Moving into the e-government era

Conditions for the success of e-government strategies using the example of Estonia

A report by Sebastian Rieger and David Deißner – published by the Vodafone Institute for Society and Communications
"Moving into the e-government era – Conditions for the success of e-government strategies using the example of Estonia" is a publication by the Vodafone Institute for Society and Communications (2014).

This report analyses the conditions for success of Estonian e-government projects, takes from it insights that are potentially transferrable and outlines recommendations for political decision-makers. Eight areas of action provide an overview of current and future challenges in the provision of digital administration services.

The report is based on background discussions with Estonian e-government experts from the government, ministries, companies and science. We would like to thank the following discussion partners for their support and intensive input:

- Hannes Astok, Director of the e-Governance Academy (Tallinn)
- Luukas Ilves, Head of International Cooperations, Information System Authority (RIA)
- Rainer Kattel, PhD, Professor of Innovation and Technology Policy, Technical University of Tallinn
- Tarvi Martens, Technical Director, Certification Authority (Sertifitseerimiskeskus AS)
- Mart Maasik, Head of Business Innovation, SEB Bank (Baltic division)
- Dr. Viljar Peep, Director General, Estonian Data Protection Authority
- Pille Parikas, Managing Director, eSchool (Koolitööde AS)
- Jaan Priisalu, Director General, Estonian Information System Authority (RIA)
- Helena Raud, former Cyber Security Coordinator at the Ministry of Economics and Communication
- Siim Sikkut, National ICT Policy Adviser, Government Office of Estonia
- Tiit Tammiste, Head of Technology, AS EMT
- Ragnar Toomla, Head of E-Channels, SEB Bank (Baltic division)
- Linnar Viik, former technology advisor to the Prime Minister Mart Laar
- Indrek Vimberg, Head of the Estonian ICT Demo Center

This paper does not necessarily reflect the opinions of each of the persons named in all respects. The Vodafone Institute for Society and Communications has sole responsibility for its content.
Contents

01 | Executive summary ................................................................. p. 4
02 | Introduction .............................................................................. p. 5
03 | Areas of action for expanding digital offerings ......................... p. 9

I. Actively promoting the use of digital services ......................................... p. 10
II. Trust by Design .............................................................................. p. 13
III. Building digital infrastructures ........................................................ p. 15
IV. Digital Leadership .......................................................................... p. 18
V. Exploiting the potential of the private sector ........................................... p. 20
VI. Connecting digital infrastructures across borders ............................... p. 23
VII. Mobile government ....................................................................... p. 26
VIII. Maximising benefits for users .......................................................... p. 28

Endnotes and comments ........................................................................ p. 30
E-government, digital communication between citizens, companies and state institutions represents an ambitious goal: to make communication with public authorities and administrations more time-saving, more transparent and more secure. Political decision-makers are faced with the task of initiating the development of online-based transactions with public authorities and orientating e-government projects more strongly towards the needs of Internet users.

Estonia, the most northerly of the Baltic states, has played a pioneering role in this context. The country has a highly-developed digital infrastructure with a multitude of innovative administrative services that offer a clear added value as compared to the standard visit to the public authority. Due to special historical framework conditions as well as a small population “e-Estonia” is seen by many as a successful model sui generis. Nonetheless, the Estonian strategies and concepts and the practical experiences in their implementation are of particular value for political decision-makers from other countries. On the basis of extensive interviews, eight central areas of action were identified in which decision-makers from politics can have a stronger influence on the success of public service delivery. The focus was on the fundamental transferability of the recommendations.

I) Actively promote the use of digital services: e-government offerings are seldom overnight successes. In particular when propagating new services, incentives or rewards (“online bonus”) make it easier to address potential users. Further, different authentication processes should be provided to facilitate access.

II) Enable data monitoring and transparency: users should have the opportunity to monitor when and in what context their data is viewed and used.

III) Setting up digital public infrastructures: the pooling of various administration processes enables time-saving and user-friendly online transactions with public authorities. What is needed is access via electronic ID card functions and a standardised data exchange between administrative units.

IV) Digital leadership: e-government reforms require specialised organisation and a political mandate to coordinate and uniformly implement cross-administration digitalisation projects.

V) Exploiting the potential of the private sector: partnerships between companies and public institutions can substantially increase the attractiveness of e-government offerings. The prerequisite for this are financing models that are accepted by operators and users.

VI) Combine digital transactions with public authorities across borders: in Europe the demand for administrative offerings across national borders is increasing. The costs to companies, citizens and public authorities can fall if e-government strategies and technical standards are more consistently harmonised with one another.

VII) Mobile government: mobile technologies represent accelerated and location-independent communication on the basis of easy-to-use applications. Within the public sector smartphones and tablets help to open up new access channels or better manage public spaces.

VIII) Maximising benefits for users: e-government offerings are particularly attractive if they can be deployed in a range of settings or permit substantial time savings. Online administrative offerings must offer users a substantial benefit as compared with a standard visit to a public authority.
The digital transformation is posing new challenges for the public sector. Across Europe public administrations and governments have been developing programmes and strategies for shifting communication between public authorities, citizens and companies into the digital world.

The aim of these investments in the area of e-government is to exploit the potential of advancing digitisation in the public sector as well. However, latest insights into the risks to data security in the digital context show that in a democratic society efficiency gains cannot be bought at the expense of a risk to privacy and lack of say and monitoring by citizens. The decisive issue will therefore be how the digital transformation of the public sector can be structured transparently, securely and user-friendly.

Ultimately, the benefits of digital administration are plain: they are in no way limited to cost savings and efficiency gains on the part of the state. Instead, successful e-government initiatives generate direct value in the daily lives of citizens and companies. First, online visits to public authorities represent a time-saving, simplified and transparent form of contact with public administrations. Second, digital public infrastructures such as the electronic signature or the online ID function offer the opportunity to reduce transaction costs for the economy as a whole and initiate innovations in the public and private sector. The success of e-government initiatives is largely dependent on whether digital offerings are accepted, recommended and propagated by the citizens.

Despite a growing number of offerings: satisfaction with and use of e-government is on the decline

However, current surveys of users show that state online offerings are increasingly encountering dissatisfaction. Although a UN study (2012) describes the European Union as the most highly-developed e-government region in the world and EU states are constantly providing more offerings for citizens and companies, an international study recently pointed to a clear decline in the use of e-government services. This negative trend is also confirmed by a comprehensive survey in the EU member states on behalf of the European Commission (2012).

Various potential causes are discussed, and these may vary by country. However, what is particularly striking nonetheless is the clear rise in the fear of data theft, measured by surveys in Germany, Austria, Switzerland, the USA, the UK, Northern Ireland and Sweden between 2012 and 2013. Alongside a range of data protection scandals and cases of internet crime, it is assumed that the global surveillance scandal has dented trust in digital communication between citizens and state. Intensive discussions surrounding the revelations of the whistle-blower Edward Snowden fuel concerns about the protection of the privacy.

As well as a loss of trust by users, user-unfriendly or obsolete online administration offerings are a further source of increasing dissatisfaction. They often do not meet the requirements of a broad user base. This is hardly surprising: many offerings are still user-unfriendly, inaccessible, save little time or simply provide no benefit compared with a regular visit to the public authority. One negative example of many is the e-mail technology “De-Mail” introduced in Germany, which is envisaged as a communication standard between citizens and public authorities. At the end of 2012 even the test users...
of the renowned consumer organisation Stiftung Warentest failed in their attempts to operate the service in combination with an electronic ID card. The weaknesses of e-government offerings are becoming yet more apparent as an increasing number of citizens are managing complex tasks with the aid of easy-to-use commercial online services or apps. This lowers people’s understanding of long-winded log-in procedures or public authorities’ obscure platforms.

**E-government as a political challenge**

The increasingly critical perception of e-government strategies and offerings is intensifying the pressure on political decision makers. Administrative offerings should be more time-saving, transparent and secure and also have higher online availability. The introduction and development of state IT projects has become the subject of a public debate in which government representatives need to assume responsibility for unsuccessful technology. In the USA severe errors in the planning and development of the state’s online offering healthcare.gov resulted in hefty criticism being levelled at the US government in 2013. For the first time in history a US president had to apologise for a website. Rising user numbers will further increase the pressure for digitisation projects to succeed.

Political decision-makers are facing the challenge of supporting the design and planning of an e-government offering from an early stage, regarding it as a political process and communicating it accordingly. The networking of the public sector involves complex and highly-sensitive social decisions being taken in the area of the private sphere, security and financing. State online offerings establish or use technical standards and presuppose that the actors involved also accept these and propagate them freely – especially end users. If the various interests of the user groups are not sufficiently taken into account at the planning stage or if decisions appear to lack transparency, online services can become an arena for political conflicts. This can be seen for instance in the failed introduction of the ID card in the UK. Original plans envisaged linking the ID card to a state database that could contain up to 50 personally-related items on information of each citizen – including a number of biometric features. The comparatively large scale of the planned register increased reservations among the population and fuelled the discussion surrounding the protection of the private sphere.

The success of e-government projects is dependent on a large number of different factors, which vary depending on political, material and cultural framework conditions. Nonetheless, political decision-makers can actively support the planning of digital public services and make a substantial contribution to their successful realisation by setting the right strategic course. The exchange of political empirical values, strategies and best practices between European member states is a key precondition for this.

**Estonia: a test laboratory for the digital public sector**

Estonia is particularly important for the exchange of experiences in the area of digital public services. The most northerly of the Baltic nations is considered a European success story in the area of user-centric e-government. The country has a highly-developed digital infrastructure that is used as a matter of course on a daily basis by the citizens and the companies of the country, for example when they need to confirm their own identity or sign documents online. Additionally, a range online administration offerings have been developed that in part combine visits to several public authorities and enable considerable time savings. According to the Estonian government, the digital signature helped to save time worth a total of two per cent of the annual gross domestic product. Within the
Within the centrally-organised research system of the Soviet Union Estonia was developed as a research location for information and communication technologies in the 1950s.

The Baltic state reattained independence in 1991. There followed a rapid democratisation process as well as a comprehensive liberalisation of the economy. High direct investment, in particular from Finland and Sweden, underpinned the economic growth.

The technical reconstruction in administration and government commenced at the beginning of the 1990s with a low IT budget. The expansion of the IT infrastructure was driven forward by a broad network of scientists, IT experts, companies and politicians.

In 1996 the Estonian president announced the “Tiger Leap” programme. Computers and IT courses were included in the Estonian school curriculum.

In 2000 the parliament declared Internet access to be a human right.

Estonia joined the EU in the course of its easterly expansion in 2004. Estonia became a member of NATO in the same year.

2005: Internet voting was available for the first time in regional elections. Online voting in national parliamentary elections has been possible since 2007.

2007: Estonian ministries, banks, intelligence agencies and Internet providers were targeted by an extensive cyber attack. A range of online offerings and electronic payment transactions were affected.

The Estonian capital Tallinn became the location of NATO’s cyber defence centre in 2008.

In 2011 the EURO was adopted as the national currency.
administrative units, the digitisation processes were made leaner and responsibilities re-organised. The digitisation of the public sector has been driven forward by state institutions and companies – often in partnerships – who have supported the communication of this process since the beginning of the 1990s. Alongside the Estonian government and various ministries, banks and telecommunication companies have been key actors in building up the Estonian e-government system.

Given a population of 1.3 million people, centrally-organised administrative structures and special starting conditions after the country’s independence in 1991, the Estonian e-government is often regarded as a successful model sui generis. There is no doubt that the historical conditions and the particular cost and innovation pressure were highly favourable for a radical restructuring of the public sector in Estonia. The question of whether the Estonian e-government architecture could actually be transferred to other states is therefore anything other than trivial. However, we can learn lessons from Estonia: other European states and companies are becoming more interested in individual areas of the Estonian digital sector. Most recently, at the end of 2013, the Finnish government announced that it was adopting parts of Estonia’s system for networking digital public authority services. In the spring of 2013 the UK government also agreed a partnership with the Estonian public authorities to initiate an exchange of experiences in the area of e-government and to improve the attractiveness of existing offerings.

Exploiting experiences from Estonia for political decision-makers

Since 2000 Estonia has been expanding its digital sector and coordinating the interplay of various actors from the public sector and private economy who have acquired valuable experience and practical knowledge in the development, coordination and propagation of e-government projects. Even if the overall success of e-Estonia is unique in the international comparison, the existing know-how represents a valuable resource to increase the prospects for success of e-government initiatives in other European states.

On the basis of extensive interviews with e-government experts from government, administration, commerce and science, eight central areas of action have been identified for this paper in which decision-makers from politics and administration can exert a stronger influence on the success of the digital public sector. The aim of the discussions underlying this paper was to uncover the success factors for the development and implementation of the Estonian e-government architecture and offering landscape, focusing in particular on strategies that are fundamentally transferrable.
03 | Areas of action

I. Actively promoting the use of digital services

II. Trust by Design

III. Building digital infrastructures

IV. Digital Leadership

V. Exploiting the potential of the private sector

VI. Connecting digital infrastructures across borders

VII. Mobile government

VIII. Maximising benefits for users
Incentives and rewards were a key component of the Estonian e-government strategy from the outset. They also helped with the introduction of the electronic tax return, which is today used by around 95 percent of the Estonian population. Citizens who contacted the finance authorities via the online channel benefited from substantially shorter processing times. This also means that the online tax return can produce a substantially faster repayment of taxes – in some cases this can be as soon as five days after receipt of the application. An “online bonus” is also an effective means of communication when launching e-government projects.

Digital offerings also become more attractive if the users can access an online service via various channels. Alternative login procedures expand the group of potential users by taking various usage habits into account. If people can confirm their identity, for example using authentication via an electronic ID card and card reader (e-ID), via smartphone (mobile ID), the digital public authority visit gains flexibility and can be used anywhere. The Estonian citizens’ portal eesti.ee that pools the lion’s share of public authority offerings on one website can be accessed via three parallel access routes. As well as authentication per ID card and mobile device, citizens can also access the portal via the login procedures of large Estonian banks.

As mentioned earlier, partnerships with private providers were an effective instrument to extensively appeal to potential users. In Estonia the banks played an active role in propagating the electronic ID card (e-ID) by using their own branch network for distribution and advising citizens: “We used our branches to distribute card readers. But even more importantly we were able to answer questions about this new technology in situ” says Mart Maasik, responsible for corporate innovation at the Scandinavian SEB Bank.
Central access: the citizens’ portal eesti.ee

The state portal eesti.ee is the central point of contact for over 100 digital citizens’ services. The aim of the website is to provide user-friendly and uniform access to all e-government offerings. The portal is accessed by logging in using an e-ID or mobile ID. Alternatively, users can access the site via the authentication procedure of their own bank. Within the portal services include online visits to public authorities or digitally signing and sending documents. The portal further offers a control instrument within the state information system. In one area of the portal users can check which public authorities have accessed their data and for what purpose. The website interface can be individually customised and has offered reminder functions since 2013. Users can be automatically alerted if their pet’s booster is due or their tax return needs to be submitted. Around 10,000 people visit the eesti.ee platform every day. Developers are currently working on an interface especially for mobile devices.
The diffusion of e-government offerings and infrastructures is also influenced by pricing. As a rule, Internet users are not used to paying directly for e-mail postboxes or cloud services in the digital world. Financing is often done indirectly, e.g. by exploiting personal data or using advertising. If in contrast citizens are asked to pay directly for online contact with public institutions, fees – according to the opinion of the experts questioned – would have a deterrent effect in many cases. In the introduction of the mobile ID card function (mobile ID) in Estonia, private providers tackled this problem. “We had long [internal] discussions about the business model,” explained Tiit Tammiste, Head of Technology at the Baltic mobile company EMT. “We ultimately decided to subsidize the costs of the mobile ID function in the launch phase for our customers.” Estonian mobile providers see the mobile ID card function not as a short-term income stream, but rather as a driver of innovation and the basis of a range of service offerings with long-term amortisation.\(^\text{13}\)

Overall, legal obligations are without a doubt the most effective means of extensively introducing e-government offerings. However, they are not enough to appeal to potential users. Their distribution requires sales-like structures, which are difficult to establish single-handedly by public institutions.

- The benefits of e-government offerings need to be directly apparent in citizens’ everyday lives and clearly communicated by the public bodies. Incentives and rewards (“online bonus”) increase the attractiveness of online channels.
- Various authentication methods enable a flexible or location-independent access and reduce access barriers for potential users.
- The financing costs of e-government offerings should not be passed on as transaction fees for their use.
Estonia’s ministries and public authorities are networked to a significant extent. The national information system connects hundreds of public databases of various ministries and public authorities. The data exchange between administrative units means that over 90 percent of public citizens’ services can be accessed online. This strong networking of state databases necessarily means that citizens’ personal information is potentially accessible to a large group of people within the administrative apparatus. Although Estonia has relatively rigorous data protection laws and strict restrictions on access rights and monitoring instances, abuse cannot be ruled out. However, at the same time the state information system offers monitoring opportunities on the user side. One area in the Estonian service portal enables citizens to monitor which public authorities have accessed their data for which purposes – with exceptions for instance for criminal investigations. The monitoring mechanism represents a promising approach of how a highly-networked public sector can be structured in a more transparent manner. Given that unauthorised access to personal data (such as the illegitimate access to patient data by non-competent hospital employee) can be traced, in many fields approaches can be developed to increase the transparency of state conduct and the protection of personal data.

E-government services invite citizens to engage with public authorities digitally and to transmit personal data. Online communication with the state is – as with a regular visit to a public authority – not always unproblematic. By using communications technologies the expectations and reservations on the part of the users change. Alongside data theft and identity fraud, the possibility that data is being collected and monitored can also negatively affect the acceptance of e-government. Recently a comparative survey (2013) in Austria, Germany, Switzerland, the UK, Sweden and the USA pointed to a loss of trust and increasing security concerns in the use of online public authority offerings. In light of the global surveillance scandal, too, political decision-makers are faced with the challenge of designing digital services in the public sector such that social expectations of transparency and private sphere are reflected in the technical architecture.

Security concerns and a lack of trust in the handling of personal data vary by a country’s political culture or history. Nonetheless, they are of crucial importance in the use of digital public offerings. The causes of security concerns are manifold and their manifestations are difficult to measure. Although personal perceptions of private sphere, age or also political attitudes are considered central influencing factors, at the same time state e-government strategies cannot and should not aim to influence reservations or fears on the part of users. Instead, reforms should be aimed at the offering side and provide systems that offer a high degree of transparency, enable monitoring by the citizen and increase data security. Although Estonia’s digital public authority offerings enjoy a comparatively high level of acceptance among its citizens, a range of interesting approaches can be identified in the public sector by which transparency and user autonomy can be maintained or even increased in the digital context.

“...
Similar approaches are also possible in the planning and development of electronic ID cards (e-IDs). E-IDs have a range of benefits in the digital world and can be used to confirm an individual’s identity or to access administrative and private offerings. Yet they are not without controversy. Depending on the cultural or historical context there may be reservations regarding security, the protection of the private sphere or the creation of large digital registers. If the introduction of e-IDs is decided, a system should be chosen that aims to provide the highest possible level of protection of personal information or can manage with a minimum level of data. A negative example is the British ID card, the introduction of which was unsuccessful. An ID card was envisaged that was to be linked to up to 50 personal items of information and biometric features. In Estonia the public authorities and IT experts opted for a less data-intensive variant. The Estonian e-ID does without extensive registers and a chip contains simply the ID card number, the name, date and place of birth, the gender of the ID card holder and the validity date. This does not limit its functionality. “The electronic identity can be described as a form of key which can initiate the exchange of data between different administrative bodies,” explains Dr. Viljar Peep, Director General of the Estonian Data Protection Authority.

Experience from Estonia also shows that partnerships with non-state actors can help to address the different security needs within the population. In Estonia it is a legal requirement to hold an ID card with an electronic chip. However, it is up to citizens whether they use the electronic functions. Many public authority visits can alternatively be used with the login procedures of Estonian banks. Currently the access procedures of five financial services providers have been approved. The authentication procedures of the banks further played a key role in the early years of the digitisation of the public sector. Online banking was one of the first sensitive services that Internet users trusted. In 2000 citizens were able to submit a tax return to the fiscal authorities via the banks’ websites even before the introduction of an e-ID.

Designing e-government offerings to take account of the different social expectations of data protection and private sphere is a sophisticated task that necessarily turns out differently depending on the social and legal starting position. The specified examples from Estonia are promising approaches that could be developed further and at least partially adapted in other countries. It is not always easy to establish in advance whether a service or a digital infrastructure will be seen to be transparent or secure. IT strategies require in any event detailed feedback with the users and a broad stakeholder dialogue. E-government projects should therefore not only be considered simple tender processes, but understood and planned as a political process. Technical solutions for greater transparency, control and security will become more significant in future. This also involves offering users greater opportunity to participate.

- Reservations in the area of the private sphere and security are difficult to influence on the user side. E-government strategies should start on the offering side and provide technical opportunities for greater transparency and data protection.

- Online-public authority offerings should therefore work sparingly with data and offer monitoring options for users.

- Access to e-government offerings should take into account various user types and offer alternatives in the authentication area.
E-government offerings are especially well-accepted by users if they accelerate, simply and automate contact with public authorities. In order for tax returns to be pre-populated by a system or applications made without having to visit public authority, a digital public infrastructure was a central requirement. First, the public sector requires an opportunity to exchange information between the different administrative units. Second, it is necessary to set up a system for personal authentication on the Internet so that an individual’s identity can be proven for online visits to public authorities.

Networking existing databases saved costs – also because data does not need to be interrogated more than once [by citizens and companies].” Further cost benefits result because the same infrastructure can be used at the same time by citizens, civil servants and companies to access public data sets and services. Additionally, x-road is largely based on open technical standards. This lowers dependency on private IT and software providers and facilitates interconnection with other systems.

The decentralised architecture can lower the vulnerability to attack and guarantee that data sets are distributed across different institutions or are retained by different administrative units. Each ministry retains the control and responsibility of its own data sets – for the most part large data processing centres are not required.

The implementation of a state information system is not only a technical, but also an organisational and legal challenge. To drive forward the expansion of x-road in Estonia, a cross-ministry organisation (Estonian Information System’s Authority) was set up that actively integrates administrative units and public authorities into the standardisation process and accelerates the networking of the public sector. This organisation further coordinates the integration of private providers who want to integrate the e-ID service into their own offerings.
X-Road: Estonia’s digital infrastructure

“X-road” has been the digital backbone of e-Estonia since 2001. As a data highway of the public sector it networks the services and data sets of administrations and public authorities. A total of 300 million transactions were undertaken in 2012 between more than 600 organisations, national registers and databases. Users can access all available public authority services via a central portal – irrespective of responsibilities within the administration. The electronic ID card serves as an access key. X-road means that data does not need to be obtained twice from public authorities. If a citizen enters a new address, the existing information is accessed for future visits to public authorities. Tax returns or administrative applications are thus partly pre-populated. Interoperability lay at the heart of the development of x-road: state organisations were to be integrated into the network as simply as possible. This also applies to private providers who want to use the electronic ID card as a login procedure. The system uses Internet services and has a decentralised structure: administrative units retain control of their own data sets. There is no need to create connected, large databases. Currently the Finnish government is considering using parts of x-road to set up its own information system.
Alongside the x-road, the e-ID is the second pillar of the Estonian digital infrastructure. It is the access key to Estonia’s public information system and was introduced as early as 2002. Today around 86 percent of the population have it – and of these around 40 percent use the online functions. The card contains an electronic chip that has three separate functions: first, an individual’s identity can be confirmed during online visits to public authorities and private providers. Second, legally-binding documents and contracts can be digitally signed and dispatched. Third, the chip contains an email address that enables communication with public authorities and can be forwarded to a private mail address. In Estonia over a million e-IDs have been issued within five years (with a total population of 1.3 million). The relatively rapid spread is due above all to the fact that the ID card with digital functions was introduced on a mandatory basis. Acceptance was increased by means of a wide offering of digital visits to public authorities, partnerships with banks and communication providers as well as minimal costs on the part of the user. In 2009 it cost around 10 euros to apply for an ID card with e-ID function.

The historical framework conditions eased the way for the expansion of Estonia’s digital infrastructures. With the independence of the Baltic state at the beginning of the 1990s there began an extensive restructuring of the administration. For that reason, Estonia’s digital infrastructures cannot be taken as a wholesale model. Nonetheless, the empirical values from government, companies and universities are valuable for increasing the success of e-government projects in other countries and avoiding known errors.

- A system for exchanging data between administrative units is a key requirement for developing attractive and time-saving e-government offerings.
- A digital infrastructure lowers costs over the long term with the integration of new offerings and fosters innovations in the public sector.
- Public information systems should be set up in a decentralized manner in order for individual organisations to remain independent and to avoid the centralised storage of large quantities of data.
- Digital infrastructures require open technical standards in order to be deployed and further developed by a broad group of actors. In the long term they also facilitate the communication of digital services across national borders.
The expansion of the digital public sector in Estonia enjoys intensive and broad political support that to date remains an exceptional case in the international comparison. With Mart Laar, Prime Minister from 1992 to 2002, e-government reform found its way into the national economic policy of the country. The support at government level fostered coordination and implementation of cross-administration IT programmes, which enables enormous progress in terms of digitisation. And even if today comparable political support cannot be expected in other EU countries, specialised units with a government mandate are increasingly seen as a successful model. In 2011 the British government set up a special department for driving ahead the implementation of the national digitisation strategy and develop new online services. In the same year the Danish government set up an agency that is responsible for the digitisation of the public sector. Pooling technological know how and strategic oversight helped to accelerate the development of innovative services. Similar approaches were also taken in France and Norway.

The pooling of e-government competences and the support by high-ranking political decision-makers increases the opportunity of extensively implementing digitisation strategies. However, the forced implementation of large e-government projects seems to be less advisable. Conversely, an incremental set-up of digital offerings and infrastructures makes more sense from a strategic perspective. “Large state IT projects are difficult to monitor and overextend planners and developers,” highlights Linnar Viik, technology consultant to the former Prime Minister Laar. E-government strategies should not seek to develop novel, complex technologies, but instead utilise or refine existing, established standards. One example of this is the success of the Estonian information system (x-road) – a common data highway for communication between citizens, public authorities and companies. The system was designed such that it can be incrementally expanded by new services or

“ICT strategies have to be connected to overall benefits and objectives. It’s a precondition to capture attention and get all relevant stakeholders to cooperate”

E-government reforms and initiatives frequently only have a low priority among political decision-makers. In order to set up and modernise online visits to public authorities, changes to administration structures or where possible a redistribution of competences is necessary. Further, large state IT projects harbour financial risks. Nonetheless, experiences from multiple European states show that e-government initiatives require a clear political mandate to achieve successes across various administrative units.
E-government strategies demand the support of political decision-makers as well as the pooling of competences and resources in a specialised, cross-administration institution.

Public offerings and infrastructures should be developed incrementally and be made interoperable with a maximum number of other systems or services. Additionally, technical standards should allow citizens and companies to further develop existing services or create new applications.

E-government strategies should be linked to a clear strategy and foreground user benefit. Communicating the potential benefits is essential.

To drive e-government reforms forward as a political programme, political decision-makers rely on the cooperation and support of many different actors in the public and private sector. “ICT strategies have to be connected to overall benefits and objectives. It’s a precondition to capture attention and get all relevant stakeholders to cooperate,” explains Siim Sikkut, responsible for digital strategies in the Estonian government. E-government initiatives can be communicated and implemented more easily if an overarching goal is formulated. One example from Estonia is the requirement that the same data of citizens or companies is never interrogated twice. Digital services are developed with the specification that only a minimum of user data is interrogated. Originally established as a policy for reducing bureaucracy in reporting by companies, this developed into a guiding principle for improving the quality of online offerings.

E-government initiatives require consistent political leadership in order for the digitisation of the public sector can be more strongly orientated towards the needs of citizens and companies. Reforms should be approached incrementally and prioritise online administrative offerings that enable clear time savings on the part of the users.
E-government services and infrastructures are fundamentally different from other state technology projects. They cannot be developed, put out to tender and ultimately commissioned in a hierarchical process. Their flawless functioning, the propagation and acceptance by users are just as much success criteria as is technical completion. Decision-makers from politics and administration are faced with the challenge of including private providers and social actors in such a way that attractive offerings are developed and propagated without high costs being incurred.

The coordination and cooperation between state institutions and technology-driven companies is a central area of action in the e-government sector. Private providers are specialised in developing innovative systems that at the same time are aimed at the needs of users. If partnerships are successful, the quality and reach of public services can be substantially increased. The banking sector in Estonia began to introduce the first online banking offerings with the introduction of reliable and comparatively user-friendly login procedures for end users in 1996. Administrations and public authorities followed suit and managed users via the banks’ authentication procedures in order to offer their own state services online. Additional expenditure for public budgets or end users was avoided in this way. “At that time there were no direct financial incentives for the banks,” explains Ragnar Toomla, head of Online Services at the Baltic SEB. “In the long-term we were interested in winning over users for our Internet channels.” Converging public and commercial interests were the precondition for a substantial innovation drive within the public sector.

If companies come together and cooperate across sectors, their scope of influence can increase substantially. In 2001 Estonian IT manufacturers, telecommunication companies and banks set up a common foundation (tiger leap foundation) with the aim of increasing the low level of Internet use at the time within the population and familiarising people with new content and services. In collaboration with the Estonian state, Internet and IT courses for around 10 percent of the adult population were performed and financed. These were followed by information campaigns on IT security. The cooperating companies understood the joint commitment to be a long-term commercial investment in establishing a market for online and IT products. In the education sector, with the support of the school authorities and schools the online platform “eKool” (e-school), was set up which today the majority of teachers, pupils and parents use to organise the school day.

“All participating providers agreed that data security is a common task and takes precedence over competition”

A further important incentive for cooperation between the private providers and the public sector is the security of digital transactions. Banks and online retailers are reliant on users trusting digital channels and data remaining protected. This applies in particular to communication between public
The digital school platform eKool

Since 2003 Estonian schools have been using the online platform eKool to improve cooperation between schools, teachers and parents. eKool is not a classical e-learning application. The platform aims to reduce organisation and communication overheads in the school day. The website is used by 70 percent of schools and, depending on the user type, offers a range of functions:

- From the teachers’ perspective messages from teachers and pupils are received, grades and absences entered into a “digital register”, homework issued and class diaries kept.
- With a digital timetable pupils have an overview of grades, homework and exams in all subjects.
- Parents can follow their children’s school day and grades in a calendar as well as monitor absences. Sickness absence can also be submitted digitally.
- School heads have an overview of teachers’ workloads and the development of individual classes. School authorities are also provided with automatically generated reports.

EKool was the product of a foundation initiative (Tiger Leap Foundation) of the Estonian IT and telecommunication companies and was further developed in collaboration with schools and school authorities. Today the online-service is an independent private company that works closely with school authorities and ministries.
Moving into the e-government era | Areas of action for expanding digital offerings

• The integration of private suppliers into the set-up and provision of e-government offerings can substantially increase the innovative power of the public sector and accelerate the propagation of digital offerings.

• The prerequisite for the privately-operated e-government offerings is a balancing of the interests of the providers (business model) and users (costs & flexibility).

authorities and citizens. Estonia has a highly-developed electronic ID card system that enables all citizens to sign digital documents or confirm their identity online using with the ID card (e-ID). The technical infrastructure behind the e-ID is operated in conjunction with Estonian mobile providers and banks as an independent company. “All participating providers agreed that data security is a common task and takes precedence over competition,” explains Tarvi Martens, developer and technical head of e-ID infrastructure. The “Certification Centre” (AS Sertifitseerimiskeskus) is an official partner of the Estonian state and is overseen by the Data Protection Authority as the operator of the national digital ID card system. Although the company took ten years to recoup its own costs, it is generating a profit today and successfully serves a range of companies as well as state organisations at home and abroad.

The high quality and simplicity of the Estonian e-government offerings is hardly conceivable without the close cooperation between public and private sector. The manageable size of the Estonian market made it easier for private investment in pilot projects and common agreements amongst market participants. Political decision-makers are facing the challenge of integrating private companies not just as suppliers, but also as active providers of e-government initiatives and identifying approaches for partnerships in the private and public sector. They must be able to balance public and commercial interests such that digital public services are ideally free-of-charge for the end user.
The interaction and the networking of the e-government offerings and infrastructures, however, is a complex and difficult task. Technical standards and legal obstacles often block the way. Different IT systems in the EU countries are not always the most pressing issue. “A key challenge is the political consensus between expert groups and representatives of the member states,” emphasises Tarvi Martens, technical developer of the e-ID. The Estonian government is seeking to drive cooperation forward at the European level and to act as a mediator. One of the most ambitious projects is the digital signature, with which contracts or documents in the EU no longer need to be signed by hand and sent by post. Concluding legal transactions digitally, with the aid of an encryption procedure guarantees the origin of the signatures and can help companies in particular to automate and expedite processes. The reduction of transaction costs, postage and travel expenses – such as in the context of signing company agreements – and the associated reduction of harmful climate emissions are an obvious benefit.

The integration of digital infrastructures at EU level is a long-term political process that requires a high degree of cooperation and input by the member states. In parallel to that, e-government partnerships between individual member states can accelerate the development of offerings. The Estonian public authorities enjoyed an initial success in 2008. Since then users of an electronic ID card from Portugal, Finland and Belgium have been able to register a company online with considerable time savings. Further partnerships are planned with the neighbouring Scandinavian countries, the UK and the Netherlands.

The mutual recognition and networking of digital administrative offerings may be preceded by intensive negotiations and lengthy political agreement processes between European administrations and standardisation committees. However, in the long term they form an important prerequisite for mobil-
Visualising company structures

The online portal of the national company register is one of the most highly-developed e-government offerings in Estonia and pools a large part of the digital communication between the administration and economy. Since 2007 an online procedure has reduced the time needed to set up a company to around two hours and has completely replaced the need to visit a notary. Additionally, paperless amendments can be made to the commercial register or financial statements uploaded. The high level of digitisation of the register further enables a graphical representation of company structures. Relationships between legal and natural persons can be presented graphically and searched via a visualisation function. This facilitates inquiries by the fiscal authorities in the area of the prevention of money laundering and simplifies background checks in business life. In future networking with other European registers is planned to increase the transparency of cross-border company structures.
ity and cross-border trade in Europe. For example, 17 European states have adopted the pilot project STORK (Secure Identity Across Borders) to enable electronic proof of identity across borders in future.

- The networking of e-government offerings reduces the bureaucratic overhead and costs for European companies. At the same time the required workload for national public authorities to process foreign applications can be reduced.

- In parallel to the long-term collaboration at EU level, the integration of administrative offerings should also be driven forward between smaller groups of states. Pilot projects with neighbouring countries can produce short-term successes, for instance in border regions, and can be expanded incrementally.
In 2011 more mobile devices were sold than desktop PCs for the first time. The spread of smartphones and tablets has generated an innovation drive that now also extends to the public sector. Mobile data recording of public spaces, collaborative projects between citizens and administrations or mobile access to public authorities are among the first promising fields of application. With the success of mobile operating systems and apps, the requirements regarding operability and technical know-how increase at the same time. In the course of the integration of smartphones and mobile phones into e-government strategies, the task of adapting digital offerings to changing user behaviour and using mobile applications as a resource for the public sector emerges.

Over recent years mobile technologies in Estonia have developed into a firm feature of the communication between citizens, companies and the administration. Smartphones and tablets, or rather the SIM cards they contain, can be used as a substitute for the electronic ID card, for example to send messages to public authorities, submit tax returns or use mobile banking. “The electronic ID card was one of the factors for success in the digitisation of Estonia. For us developing a mobile ID function (m-ID) was a logical consequence,” explains Tiit Tammiste, responsible for the introduction of the m-ID at the Baltic mobile company EMT. To use the m-ID, customers are given a new SIM card. In combination with a PIN code the mobile device can be used as an alternative to the electronic ID card (e-ID) to access all e-government offerings, confirm an individual’s identity with private providers or sign digital documents. The mobile device replaces the card reader, which is a requirement for the use of the electronic ID card on the PC.

“The electronic ID card was one of the factors for success in the digitisation of Estonia. For us developing a mobile ID function (m-ID) was a logical consequence”

For Estonian mobile operators the m-ID has to date been less of a profitable product, but rather the foundation of new mobile fields of business and an additional incentive for customers to access services via mobile devices. Depending on the provider, the SIM card with an m-ID function is available free of charge or for around one euro per month.20 The technical infrastructure behind the m-ID is – as is also the case with the e-ID – operated jointly by technology companies and banks and overseen by the state. With currently around 40,000 mobile users, the mobile ID card is spreading steadily. However, with the m-ID an additional instrument is available to improve access to public online offerings and offer them independent of location.

With the ability to analyse large data sets, a further area of action has emerged for decision-makers in politics and administration. Estonian and Belgian researchers pointed to the potential of big data in a study from 2012,21 for which they analysed masses of positioning data from car drivers.
On the basis of mobile phone signals, the traffic flow on a section of motorway of the capital Tallinn was recorded and analysed. The study provided better understanding of the influence of commuter traffic on the development of traffic jams. Data analyses such as these could support public authorities and administrations in planning or managing cites and public spaces more efficiently. However, the anonymised use of personal data by the state requires precise objectives, rules and transparent procedures. Mobiles and smartphones are perceived to be personal items that store private communication and enable conclusions to be drawn about people’s social life and their movements. The extent to which mobile devices can be integrated into the public sector must be decided in future in dialogue with the users.

- **Mobile access increases the attractiveness and user-friendliness of digital public authority offerings.**

- **Operating systems of apps and tablets require the development of easy-to-use e-government services to win over new user groups.**

### The mobile ID card

The mobile-ID (m-ID) is the next stage of development of the electronic ID card for mobile phones, smartphones and tablets. This is a special SIM card that can be used in any device to manage transactions with public authorities whilst on the move and without a card reader. Originally introduced as an offering from the Estonian mobile provider EMT, the m-ID today is a component of the national e-government infrastructure. Alongside the option for confirming an individual’s identity, the m-ID enables digital documents to be signed and checked. For the logins to the state e-government portal eesti.ee, the user in first instance is prompted to enter a four-digit mobile ID code. To confirm communication with public authorities, following the login the secret code of the electronic ID card (e-ID) must be entered. The m-ID is offered by three Estonian mobile providers and, following receipt, needs to be activated on a public authority website via e-ID. Also, in the case of commercial services (e.g. online banking) mobile authentication is possible. Since 2007 40,000 customers have registered for the m-ID (correct as at March 2013). Its propagation has been slow in the beginning, but is increasing as mobile use rises. Today around 1,500 new users register for the mobile ID card every month.
European benchmarks and comparative studies demonstrate continuing progress in the expansion of the digital public sector. At the same time, in many European states today only a small number of visits to public authorities can be fully completed via the Internet. The low number of attractive e-government offerings and the low quality of some of them correlates with falling acceptance by users. Digitisation strategies should therefore focus on the development of such offerings that provide the users with a direct benefit as compared with existing administrative offerings.

If a public authority offers services via the Internet, in most cases citizens can choose whether to conclude the visit to the public authority offline, as they are accustomed to. A competitive situation arises in which the user ultimately decides. The more difficult the access or the application, the more probable it is that users will fall back on familiar processes. Further, the first visit to an online portal or the installation of a software application always represents additional effort for the user. Online visits to public authorities should therefore demonstrate a clear benefit to a large number of groups of people and organisations as compared with offline alternatives.

In Estonia the electronic ID card is not only used to confirm an individual’s identity, but further has an easy-to-use function for digitally signing any documents. In legal terms the digital signature is equivalent to a standard signature and can be used on all file formats. The offering enables considerable savings in terms of costs and time in that important contracts can be emailed instead of posted. The prerequisite is the Estonian electronic ID card with a card reader or a mobile phone with a mobile ID card function (m-iD). An app enables documents to be signed from a smartphone whilst on the move.

Estonian citizens, and in particular companies and administrations, use the service intensively and together provide some 80,000 signatures a month. In 2012 the electronic signature was used in 89 percent of all companies.

“E-Government strategies should follow a holistic approach and combine services into a coherent whole – even if this requires reorganising administrative processes”

“The time saved is one of the most important success factors,” explains Rainer Kattel, Professor for Innovation and Technology Policy at the Technical University of Tallinn. However, it is not sufficient for transferring existing administration processes onto the Internet. Clear time savings often only result when e-government projects combine or reorganise administrative steps. A further example from Estonia is the birth of a child. After the birth in the hospital the baby is given a temporary ID card number that is issued by the consulting doctor and registered online. Parents can then, from home, complete all necessary formalities in a sequence of consecutive steps without visiting different public authorities. The citizens’ portal enables for example the name to be registered, the child to be registered for health insurance or state social services to be applied for. E-government offerings have a high value for users if they cover an entire “life situation” and are planned from the perspective of citizens or companies. Similar examples can also be found in Estonia for the registration of a company or for tax returns. “E-Government strategies should follow a holistic
approach and combine services into a coherent whole – even if this requires reorganising administrative processes,” explains Linnar Viik, technology advisor to the former Prime Minister Laar.

Time-saving and simplified online visits to public authorities require an incremental networking of administrations. Above all legal and organisational obstacles present a challenge in this respect. Successful e-government initiatives are therefore to an extent reliant on complex administrative reforms that need to be conceived from the users’ perspective.

- Digital visits to public authorities need to promise users a clear additional benefit if they are to be accepted as new offerings.
- E-government offerings should not only transfer existing administration processes into the digital world, but should also pool visits to public authorities such that certain “life situations” are covered.
- Clear time savings and the reduction of costs are the most effective arguments to convince users of digital administrative offerings.

The electronic ID card

Since 2002 the electronic ID card (e-ID) has been the access key to Estonia’s digital world. With the aid of a card reader the e-ID enables people to get married, register a property in the property register or vote in parliamentary elections from the comfort of their home. During the 2011 parliamentary elections a quarter of voters voted online. Alongside the access to around 400 e-government services, digital documents can also be signed and sent with legally-binding effect – irrespective of the file format used. As an ID card document and driving licence the e-ID is mandatory for citizens, yet more than 40 percent of the population use the digital functions. The option for using the ID card for online banking as well as other commercial services has resulted in a comparatively high acceptance.

The electronic chip of the e-ID itself only saves a minimum amount of personal data, including the ID card number, the name, date and place of birth, the gender and the validity date. Comprehensive personal data is stored decentrally at the respective public authorities. For e-government services that stretch across a number of public authorities, the e-ID activates the necessary data exchange so that for example an electronic tax return can be automatically populated with information from the residential register. At the same time citizens can trace in detail which personal data has been accessed by public authorities on the e-government portal eesti.ee.
End notes

Vodafone Germany founded the Vodafone Institute for Society and Communications in 2011 to analyse social mega trends with a particular focus on the potential for and impacts of mobile technologies. The Institute’s objective is to comprehensively investigate the potential of mobile technologies to change society and derive knowledge for science, politics and business from its activities. It will particularly focus on the interrelationship between technological and social progress. Through joint research projects, own studies and the development of specific mobile applications, as well as publications and events, the Institute will initiate and lead dialogue about the mobile future.