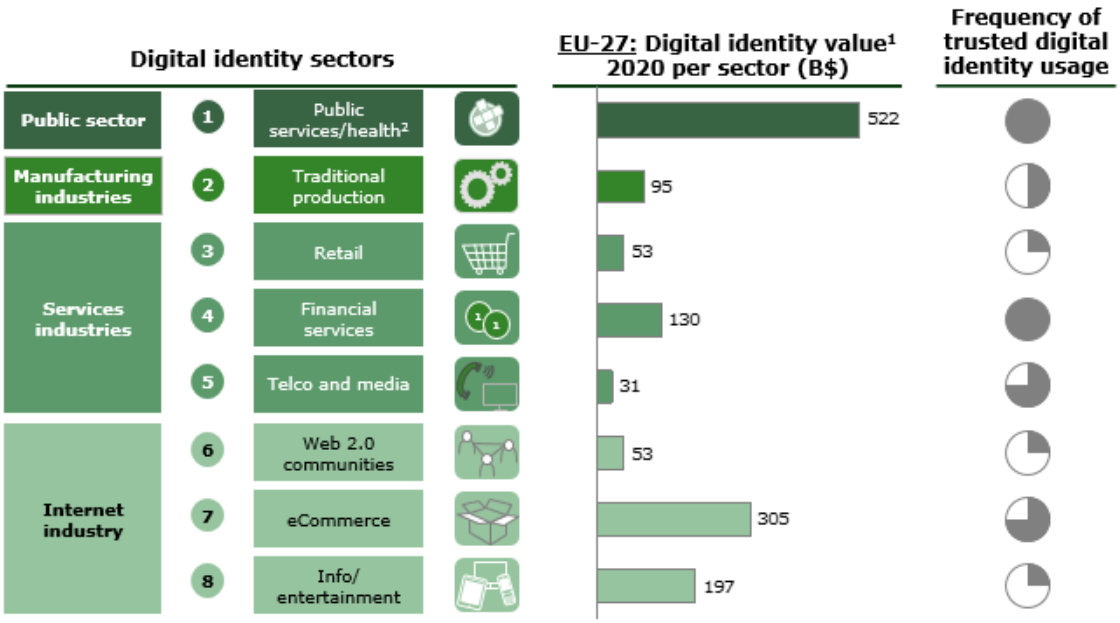
Today's digitally confident citizens expect public services to be available across all channels, the instant they need them and there is considerable pent up demand for eGovernment services.

This is positive news for governments looking to use the introduction of next generation Government eServices as an opportunity to consolidate and migrate information delivery and transactions online. Measurable outcomes of enabling self-service for citizens include faster, better quality and lower cost transaction processing plus the generation of improved transactional data sets to support enhanced decision-making.

Stimulating the digital economy

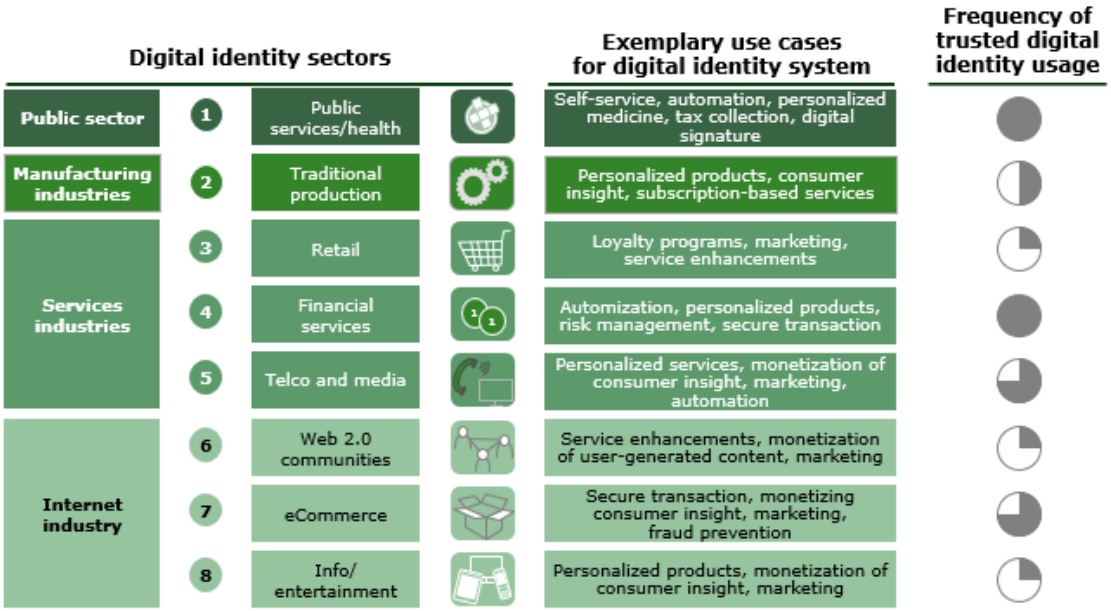
The wider benefits of the trusted digital identity as a key enabler of the wider digital economy are significant. According to the BCG model, the greatest value will be seen in the public sector – with a predicted value of $522 bn as we see in Chart four. This will be driven by use cases including: self-service, automation, personalized medicine, tax collection and digital signature.

Chart 4: Governments create digital economy value by introducing a trusted digital identity framework



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. But they can do more besides. By acting as the national validation gateway for ID service providers, governments will be able to accelerate the wider digital economy as we see in Chart 5.

Chart 5: Use case examples for digital identity systems



This creates a wealth of additional value and opportunities for manufacturing, service and internet-based industries to use digital identity to:

- initiate new loyalty programs, marketing and service enhancements
- monetize user generated content/insights/marketing
- introduce personalized products, subscription based services
- undertake secure transactions and process automation
- carry out data driven R&D.

Enabling this wider digital value creation, however, will depend on the ability of governments to develop digital identity frameworks that inspire trust and public acceptance. This will begin with the creation of a clear national policy strategy for digital identity management that benefits all and makes the creation of innovative online public and private services possible.

4. From Vision to Reality

Citizens are keen to take advantage of the convenience of anytime, anyplace, access and the opportunity to tap into more relevant and personalized service delivery.

From a citizen/consumer expectation perspective, however, the take-up of digital identity applications is heavily dependent on trust. This means the way in which digital identity develops is a primary concern but if governments are able to calibrate privacy controls and benefits appropriately, people will be comfortable and amenable to sharing personal data.

Turning the eGovernment – and wider digital economy – vision into a reality will therefore depend on governments and public bodies following guiding principles that underpin digital identity value creation.

4.1. The guiding principles of trusted digital identity

4.1.1. Protecting privacy

Organizations need to provide options for control regarding data sharing, building in 'privacy by design'. This will include giving citizens/consumers dashboards that enable them to change usage rights and define standard profiles for data usage.

4.1.2. Transparency

Organizations need to be fully accountable for a trusted flow of data, adhering to clearly defined codes that set out how they treat and use personal data. Any misuse will have a direct impact on the secure identity provider's reputation.

4.1.3. Responsibility

Organizations need to increase data security in order to safeguard digital identity. This protection should extend to organizational processes and should include a commitment to trace misuse and hold offenders accountable.

4.1.4. Communication

The benefits of any secure identification solution must be communicated clearly to all relevant parties in order to assure sustainable usage. The focus in all scenarios should be on enabled use cases rather than product/technology features.

4.2. The evolution to trusted digital identity

Until now the authentication of identity has proved a major bottleneck to the widespread realization of trusted digital identity. A number of high profile eGovernment implementations across the world, however, has meant that a growing number of citizens are now able to create an online government account and populate their profile with preferences and consents.

This expansion of digitally enabled citizens provides the ideal conditions for governments to initiate better and more harmonized service delivery across all agencies, and unlock the full value of digital identity in a sustainable and citizen-centric manner.

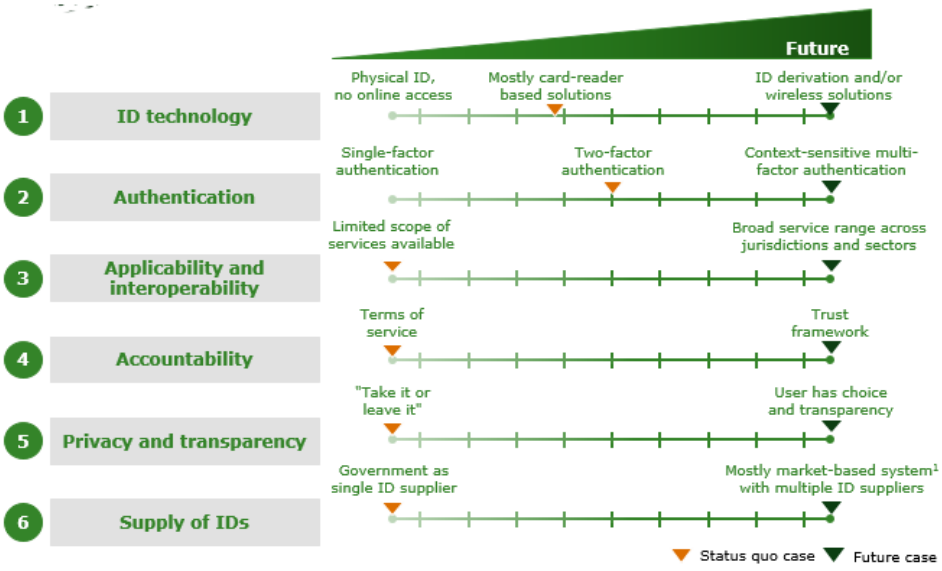
But if citizens are to benefit fully from a trusted digital identity that can be used to securely access both public and private services, then a fully interoperable environment needs to evolve to support secure and transparent data exchange between all parties – citizens, public and private sectors.

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.

4.3. The trust framework

From a technical standpoint the trust framework will an infrastructure that facilitates and enables trust and confidence between all members, delivering streamlined identity and data verification based on summary digital credentials. Many of these elements are already in place today, as we see in chart 6.

Chart 6: trusted digital identity use cases and product evolution towards 2020 vision



4.3.1. ID technology

Today's card-reader based solutions are evolving towards smartcard-based secure electronic ID verification while smartphones now have the capability to deliver electronic ID (eID) via standard contactless interfaces such as NFC (near field communications) and Bluetooth.

Smartcard-based eID delivers the benefits of the secure storage of personal ID information and offers direct control to users over their personal identity and data. For maximum mobility and compatibility across devices, eID derivation enables the root ID to be held in a secure document with additional 'derived' IDs being stored locally or in the cloud.

The question of where these identities are stored is crucial for obvious security reason 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.

This approach makes it possible for eDocuments to authenticate a user based on access to appropriate levels of the root identity, offering only enough information to authenticate transactions without revealing details on which that identity is built. In this way privacy is served, and a greater level of user trust assured.

4.3.2. Authentication

Today's 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.

But as we evolve towards the 2020 vision, context-aware authentication will be required to determine the identification method(s) most appropriate to the security requirements of the use case in hand; for example, multi-factor authentication involving biometrics can be added if required for high stake applications such as access to health records, with simple authentication being reserved for low-stake applications such as small payments. This approach ensures that convenience and security are both served to the benefit of users and organizations/governments alike.

4.3.3. Interoperability

Extending digital identity beyond today's limited scope of services to a broader service range that crosses jurisdictions and sectors is dependent on greater application and process interoperability.
Today citizens accessing private sector (retail, financial services, telco and media, Web 2.0 communities, information/entertainment) or public sector services will encounter multiple non-compatible systems, each requiring a separate ID.

In the future a single digital identity, made possible by an identity federation that enables the secure and standardized exchange of information by all parties, will enable citizens to access any public or private service.

4.3.4. Accountability

Trust frameworks will require policies and standards that establish what user information is accessible, which entity provides it, and gives citizens a degree of control over what data they make available - with the option of surrendering additional data for non-core services.

From a practical standpoint these policies will encompass enhanced discoverability, the definition of the summary digital credential itself, establish the procedures relating to digital inboxes/vaults that support information storage and communication and enable a 'tell us once' standard that supports information re-use/pre-filling.

4.3.5. Privacy and transparency

The pace of digital services uptake is heavily dependent on public acceptance and privacy and transparency are the twin pillars of a successful eGovernment implementation. That means governments need to:

- make data usage highly transparent
- communicate what information is being stored and the rationale for storage
- define access rights, maintain access logs and legislate a legal framework relating to data use.

Gaining buy-in from citizens will also mean giving users a degree of control over their information, with the option of surrendering further information to take advantage of non-core services.
Finally, regular audits should be put in place to eliminate system weaknesses together with third party assessments to provide additional credibility.

4.3.6. ID supply model

Today the starting point for most countries embarking on e-Document services establishes the government as the only supplier of electronic IDs. While this instils high trust levels in citizens and makes it possible to leverage existing government infrastructures, in the longer term it may prove less cost effective and has the potential to limit innovation.

In the medium to long term, many countries will move to a mixed supply scenario in which electronic ID is supplied by both government and private organizations. Ultimately, some countries may opt for a full market-based solution in which private organizations alone fulfil the delivery of electronic IDs.

Making the move to a mixed supply/full market-based model delivers a number of benefits for governments, including the ability to monetize e-Documents and generate a low cost and expansive framework that stimulates and extends the wider digital economy.

Managing a successful transition to such models will, however, depend on governments putting in place structures that actively establish widespread trust and support, to as great a degree as possible, interoperable standards and certifications. This will require a significant and sustained coordination effort.

5. eGovernment in the world today

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

Variations in cultural, legal and political influences around the globe, however, mean that governments in individual countries are adopting one of three Identity Framework models in pursuit of their national digitization vision and e-authentication initiatives.

5.1.1. Model 1: Multi-channel identity framework based on national eID

Countries that have pursued a multi-channel identity framework based on the government acting as the primary provider of a national eID as a root identity to provide faster and more secure public services to their populations include the Sultanate of Oman (the first smart card-based national ID solution deployed in the Middle East), the United Arab Emirates, and Estonia.

5.1.2. Model 2: Structured identity framework delivered via a federation

Countries pursuing a structured identity framework delivered by a federation of endorsed identity providers include Sweden, Finland, Singapore and Norway. In Norway, for example, the single sign-on portal gives citizens access to over 300 government services and supports multiple levels of authentication that include PIN code authentication, bank-issued electronic ID and certificates stored in USB pens issued by a private company.

5.1.3. Model 3: Open identity framework with no national scheme

The UK and the US currently operate an open identity framework without a national ID scheme.

5.2. eGovernment in action

5.2.1. Case 1: United Arab Emirates

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 the UAE eGovernment strategy is to provide innovative channels in a time and cost-effective manner. The official UAE government portal brings together federal and local government bodies under one umbrella and provides information to support accessing government services via the Internet, fixed and mobile phones and kiosks – as well as traditional service centers. The portal offers a number of interactive and transactional services (bill payments, license renewals) and guidance on a range of matters relating to how to apply for a visa or a health card.

The public also has access to a variety of government data and information (economic data, population statistics, etc) via the portal.

Citizens reap the benefits of efficient connectedness in their digital lives while UAE businesses can network, transact and interact to share knowledge and innovation.

5.2.2. Case 2: Malaysia

Announced in 1990, Malaysia's e-Government initiative had two key objectives: to improve government internal operations and to enhance the convenience and accessibility of interactions between government and citizens, and between government and businesses.

Extending the initiative across the country, Sarawak, the largest of Malaysia's 13 States and one of the two States located on the third largest island in the world – Borneo, now boasts a range of online services in support of its goal of creating 1.5 million jobs and long-term economic prosperity by 2030.

Since 1995 the Sarawak State Government has successfully initiated and implemented various online services and information services to effectively and efficiently distribute services to its citizens 'without time and space constraints'.

By 2011 a third of government services were online, including the popular Paybills Malaysia initiative that enables one-stop online payment of services from utilities to land rent. Latest figures point to some 1375 services now being available online from 'mygovernment', the Government of Malaysia's official portal.

5.2.3. Case 3: Estonia

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.

eGovernment in Estonia began with the development of a functional architecture that enables government databases to communicate, the introduction of a state ID card and the creation of a public key infrastructure. This was backed by a nation-wide state information security policy designed to create a safe information society for business and consumers.

State issued ID smart cards unlock access to government eServices and allow Estonians to send and receive encrypted emails. Today, Estonian citizens can register their tax, vote in national elections, access e-health records or school reports and register newborn children online.

6. Key principles and conclusions

The analysis uncovers a wide range of opportunities as we move towards 2020. For governments, the value comes through dramatic cost savings and greater citizen engagement. The user enjoys a richer, more secure and convenient experience, while the economy as a whole benefits as new eService models accelerate the growth of the private sector.

Underpinning this opportunity is, of course, the issue of trust. And this begins and ends with the integrity of the digital identity. Here the buck must stop with national governments.

Their role is not simply one of service delivery in the digital world, but service enablement. Citizens, healthcare providers, finance houses and more will all look to government to deliver the base identity - the anchor - on which all else is based.

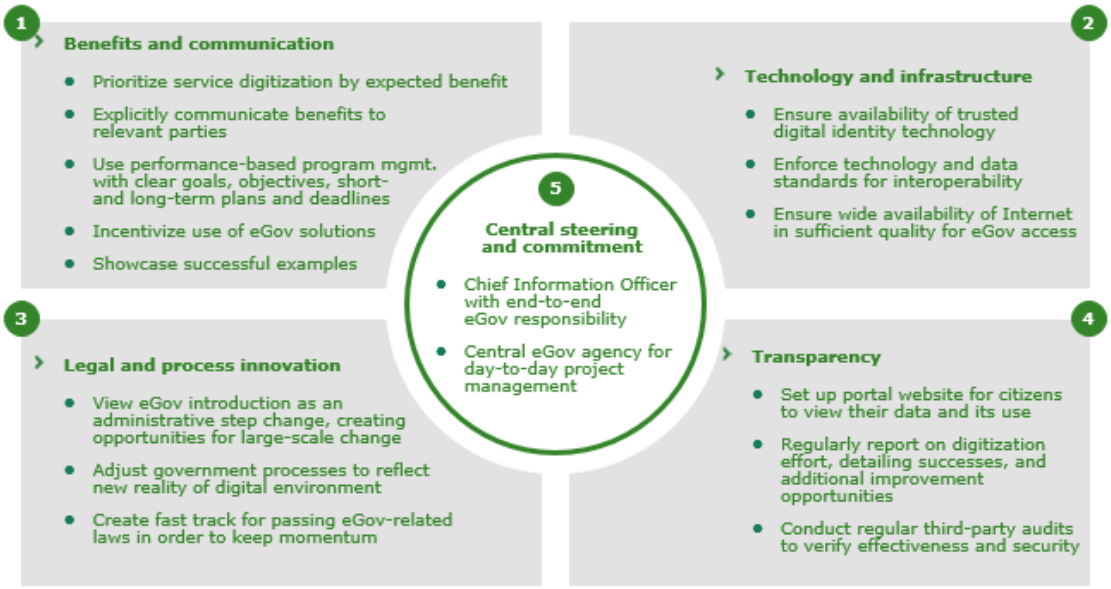
With governments already playing a key role in managing today's physical identity worlds - from birth, marriage and death certificates, through passports and driving licenses to national identity cards – the scene is set for them to deliver the same in the digital world of the very near future.

Should governments fail to take the initiative, they risk missing out on the kind of macro-economic benefits offered by a secure eServices boom.

Strategic Take Aways

Despite the complexities of the challenge, the Secure Identity Alliance and Boston Consulting Group analysis identifies five key recommendations for the successful implementation of eGovernment service: all of which stem from the development of a set of clear objectives, overseen by a committed and expert steering committee as we see in Chart 7 below.

Chart 7: Principles of successful eGovernment implementation



Furthermore, the Secure Identity Alliance is helping to drive international collaboration between government and non-government organizations through the creation of an eServices Provision Tracker (eSPT). An evolving program, the eSPT will offer an exhaustive market sizing and reference tool via a comprehensive analysis of the emerging market for government eServices across the globe.

Reporting on live implementations, the credentials chosen and the identity services provided, the eSPT identities service design, implementation and communication best practice to provide government, non-government organizations and private companies with the intelligence they need to build the next generation of secure, cost effective eServices.

Through the eSPT program and a host of other leadership and advisory services, the Secure Identity Alliance is helping governments, agencies and other public bodies realize the wide range of economic, public health, electoral and sustainability opportunities offered by the shift to digital service provision.

For more on the work of the Secure Identity Alliance visit www.secureidentityalliance.org