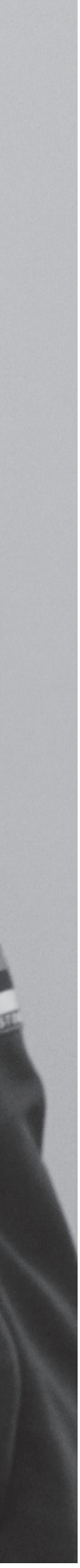
e-ESTONIA

e-Governance in Practice

Contents

President of Estonia,
H.E. Mr Toomas Hendrik Ilves



e-Society

What It Is & How It Works

Estonia is one of the most advanced e-societies in the world. An incredible success story that grew out of a partnership between a forward-thinking government, a pro-active ICT sector and a switched-on, tech-savvy population. Estonia boasts the world's leading IT infrastructure and e-services.

Estonian e-Society **indicators**:

100%
of schools and local governments have computers

99%
of **bank** transfers are made electronically

98%
of tax returns are made via e-Tax Board

95%
of medication is bought with a digital prescription (2014)

80%
of families have a computer at home

88%
of homes have a broadband connection

66%
of the population participated in the census via internet (2011)

30%
of votes were cast over the internet during the last Parliament elections (2015)

Today, the Internet is such a regular fixture in our lives that we only notice it when it disappears. Decision-makers in almost all developed countries have understood the importance of the Internet for the economy, and people's well-being, but also its overall role in the development of modern states.

In addition to the Internet, mobile network technologies are also constantly evolving and keep coming up with better solutions. Over the years, the development of the Internet and mobile communication has led to the emergence of completely new areas of business, as well as bringing about drastic changes in how modern states are governed. Nowadays the citizens of a country are primarily connected digitally rather than physically. Estonia is a unique country in the world in terms of the speed and level of e-society development. "e-Estonia" is the term commonly used to describe Estonia's emergence as one of the most advanced e-societies in the world – an incredible success story that grew out of the partnership between a forward-thinking government, a proactive ICT sector, and a switched-on, tech-savvy population. In addition to fast broadband connections, the rapid development of this digital society was also bolstered by the application of secured data exchange solutions and the introduction of an electronic identity (eID) – two key ICT projects that have been operating smoothly for more than 15 years. As a result, e-services have become routine for citizens of Estonia: i-Voting, e-taxes, e-police, e-health care, e-notary, e-banking, e-census, e-school and much more.

How is this possible? First magic ingredient is the data exchange layer X-Road. It is the environment that allows the government's various databases and registers, both in the public and private sector, to link up and operate in harmony regardless of the technical platform they use. Almost 15 years of active duty with no down time, and as a result we have over 170 databases offering their services via X-Road. Secondly, in Estonia digital signatures and authentication are legally equivalent to handwritten signatures and face-to-face identification. The eID opens the door to all e-services while guaranteeing the highest level of security and integrity. Currently, the eID is actively used by 60% of Estonians without a single security incident since its launch in 2002.
(Reference: e-Estonia website)

The main question is - should we protect the king (i.e. the person) or the route (where the king is travelling)? In Estonia, we have chosen the king, meaning we prioritise the protection of personal data. We use public Internet, but the data that is exchanged is encrypted and digitally signed. However, all other alternative systems have high-level security requirements as well. What is more, in 1997 the "only once" principle became a legal imperative, meaning that the authorities could not ask an individual to provide information she or he had already provided to any part of the administration. (Reference: Public Governance And Territorial Development, OECD, Paris, Https://Www.Oecd.Org/Gov/Key-Findings-Estonia.Pdf)

This publication provides an overview of the creation and management of the information society, implementing cyber security measures, setting up electronic identity and secured data exchange, developing a new generation of broadband networks, formulating necessary regulations, educating citizens, and many other important aspects of establishing an e-society.

Overview of Main Electronic Services in Estonia

TIMELINE

- 1996 e-Banking
- 2000 e-Cabinet
- 2001 e-Geoportal
- 2003 e-School
- 2005 i-Voting
- 2006 e-Notary
- 2008 e-Health
- 2014 e-Residency
- 2000 e-Tax Board
- 2000 m-Parking
- 2003 Eesti.ee
- 2004 e-Ticket
- 2005 e-Police
- 2007 e-Business
- 2010 e-Prescription


EESTI.ee
Gateway to eEstonia
My Data
Services
Topics
Contacts
Eesti.ee activated a notification service for people who forward their official e-mails
99%
of all state services are online.

Since **2003**

eesti.ee – Gateway to e-Estonia

The official Estonian State e-Services Portal **eesti.ee** is **a secured gateway** to 99% of e-services offered in Estonia.

The portal provides users with easy access and gives the government a better platform for integrating and promoting new services.

In 2014 eesti.ee offered access to 815 e-services, and was visited by Estonians from over 200 countries in the world. Altogether the e-services received ca 7 million views, which is five times more than the population of Estonia.

BENEFITS

1 EESTI .ee

single point of contact

2 EESTI .ee

easier access to all e-services

3 EESTI .ee

convenient platform for promoting new services

Procurement Initiative: Ministry of Economic Affairs and Communications and Estonian Information System Authority (www.ria.ee)
Further information: www.eesti.ee

Since **1996**

e-Banking

Our leading banks (Hansapank and Ühispank, now Swedbank and SEB) played an invaluable role in developing the first electronic solutions, and helped move the Estonian population online by offering high-quality e-banking services. By giving away free ID-card readers, and encouraging their customers to use ID-cards for securing transactions, the banks helped to promote more frequent use and wider application of the national e-identification document.

Now Estonia is nown throughout the world for its user-friendly and secure online banking. As of June 2016, only the initial procedure of opening an account requires a personal appearance at the bank (there has been talk of changing to secured first online identification), and afterward all subsequent transactions can be made online by confirming them with your electronic identity. What is more, banks are constantly lowering the daily transaction limits for online users with password cards to use more secured eID methods. As a result, the expression "going to the bank" is slowly disappearing from the Estonian language.

In addition, Estonian banks have partnered with telecommunications companies to invest in Look@World, a project that provides basic computer literacy courses to adults free of charge all over the country. As much as 10% of Estonia's adult population has participated in these courses, which were organised in 2002, 2009 and 2010. The results of all these efforts are quite staggering - today, an incredible 99.8% of all banking transactions in the country are made online. What is more, according to the European Central Bank, the banks operating in Estonia are significantly more efficient than the rest in the Eurozone.

BENEFITS

1. no need to visit the branch office in person
2. transactions are cheaper when made online
3. saves time and money for both the customer and the service provider
4. accessible 24/7
5. secured access from any place on earth (with Internet connection)

Procurement Initiative: Estonian two leading banks, Swedbank and SEB, were the main driving forces behind the development of online banking.
Further information: Swedbank www.swedbank.ee
SEB www.seb.ee

Since **2000**

e-Tax Board

e-Tax Board is the electronic tax filing system set up by the Estonian Tax and Customs Board. It has become one of the growth drivers of e-ID usage in Estonia. Since its introduction in 2000, it has helped drastically reduce the time spent by private individuals and entrepreneurs on filing taxes.

In 2002 the system reached a major developmental milestone with the introduction of automated tax declaration forms. Using a secure e-ID, the taxpayer logs onto the system, reviews their data in pre-filled forms, makes the necessary changes, and finally, approves the document with their digital signature. The process typically takes three to five minutes, and as a result, over 97% of tax declarations in Estonia are now filed electronically. In addition to individual tax returns, the system also allows for:

- corporate tax returns, incl. all relevant employee taxes
- value-added tax returns
- excise duty returns (eg. alcohol, tobacco, fuel, packaging, etc.)
- INF declarations
- customs declarations

BENEFITS

1. easy and convenient to use
2. lower administrative cost for the Tax Board
3. tax returns can be filed in 3-5 minutes
4. taxpayers receive refunds in five days
5. transparent and efficient tax collection

Procurement Initiative: Estonian Tax and Customs Board (ETCB)
Further information: www.emta.ee

Since **2000**

e-Cabinet

The Information System of Government Sessions, better known as the e-Cabinet, is a powerful tool that the Estonian government uses to streamline its decision-making process. It enables ministers to prepare for and conduct cabinet meetings, review minutes, and perform other relevant tasks entirely without the need for paper.

At its core, the system is a multi-user database and scheduler that keeps relevant information organised and updated in real time, giving ministers a clear overview of each item under discussion. Well before the weekly cabinet session begins, the ministers access the system to review each agenda item and formulate their personal positions. Should they have any objections or would like to speak on the topic, then they just need to check the relevant box. As a result, the ministers' positions are all public prior to the cabinet meeting, and decisions that have received no objections are adopted without debate, saving considerable time. What is more, the decisions made at the cabinet meetings can be e-mailed to interested parties or posted on a website even while the meeting is still in session.

BENEFITS

1. ministers are better organised
2. possible to take part in meetings remotely using audio-visual equipment
3. no need to carry around large stacks of paper
4. average session time drastically reduced from 4 to 5 hours to just 30 to 90 minutes
5. lower environmental impact
5. decision-making process is more transparent and understandable

Procurement Initiative: Government Office, Republic of Estonia
Further information: www.riigikantselei.ee/e_cabinet/

Since **2000**

m-Parking

Mobile parking, or m-Parking, is a convenient system that enables drivers to pay for their city parking via mobile phone. Today it's the most widely used method of payment for parking, with 90% of parking fees paid via mobiles.

Drivers wishing to park their cars can either use a location-based application or send an SMS with the parking zone's code. When the agency checks the vehicle's registration number in their database, they will receive confirmation that parking is registered. Upon leaving, the driver discontinues the parking service using the app or sends another SMS. At the end of each month, the total cost of monthly parking is added to the driver's mobile phone bill. The system is suitable for both public and private parking lots.

The Estonian m-parking system has been adopted, copied, replicated and mimicked all over the world (e.g. the US, Canada, Austria, Sweden and Dubai), and thus it has become practically impossible to track all the various modes of implementation. However, as of June 2016, Estonia remains the only country where mobile parking is the prevalent method of payment and is applicable in all the paid parking areas all over the country.

BENEFITS

1. convenience – farewell parking forms
2. local municipalities save on parking meter infrastructure

Procurement Initiative: Tallinn City Government in collaboration with a leading mobile network operator
Further information: www.parkimine.ee/en

Since **2003**

e-Geoportal

The Geoportal administered by the Estonian Land Board is a convenient tool pooling information from a variety of map servers and spatial data services, eg. the portal links to the electronic Cadastral Register, containing information on the value, natural status and use of land.

Paired with the geographical information system (GIS), the e-Geoportal delivers real-time geographical data via the X-road, enabling advanced map-based visualisations that power many of the location-based services in Estonia. The Estonian e-Geoportal is a part of the Estonian Spatial Data Infrastructure, which in its turn is a part of the Infrastructure for Spatial Information in Europe (INSPIRE).

Another important e-service is the e-Land Register that links to the official property ownership database, pooling information related to ownership and limited real rights on immovable property in Estonia. This electronic registry has transformed the way property transactions transpire in Estonia nowadays, eliminating the need to visit a public office and spend hours waiting for a civil servant to review records. This paper-free system has significantly reduced the process time for land transactions. As a critical tool for the real-estate market, it ensures transparency, listing the registered owner of each property holding, indicating property boundaries and providing other relevant information (incl. cadastral information, encumbrances, mortgages, etc.) for potential buyers. What is more, businesses also benefit from the convenience of having instant access to land registry information and the ability to confirm ownership with just a few clicks of the mouse.

BENEFITS

1. easy to make inquiries regarding general property information
2. convenient access to land registry documents
3. saves time, administrative costs, and allows paper-free administration
4. transparent system curtailing real estate fraud and corruption

Procurement Initiative: Estonian Ministry of Justice, Centre of Registers and Information Systems
Further information: Estonian Land Board Geoportal www.geoportaal.maaamet.ee,
e-Land Register www.rik.ee/en/e-land-register

e-School

Since **2003**

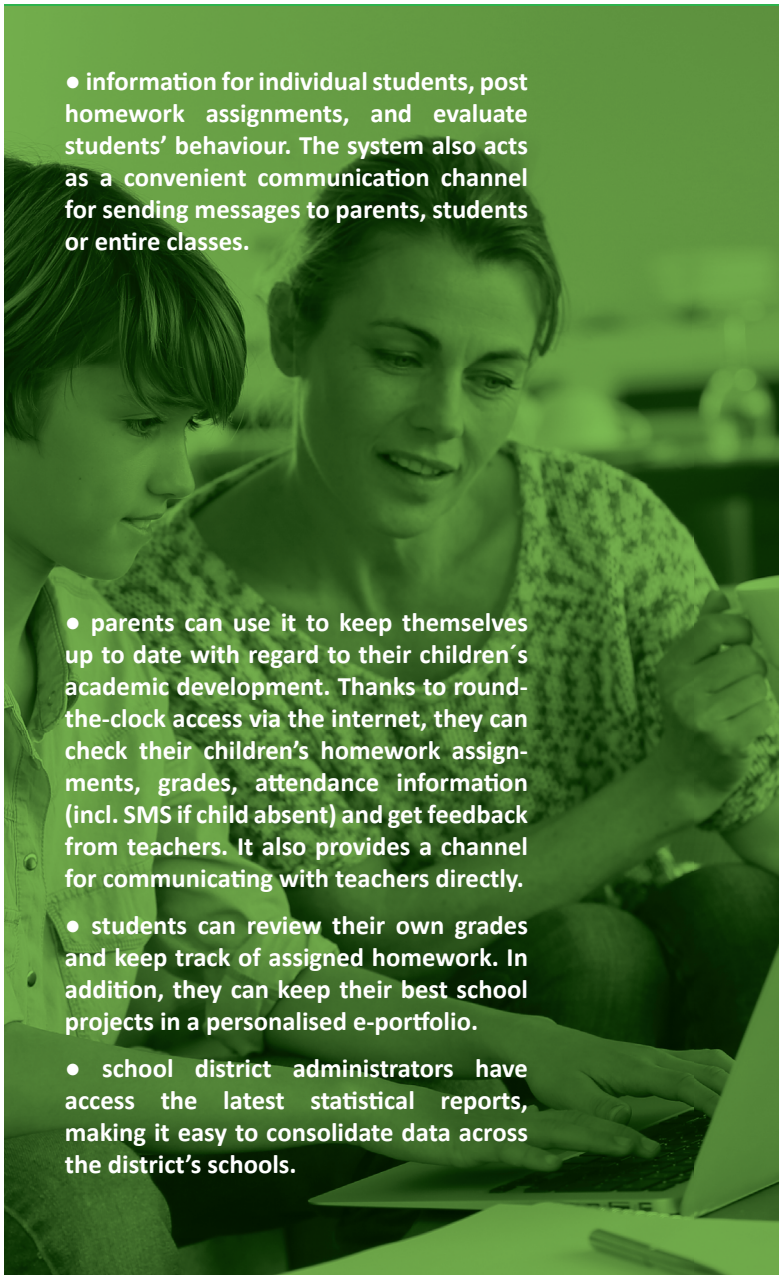
The e-School has become one of the most widely used e-service in Estonia.

The main goal of the e-School is to make study-related information easily accessible for both children and their parents, facilitate the work of teachers and the school management, and generally engage parents more actively in their children´s education.

BENEFITS

1. kids have an overview of their grades and overall progress, and they can also access their homework assignments
2. parents can be more actively involved in their children's education
3. improved communication between teachers and parents
4. more efficient organisation and record-keeping for teachers

The system offers a range of different functions for its various users:



- **information for individual students, post homework assignments, and evaluate students' behaviour. The system also acts as a convenient communication channel for sending messages to parents, students or entire classes.**
- **parents can use it to keep themselves up to date with regard to their children´s academic development. Thanks to round-the-clock access via the internet, they can check their children's homework assignments, grades, attendance information (incl. SMS if child absent) and get feedback from teachers. It also provides a channel for communicating with teachers directly.**
- **students can review their own grades and keep track of assigned homework. In addition, they can keep their best school projects in a personalised e-portfolio.**
- **school district administrators have access the latest statistical reports, making it easy to consolidate data across the district's schools.**

Procurement Initiative: Look@World Foundation www.vaatamaailma.ee/lookworld

Further information: www.ekool.eu

e-Ticket

Since **2004**

The e-Ticket is a ticketing solution introduced in Tallinn in conjunction with the implementation of personalised tickets in the local public transportation system. As a result, nowadays only tourists buy paper tickets when using public transport in Tallinn.

The main reason for introducing e-ticketing in Tallinn on such a large scale was the new policy launched by Tallinn City Government aimed at local residents, and offering a new scheme of discounts and concessionary fares for specific groups (eg. students, seniors, and disabled people, etc.). In order to have a better overview of passengers and their status, the initial idea was to issue new personalised travel cards for specific user groups, which would have entailed high auxiliary costs as well as inconvenience for the user.

However, the process of transitioning to personalised ticketing was facilitated by two related developments. Firstly, the Government launched the ID-card with electronic identity initiative. Secondly, it coincided with the wider implementation of secured data exchange layer X-Road, which enables queries to different databases. Eventually, these two developments formed the basis for the ID-card based e-ticketing solutions implemented in the public transportation system in Tallinn.

BENEFITS

1

more convenient and streamlined system for the customer, i.e. no need to purchase a physical ticket- all you need is a phone or a computer with an Internet connection

2

easier to check the validity of tickets, i.e tickets are stored on ID-cards, and must be validated upon each entry

Procurement Initiative: Tallinn City Government
Further information: www.ridango.com

Since **2005**

e-Police

Estonia's electronic police system is based on the idea, that providing the best possible communication and coordination will lead to the most effective policing.

The e-Police system comprises two main tools: a mobile workstation installed in each patrol car, and a positioning system used in the headquarters, showing each officer´s location and status. As a result, each police vehicle is equipped with a computer in the luggage compartment, a monitor, a positioning device, and access to a digital map. In addition, the mobile workstations installed in patrol cars give officers in the field nearly instantaneous access to vital information, enabling aggregated queries from police databases, Citizen and Migration Board, Motor Vehicle Registry, Traffic and Insurance Fund, etc.

BENEFITS

1

the control centre knows the location of each patrol car at any given time

2

improved efficiency, eg. 70% increase in offense reports handled per day, road fatalities have decreased by over 400%, 1000% increase in vehicle queries performed per month.

Procurement Initiative: Estonian Police and Border Guard Board
More information: www.politsei.ee

i-Voting

Internet voting (i-Voting or online voting) is a system that allows voters to take part in national or local elections by casting their ballots online via an Internet-connected computer, from anywhere in the world. It is used as an additional voting method to improve accessibility to elections, and should not be confused with other electronic voting systems used elsewhere that rely on special voting devices set up at the polling station.

Since **2005**

The Estonian solution is simple, convenient and secure, allowing voters to cast their ballots from a location of their choosing (home, office, abroad), without having to go to a polling station. There is a special designated pre-voting period during which the voters can log onto the system using their ID-cards or Mobile-ID which establish the voter's identity. However, upon casting a ballot the voter's identity is removed from the ballot before it reaches the final counting stage performed by the National Electoral Commission, and thus, each vote remains anonymous.

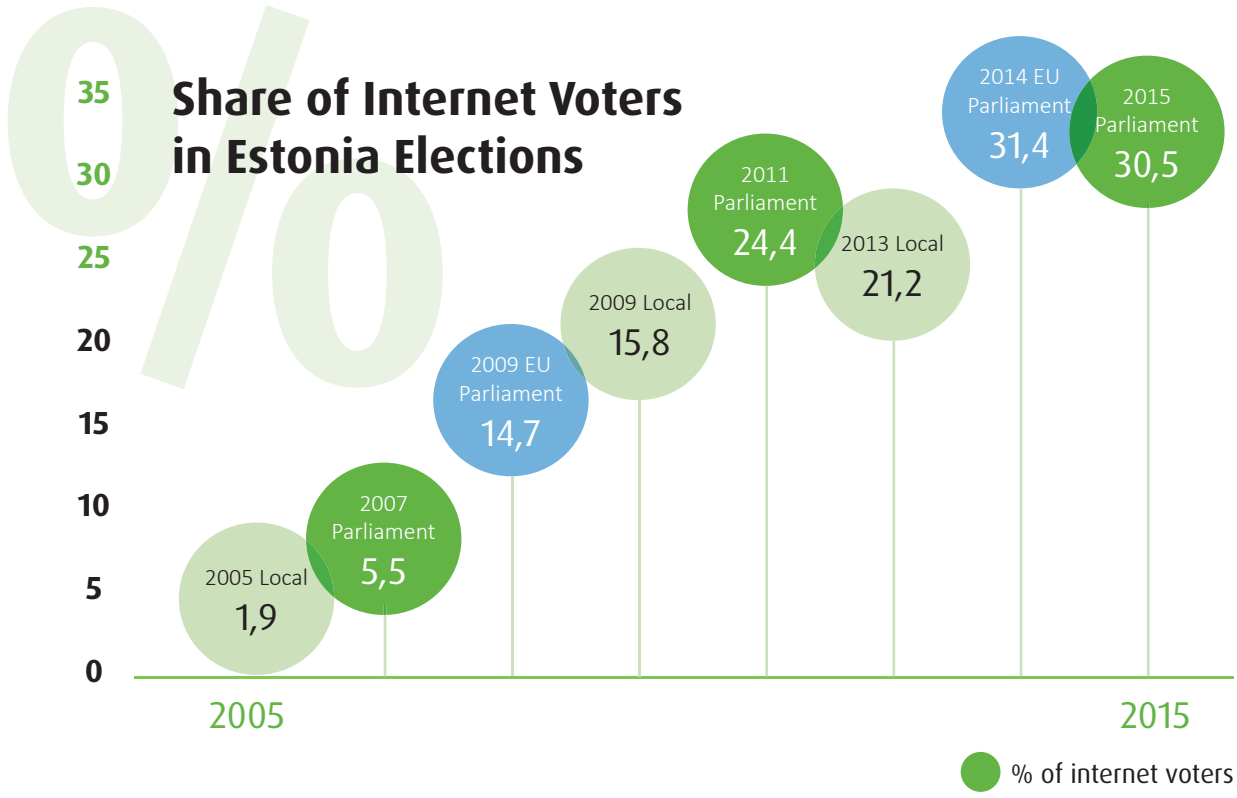
The system also allows online voters to re-cast their vote during the designated online voting period, which leads to their previous vote being deleted. After the online voting period ends, polling stations receive a list of confirmed online voters in order to prevent them from voting for the second time on election day.

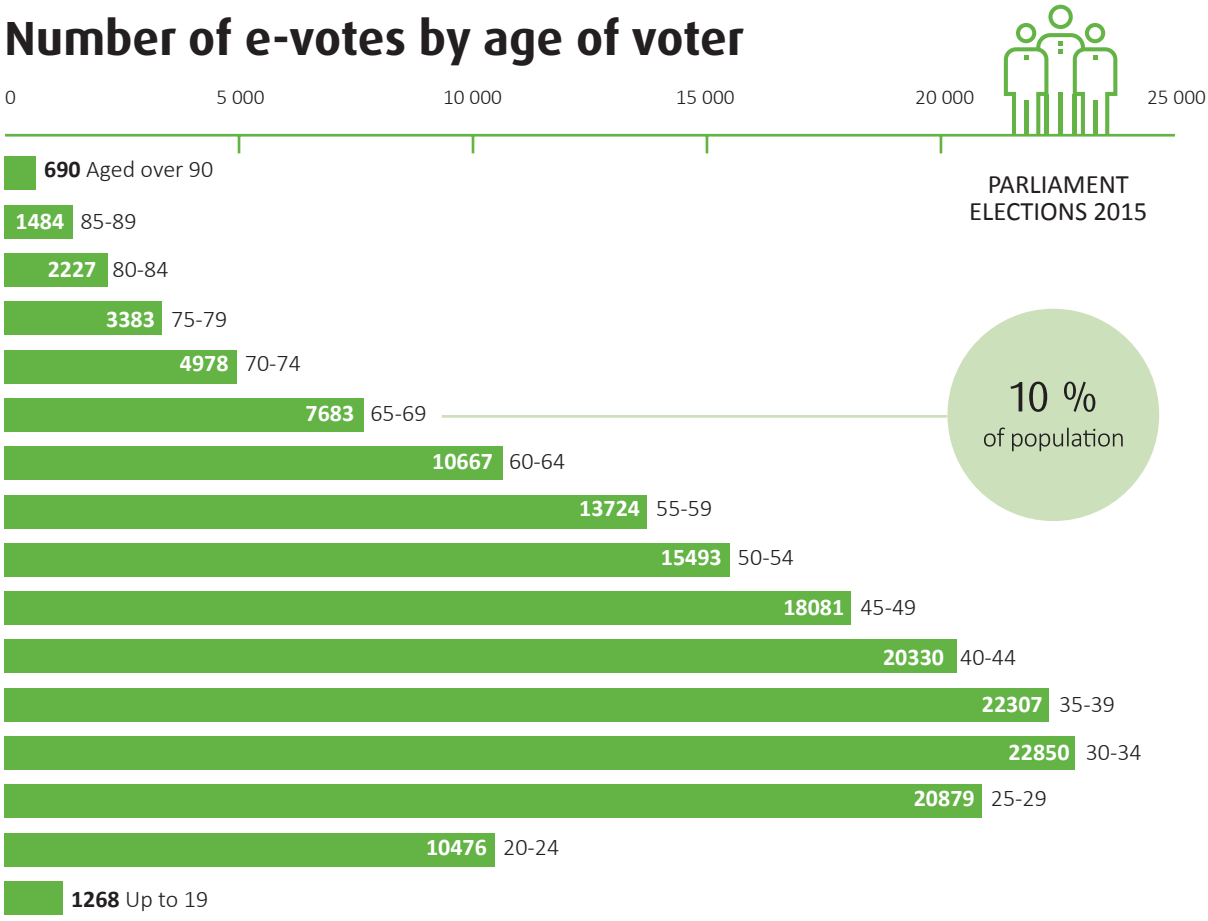
In Estonia, Internet voting was first introduced during the local elections in 2005, when about 2% of all participating voters cast their ballot via the Internet. Thus far, i-Voting has subsequently been used eight times in Estonia, with the number of online voters increasing each time, with ca 31% of votes cast online in parliamentary elections in 2015. What is more, during the 2015 elections, votes were received from 116 countries.

eGA Senior Expert and Politician Liia Hänni

Over 10 years of secured internet voting.

Procurement Initiative: Electronic Voting Committee of the National Electoral Commission
Further information: www.valimised.ee


Share of Internet Voters in Estonia Elections
35
30
25
20
15
10
5
0
2005 Local 1,9
2007 Parliament 5,5
2009 EU Parliament 14,7
2009 Local 15,8
2011 Parliament 24,4
2013 Local 21,2
2014 EU Parliament 31,4
2015 Parliament 30,5
2005
2015
% of internet voters


Number of e-votes by age of voter
0
5 000
10 000
15 000
20 000
25 000
PARLIAMENT ELECTIONS 2015
690 Aged over 90
1484 85-89
2227 80-84
3383 75-79
4978 70-74
7683 65-69
10667 60-64
13724 55-59
15493 50-54
18081 45-49
20330 40-44
22307 35-39
22850 30-34
20879 25-29
10476 20-24
1268 Up to 19
10 % of population

Since **2006**

e-Notary

The e-Notary system is an online platform created specifically for notaries, and helps them in everyday work, also enabling electronic communication with government agencies (incl. registry queries).

The system is owned by the Chamber of Notaries and the servers are administered by the Centre of Registers and Information Systems; the latter also provides user support, user training and continued system development. The e-Notary platform can only be used by notaries and notary office employees (eg. deputy notaries, lawyers, secretaries, receptionists and archive employees).

eGA Associated Expert
Sandra Roosna

BENEFITS

1. keeping a schedule of notarising activities
2. preparing agreements and allowing digital signatures
3. making reliable queries to state registries
4. forwarding records to state registries
5. minimising paperwork, printing and repeated data entries
6. reduction of red tape between notaries and clients, faster way of doing business with notaries

Procurement Initiative: Estonian Ministry of Justice, Chamber of Notaries
Further information: www.rik.ee/en/other-services/e-notary

Since **2007**

e-Business

The e-Business Register is an online platform linked to the official database comprising the real-time data on all legal entities registered in Estonia.

In addition, the e-Business Register also hosts the online Company Registration Portal, which is an Internet platform that allows entrepreneurs to submit electronic applications, documents and annual reports to the Commercial Register. Applications can only be signed using an ID-card or Mobile-ID. Thanks to this paperless business platform, Estonia has significantly reduced administrative costs and is more attractive to foreign investors, with the opportunity to start a business within 18 minutes (as opposed to five days when using traditional methods).

Services available via the Company Registration Portal

- establishing new businesses and non-profit organisations, and submitting applications to amend, liquidate or delete registry data
- e-platform for compiling, signing and submitting annual reports
- web-based accounting software e-billing, which helps start-ups and small business to organise their accounting

BENEFITS

1. review company's general data and tax arrears data
2. access to annual reports, statutes, personal and commercial pledge data, etc.
3. real-time monitoring of processing data and record amendments of companies
4. verifying of business and entrepreneurship prohibitions of Estonian persons
5. visualise relations between various companies and persons

Procurement Initiative: Estonian Ministry of Justice, Government Office of Estonia
Further information: e-Business Register www.ariregister.rik.ee,
Company Registration Portal www.ettevotjaportaal.rik.ee

Since **2008**

e-Health

The Electronic Health Record is a nationwide system that integrates data from different health care providers to generate a single electronic file providing a comprehensive record for each patient. The system contains information on diagnoses, visits to the doctors, tests, hospital treatments, prescribed medications, etc. What is more, in emergency situations doctors can use a patient's ID card to review time-critical information, such as blood type, allergies, recent treatments, on-going medication, or pregnancy.

Though it may look like a centralized national database, it actually retrieves data as needed from the various service providers, who may be using different systems themselves, and presents it in a standard format. As a result, the documentation process is streamlined, and health care providers have access to relevant information (including image files such as X-rays), which facilitates the delivery of high quality patient-centered health care. The system also compiles data for national statistics, so that relevant ministries can measure health trends, track epidemics, and make sure that national health resources are spent wisely.

The eHealth system also includes a Patient Portal, that gives patients access to their own records, as well as those of their children. By logging into the Patient Portal with an electronic ID, the patient can review their personal healthcare history, incl. name of their family doctor, past doctor visits and current prescriptions, and even receive general health advice.

BENEFITS

1. significantly reduced administrative bureaucracy for doctors
2. access to time-critical information in emergency situations
3. health care services are more patient-friendly
4. increased efficiency in the health care system
5. collection of data on health trends is automated

Procurement Initiative: Estonian eHealth Foundation (funded by the Ministry of Economic Affairs and Communications)
Further information: e-Health www.etervis.ee
Patient Portal www.digilugu.ee

e-Prescription

Since **2010**

The digital prescription is one of the key innovations in Estonia's cutting-edge e-health care system, and a survey conducted in 2015 revealed that the electronic prescription service was the most popular e-service among citizens.

The Digital Prescription Service is a centralized, paper-free system for issuing and handling medical prescriptions, which is done electronically via an online form. All hospitals and pharmacies in Estonia are connected to the system, and in 2015, over 95% of all prescriptions in Estonia were being issued electronically.

All the patient needs to do is to present their ID-card at the pharmacy. The pharmacist then retrieves the patient's information from the system and fills the prescription. The system draws on data from the Estonian Health Insurance Fund, and therefore any state subsidies that the patient is entitled to, are also available, and the medicine is also discounted accordingly.

Another major advantage of the system is that routine refills do not require visits to the doctor anymore. Patient can contact their doctor by e-mail, Skype or phone, and the doctor can issue refills with just a couple clicks of a mouse. This helps save time for both patients and doctors, and reduces the overall administrative burden.

BENEFITS

1. medical appointments aren't required for routine refills, saving time for both patient and doctor
2. patients don't need to keep track of paper prescriptions
3. reduced paperwork in hospitals and pharmacies

Procurement Initiative: Estonian Ministry of Social Affairs, Estonian Health Insurance Fund
Further information: www.digilugu.ee

Since **2014**

e-Residency

Estonia made history by launching the first supranational e-residency scheme in the world – a state-issued electronic ID for non-residents that allows secured authentication and digital signature of documents – thus moving towards the idea of a country without borders.

All e-residents receive a smart ID-card which provides digital identification and enables the digital signing of documents. The e-resident ID-card and services are built on state-of-the-art technological solutions, containing two security certificates: one for authentication, and another for digital signing. However, it is important to note that e-Residency does not confer citizenship, tax residency, residence or right of entry to Estonia or to the European Union. The issued e-Resident smart ID-card is not a physical identification or a travel document.

Estonia's first e-resident was Edward Lucas, senior editor at The Economist, who called the e-resident's card an "Estonian Express" that offers a degree of security, convenience and privacy unlike any other national ID-scheme. In a short period of time, thousands of foreign entrepreneurs, professionals and media figures have followed Lucas's example to become Estonian e-residents, among them Shinzō Abe, the Prime Minister of Japan.

Please follow e-residency in details from page 52.

BENEFITS

1. digitally sign documents and contracts
2. verify the authenticity of signed documents
3. encrypt and transmit documents securely
4. establish a company in Estonia online, and administer it from anywhere in the world
5. conduct e-banking and remote money transfers

Procurement Initiative: Estonian Ministry of Economic Affairs and Communications
Further information: www.e-estonia.com/e-residents, www.apply.e-estonia.com

BENEFITS

6

access different e-services

7

declare taxes online, NB! e-residency does not automatically establish tax residency.

* In Estonia, digital signatures and authentication are legally equivalent to handwritten signatures and face-to-face identification, and also between partners upon agreement anywhere around the world. Recent changes in EU law mean that within the next few years Estonian e-residents will be able to easily identify themselves, access online services, and conduct business across European Union.

Prime Minister of Estonia Taavi Rõivas and the Minister of Economy of Japan Akira Amari

E-Society Management

eGA Chairman of the Management Board Arvo Ott and Indian Ocean Commission Secretary General Jean Claude de l'Estrac

Since the 1990s Estonia has had remarkable success in information society development. The major factors that have affected the evolution of the information society in Estonia include the economic factors, the active role of the public sector, technological competency, and socio-cultural factors.

e-Society Management in Estonia

Modern technology contributes considerably to the facilitation of communication between citizens, businesses and the state. The state-level IT architects in Estonia often jokingly say that the public sector should proceed in its activities from the principle "Let us have less state". Indeed, the development of the information society has significantly reduced the need for citizens to turn physically to state institutions.

Moving towards e-Governance in daily public administration, however, requires extensive organisational and administrative changes, without which the expected benefits will remain just a dream. Formation of the Estonian information society was full of challenges. **Through the e-Governance Academy, Estonia shares its lessons with the world.**

Estonian Information Policy

Digital Policy Adviser at Government Office of Estonia Siim Sikkut

In Estonia, the development of the information society is based on the Principles of the Estonian Information Policy, adopted by the Estonian Parliament in 1998. These principles were reviewed and updated in 2006 in the course of preparing the Estonian Information Society Strategy 2013. Most of these principles remain relevant today:

• The development of the information society in Estonia is a strategic choice to improve the competitiveness of the state and to increase the overall well-being of people.

• The public sector leads the way in pursuing the principles for the development of the information society.

• The protection of fundamental freedoms and rights, personal data and identity will be ensured. Individuals are the owners of their personal data and will have an opportunity to control how their personal data are used.

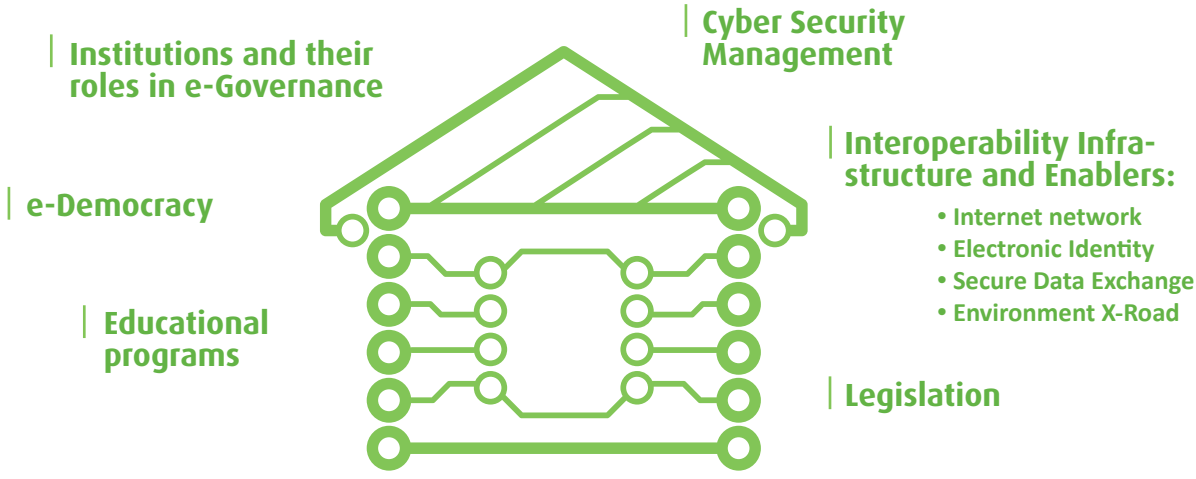
• The public sector will organise its processes so as to ensure that citizens, entrepreneurs and public bodies will have to provide any information only once.

• The information society will be developed in cooperation between the public, private and third sector as well as all with other parties, including the users of ICT solutions.

• When developing the information society, the continuity of the Estonian language and culture will be ensured.

• The information society will be created for all residents of Estonia, while particular attention will be paid to the integration of social groups with special needs, to regional development and to the strengthening of local initiatives. Everybody should have access to the internet.

The objective of further chapters is to share knowledge, best practice and competence on creating and managing the information society by developing widely accessible, relevant, innovative and sustainable cornerstones of e-Governance:



Main principles behind e-Estonia:

Ministry of Economic Affairs and Communication developed principles of information policies and supportive legislation, also took responsibility for supervision of relevant state organisations starting from 1993.

- **Centralised policy development**
- **Decentralised implementation**
- **Transparent and efficient public sector**
- **Neutrality of technological platforms**
- **Citizen / customer orientation**
- **Functioning model for protection of personal data**
- **Measures against digital divide**

e-Government developments are done mainly by responsible ministries and state agencies. Every government department, ministry or business, gets to choose its own technology, based on commonly agreed principles.

We help to increase government leaders' awareness and skills in all aspects of e-government, by focusing on e-government policy and planning issues, organisational and management frameworks, legal regulations, budgeting of ICT implementation, and basic concepts of e-government interoperability and architecture.

For more information on central e-government and change management, please contact Mr Arvo Ott.
E-mail: arvo.ott@ega.ee
Web: www.ega.ee

At the e-Governance Academy, we understand the vital role of regional governments in the development of e-administration and e-democracy. Local and regional governments are the closest governmental units to citizens in every country. They also provide the majority of public services. With this, local and regional governments can play an active role in the development of e-administration and e-democracy.

For more information on local e-government, please contact Mr Hannes Astok.
E-mail: hannes.astok@ega.ee
Web: www.ega.ee

Cyber Security Management

Cyber Security is one of the most important topics in Estonia. Estonia has developed its information society science 90' and has become highly dependent on its ICT infrastructure and electronic services. Therefore, Estonia has ensured that electronic solutions are not the Achilles heal for the society but vice versa, the enabler of digital innovation and smart solutions.

We use the term "Cyber Security" as a general word for digital data/information protection, personal data protection in electronic format, computer security, network security, e-services security, ICT security, cyber safety, etc.

Estonia has been set as an example of not only how to manage cyber incidents, but first of all, how to make electronic systems secure by design. Due to this approach Estonia has implemented a national electronic identity scheme, a legally valid electronic signature system and a secure data exchange environment X-Road for electronic services. These systems are fundamental for ensuring national cyber security at he highest possible level.

Estonian national cyber security arrangements allow public and private sectors and citizens to interact securely in a common data exchange environment while ensuring confidentiality and privacy. The result is that Estonia has thousands of e-services, which are accessible worldwide.

In 2007 the Estonian cyber security concept and implemented technologies were robustly tested in real life. Estonia experienced large-scale cyber attacks against its whole ICT infrastructure. Internet service providers were under attack as well as government websites and e-mail systems, online banking and other electronic services. The whole world witnessed, that Estonia survived without any significant damage. This proved that Estonian cyberspace is well protected and trustworthy.

Cyber Security is the enabler of rapid digital innovation.

Cyber security and the information society

In Estonia, Cyber Security doesn't exist in isolation. It is a fundamental part of information society development and supports the digital innovation. Cyber Security is not the brake, which doesn't allow digitalisation, but the enabler, which makes the rapid digital innovation possible.

With the implementation of basic cyber security measures as electronic ID and secure data exchange environment X-Road, Estonia has solved the fundamental security problem of the cyber environment. The X-Road system could be understood as the Estonian official territory in the cyberspace and electronic ID card as the passport to this virtual territory.

National Cyber security framework

We have developed a framework for national-level cyber security. This framework helps to understand how the cyber security area should be organised and roles and responsibilities shared. The Estonian national cyber security strategy from 2014 follows this concept.

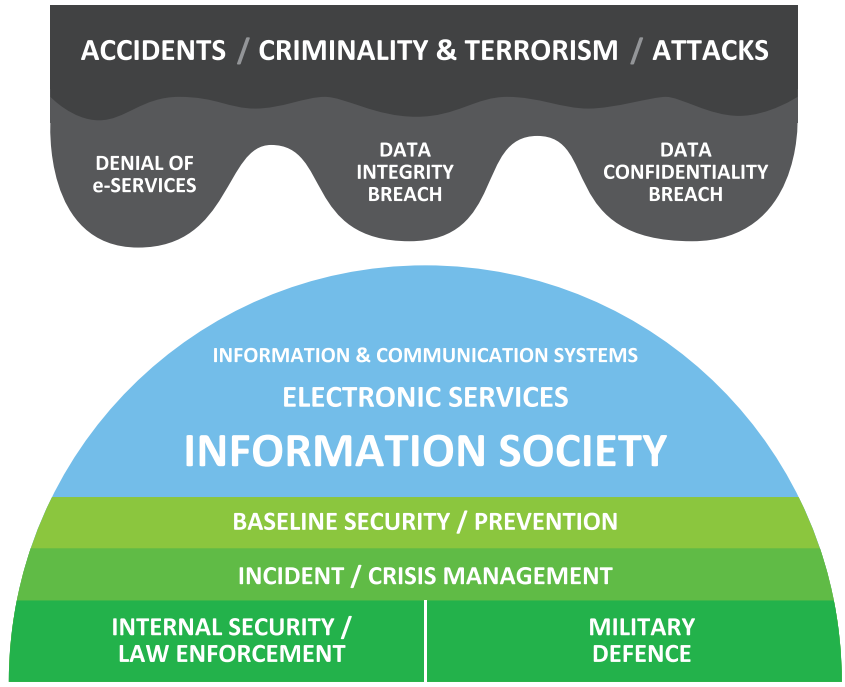
eGA Head of National Cyber Security Domain Raul Rikk

On the top of the figure, the fundamental cyber threats are presented:

- Denial of service – information services are not available if needed. *Example: large-scale cyber attacks against Estonia in 2007*

- Data integrity breach – data is modified in an unauthorised manner. *Example: the Stuxnet operation against an Iranian nuclear facility in 2010.*

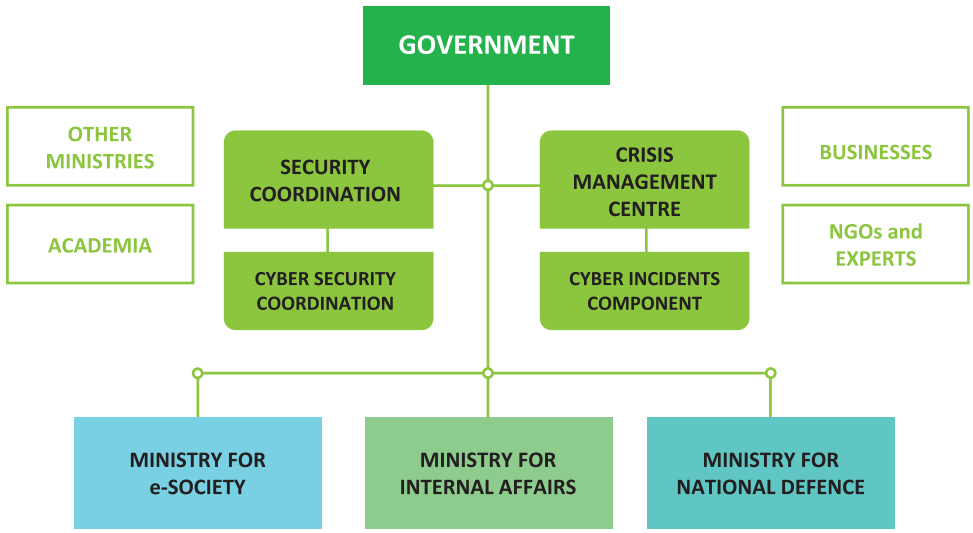
- Data confidentiality breach – data is available for unauthorised entities. *Example: WikiLeaks 2010 and the disclosures by Edward Snowden in 2013.*



Some of the incidents are simple accidents or technical failures. Other incidents might be organised by criminals or terrorists. Also, nation-states could use cyber offensive capabilities as part of special or military operations.

These threats directly affect the normal functioning of national information and communication systems and through the ICT systems, the electronic services (including critical e-services). The consequence is that the information society does not work properly and the country's governance efficiency, economy and lifestyle is harmed.

In order to manage these cyber threats, a country must have appropriate legislation and government entities that are responsible for baseline cyber security and incident management. Also the country needs legal acts and agencies for combating cyber crime and terrorism. In addition, the military should have specific legislation, units and capabilities for protecting national cyberspace.



X-road is the Estonian protected territory in the cyberspace and eID is the passport to that territory.

Cyber Security Highlights

X-Road

X-Road is the secure backbone of e-Estonia, the Estonian "protected territory" in the cyberspace. It's the environment that allows the nation's various databases, both in the public and private sector, to link up and operate in harmony. All of the Estonian e-solutions that use multiple databases use X-Road. All outgoing data is digitally signed and encrypted. All incoming data is authenticated and logged.

For more information, please see the X-road chapter.

eID and Digital Signature

Estonia has by far the most highly-developed national ID system in the world. The digital ID serves as the passport of Estonia's "territory" in the cyberspace, and access card for secure e-services. Estonians have an official ID-card and Mobile ID, which allow them to identify themselves in an online environment and give legally binding digital signatures worldwide. In Estonia, eID is actively used by 60% of population without a single security incident since its launch in 2002.

For more information, please see the eID chapter.

National Cyber Security Index

The National Cyber Security Index is a global index which measures countries' preparedness to prevent the realisation of fundamental cyber threats and readiness to manage cyber incidents, crimes and large-scale cyber crises.

The NCSI describes strategic measures which are necessary for securing public e-services, information and communication systems and the digital society in general. The NCSI could be used as a tool for national cyber security capacity building.

For more information,
please see the website www.ncsi.ega.ee

NATO Cooperative Cyber Defence Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence is an International Military Organisation located in Tallinn, Estonia with a mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

For more information, please see the website www.ccdcoe.org

How it works?

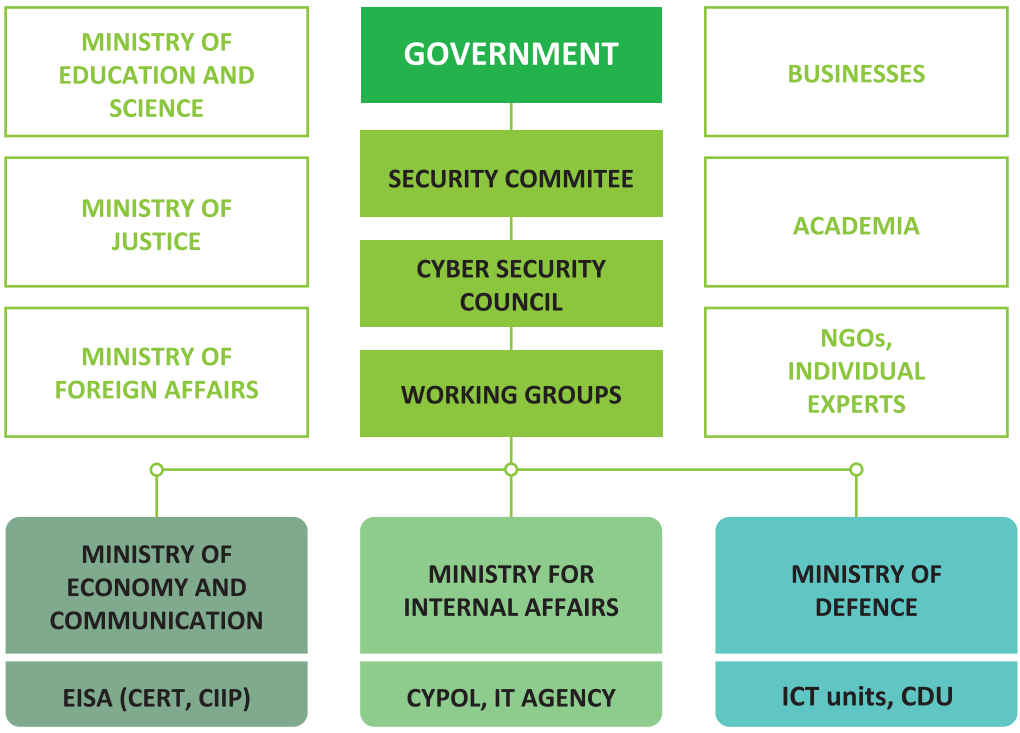
In Estonia, the most important cyber security roles and responsibilities are shared between the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, and the Ministry of Defence.

The Ministry of Economic Affairs and Communications is responsible for information society development and baseline cyber security. The national cyber security policy coordinator is placed in the ministry, at the department of state information systems.

The ministry has the State Information System's Authority, which is responsible for practical implementation of interoperability technologies and cyber protection. The national Computer Emergency Response Team is located at the Agency as well as the Critical Information Infrastructure Protection Unit. For further details, please see the chapter Institutions and Organisations

The Ministry of Internal Affairs is responsible for combating cyber crime. The ministry has different units for the fight against cyber crime and digital forensics. Also, the ministry has its own ICT Agency for police and national information systems. The ministry is also responsible for crisis management, including cyber crisis.

The Ministry of Defence is responsible for creating military capabilities. The Ministry has established the NATO Cooperative Cyber Defence Centre of Excellence and supports its administrative operations through the Estonian Defence Forces. Also, under the ministry, there is a voluntary military organisation Defence League. The Defence League is the home for voluntary cyber security experts. In Estonia the cyber volunteers are organised into the Cyber Defence Unit and they provide support during large-scale cyber incidents.



For national cyber security coordination, Estonia has established the Cyber Security Council. It works under the Government's Security Committee and deals with cyber security policy issues. In the council different state institutions, business entities, academic organisations and cyber security experts are represented.

How to start?

eGA provides various services for cyber security development. We focus on organisational, regulative and technical measures of national cyber security and provide best practice from around the world. We assist government and specific sectors in improving cyber security knowledge, developing policies and legislation, raising organisational and personnel capacity, and implementing security technologies.

We provide the following services for governments, ministries and organisations:

Policy Development

- Cyber Security Strategy and Implementation Plan
- Cyber Security Roadmap and Development Plan
- Specific Policy documents

Legislation Development

- Cyber Security legislation, regulations and guidelines
- Cyber Security standards and Baseline Security Frameworks

Organisational Capacity

- Organisational framework (structure, roles and responsibilities)
- CERT / CIRT capacity building
- Critical Information Infrastructure capacity building
- Crisis management system for cyber security
- Cyber Police capacity building
- Cyber Defence capacity building

Security Technologies

- Electronic Identification Scheme implementation (ID card, mobile ID)
- Digital signature system implmementation

Education and Awareness

- Cyber Security briefings and trainings (policies, frameworks, etc.)
- Course curriculum development for universities, schools and organisations
- Cyber Security exercises and drills (incident and crisis management)
- Awareness raising activities (demos, campaigns, events, materials)

Our products include policy documents, recommendation papers, consultancy, trainings and seminars, study visits for delegations, awareness raising events and materials, analyses and research papers, organisational change management and technology implementation.

For more information on cyber security, please contact Mr Raul Rikk.
E-mail: raul.rikk@ega.ee Web: www.ega.ee


Safari File Edit View History Bookmarks Window Help
EESTi
Gateway to eEstonia
My Data
Services
Topics
Contacts
Log in with mobile-ID
Contact
SAMSUNG

"Estonia ranks among the most wired and technologically advanced countries in the world."

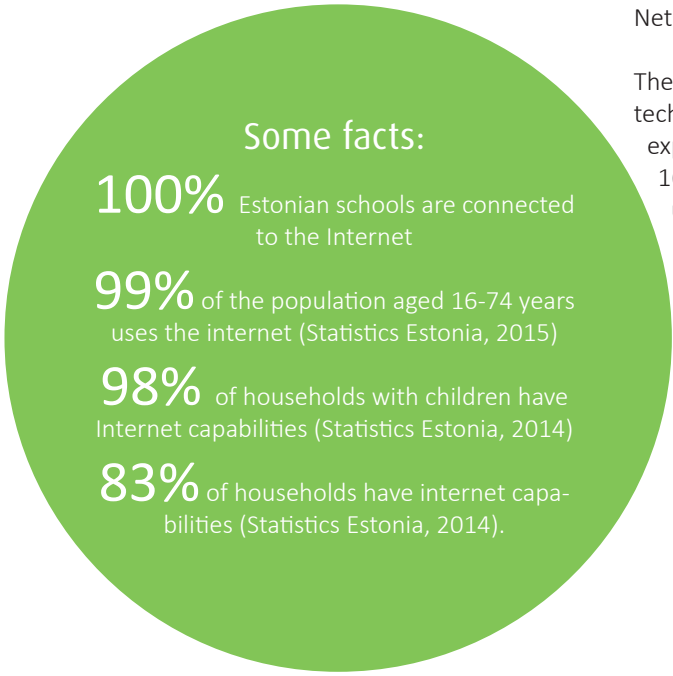
Freedom on the Net 2015

Interoperability Enablers

Introduction

Freedom House report "Freedom on the Net 2015" posits Estonia as one of the most wired countries in the world, with increasing internet access and online participation among citizens.

With a high internet penetration rate, widespread e-government services, and e-commerce, integrated into the daily lives of individuals and organisations, Estonia has become a model for free internet access as a development engine for society. Indeed, access to the Internet is considered a human right in Estonia. Certified WiFi internet connections are available in thousands of public places, and Estonia is completely covered by digital mobile phone networks (3G and 4G mobile broadband coverage). The area of WiFi internet is constantly growing and encompasses all of Estonia: www.wifi.ee



In Estonia, the first internet connections were introduced in 1992 at academic facilities in Tallinn and Tartu. The national telecommunications monopoly was subsequently privatised with the inclusion of Finnish and Swedish telecommunication companies, and a fibre-optic backbone was built with modern fixed and mobile communications services. The government continued collaborating with private and academic entities, which led

Estonia is completely covered by digital mobile phone networks (100% advanced 3G mobile broadband coverage)

to the Tiger Leap initiative launched in 1996, which aimed to bring computers and Internet connections to all Estonian schools by 2000. This program helped to build a general level of technological competence and awareness of the importance of ICT among Estonians. Ref: Freedom House report "Freedom on the Net 2015"

The advances made in the field of information technology have facilitated the increasingly exponential use of the Internet. Among 16–24-year-olds the share of Internet users has already reached 100%, and the number of Internet users among the elderly is on the increase as well. (Statistics Estonia).

Share of internet users among population

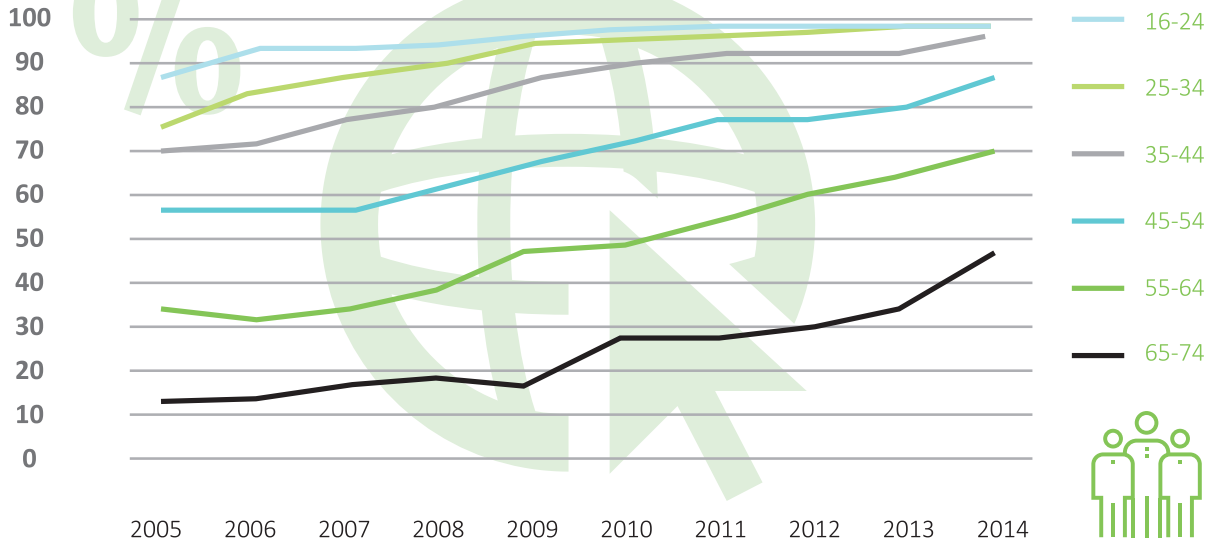


Figure above depicts the share of Internet users in the Estonian population by age groups, and the changes that have occurred during the last 10 years.

Nowadays, computer studies are introduced quite early on in Estonian general education schools. On one hand, young people have always shown greater interest in Internet use than the older generations. On the other hand, the share of Internet users among people aged 65–74 remained low although IT equipment was already widely used at the time and Internet service was available in most regions of Estonia. Year after year, the population aged 65–74 has also begun to use the Internet more actively. This has been facilitated by the decreasing service costs, and the general convenience of using e-services. As of 2009, the delivery of pension payments is made only digitally to the recipient's bank account, which may have also contributed to the increased usage of internet banking services by the elderly. Family support is important as well: often the elderly learn to use a computer and the Internet with the help of younger family members or relatives (e.g. children, grandchildren). (Reference: Statistics Estonia)

Over the past years, the issue of ensuring the privacy of individual users on the Internet has become a hotly debated topic in Estonia, with a particular focus on the privacy policies of global service providers. The Digital Agenda 2020 for Estonia, formulated by the Ministry of Economic Affairs and Communications, outlines how both technological and organisational conditions will be developed to ensure that people will always know and be able to decide when, by whom, and for what purpose their personal data is being used in the public sector. By 2020 all residents of Estonia will have access to fast (30 Mbit/s or faster) Internet, with at least 60% of households using ultrafast (100 Mbit/s or faster) Internet on a daily basis. (Reference: MKM, Digital Agenda 2020)

Broadband Networks

The new general broadband network generally consists of three parts:

- **nation-wide base network**
- **regional base network**
- **access network**

The nation-wide base network connects the regional base networks in cities and larger centres. The equipment utilised in the nation-wide base network makes it possible to transport and exchange information between different locations and different operators. The devices of end-users are not directly connected to the nationwide base network. Nationwide base networks are constructed using fibre-optic cables and usually with duplicate circles to guarantee sufficient transmission capacity and performance, so that connections are automatically rerouted in case of cable faults and there are no interruptions.

Regional base networks connect the access networks in one specific region (eg. city or a certain rural area) with the nation-wide base network. It is the connecting link between the access network and the nation-wide base network. The regional base network also connects the network devices in the region to each other, thereby allowing for data communication traffic between them. Similarly to the nation-wide base network, regional base networks are also based on fibre-optic cables and are often created as circles to guarantee there are no interruptions in case of faults.

The access network is the part of the network that is the closest to the end-consumer and connects the consumer's devices to the connection point of the nearest regional base network. Access networks utilise different devices and technologies, and their transmission capacity, quality, user-friendliness, accessibility, etc. differ considerably. Access networks can be divided into two: wired networks and wireless networks.

Wired Networks

- Over the last couple of decades' various technologies (eg. xDSL, vectoring, GFast) that make it possible to transport more data with higher quality through copper cables have been in constant development. As a result, the transmission capacity of copper cables has increased manifold. Unfortunately, this development has now reached the stage where the laws of nature come into play and further increases in data transmission capacity via copper cables over long distances is no longer possible.

- The spread of the Internet has also led to the adoption of technologies that make it possible to transport data via cable-TV networks (eg. coaxial cable). This technology created competition for historical telephone companies in regions that had a cable-TV network. Coaxial cables boast a bigger transmission capacity than copper cables, but a cable-TV network is a network shared between consumers in terms of its structure. This means that in contemporary cable-TV networks, coaxial cables are mainly used in networks inside blocks of buildings. All parts of networks located outside buildings have been replaced with fibre-optic cables. Data transmission technologies have also developed rapidly and cable-TV companies are currently offering excellent broadband connections to end-consumers.

- The access network with the biggest transmission capacity and the best quality is based on fibre-optic cables. The limits of the transmission capacity of fibre-optic cables cannot yet be foreseen, as laser technology keeps developing and coloured light can transport increasing amounts of information. There are several types of optical cable-based access networks and their common name is FTTX (fibre to the x). The most perfect optical cable access network is such where a direct fibre goes to the consumer from the network device of the base network, i.e. FTTH (fibre to the home).

Wireless Networks

Wireless access networks are mainly meant for connecting the mobile devices of end-consumers. Wireless technology is also used to connect buildings in places where the construction of infrastructure for a wired network is impossible due to natural, economic or other reasons. The main advantage of a wireless network is that it's convenient to use.

Several different technologies are used. Some technologies (eg. Wimax, WiFi, CDMA) enable the so-called point to multipoint connection, which means that there is a base station on a mast that can be used by several users at the same time. Some technologies (eg. radio links), however, enable point to point connection. Radio links need direct visibility, which means that using them in the midst of forests and mountains may be problematic.

Mobile wireless access connections or mobile networks are mainly meant for connecting the portable devices of people (eg. mobile phones, tablets, etc.) to the internet. Mobile network technologies are in constant development and keep coming up with better connections. Today, new mobile communication generations (eg. NMT, 2G, 3G, 4G, 5G) are upgraded more frequently than ten years ago. Radio waves guarantee data communication in mobile networks. There is only a limited number of radio waves that fit in the air so that they will not interfere with each other, and therefore an international agreement has been concluded regarding the radio frequencies that may be used for mobile communication.

A new generation broadband PPP project can be divided into the following stages:

Establishment of goals

Mapping out the existing situation in broadband infrastructure, market, services, competition, etc. and forecasting demand, market and technological developments.

Creation of models,

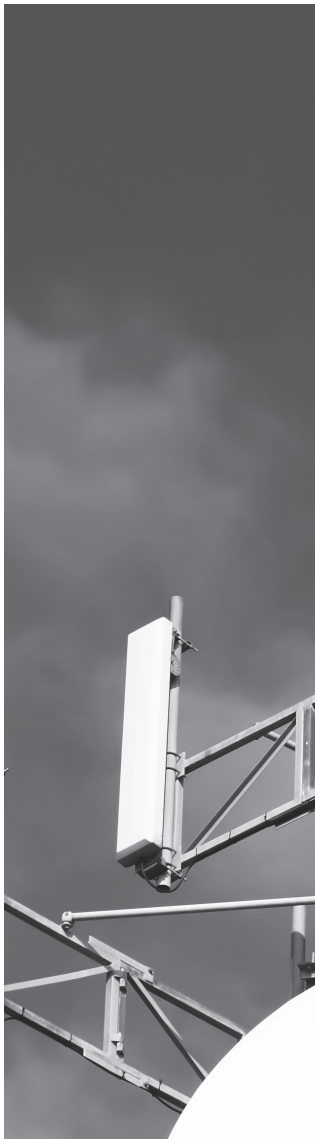
which must be based on a clear understanding of the desired extent of market intervention and the risks to be taken. Subsequently the decision on the type of intervention can be made, including about the level on which intervention will occur - will it be the wholesale market (infrastructure and connection level) or retail market (service level), and the extent of the project (nationwide, regional, complete network, base network or access network).

Business plan and financing

The project can be implemented on the basis of a long-term business plan. Although earning direct monetary profit may not be the goal of PPP projects, a business plan is the basis of both financing as well as operation. A financing package of network user fees, grants and long-term loans must be assembled in order to finance the project.

Action plan and implementation

The action plan must cover detailed network planning, organisation of construction and marketing activities. Project supervision, result monitoring and the procedure for making potential changes must also be agreed on right at the start of the project.



How to start?

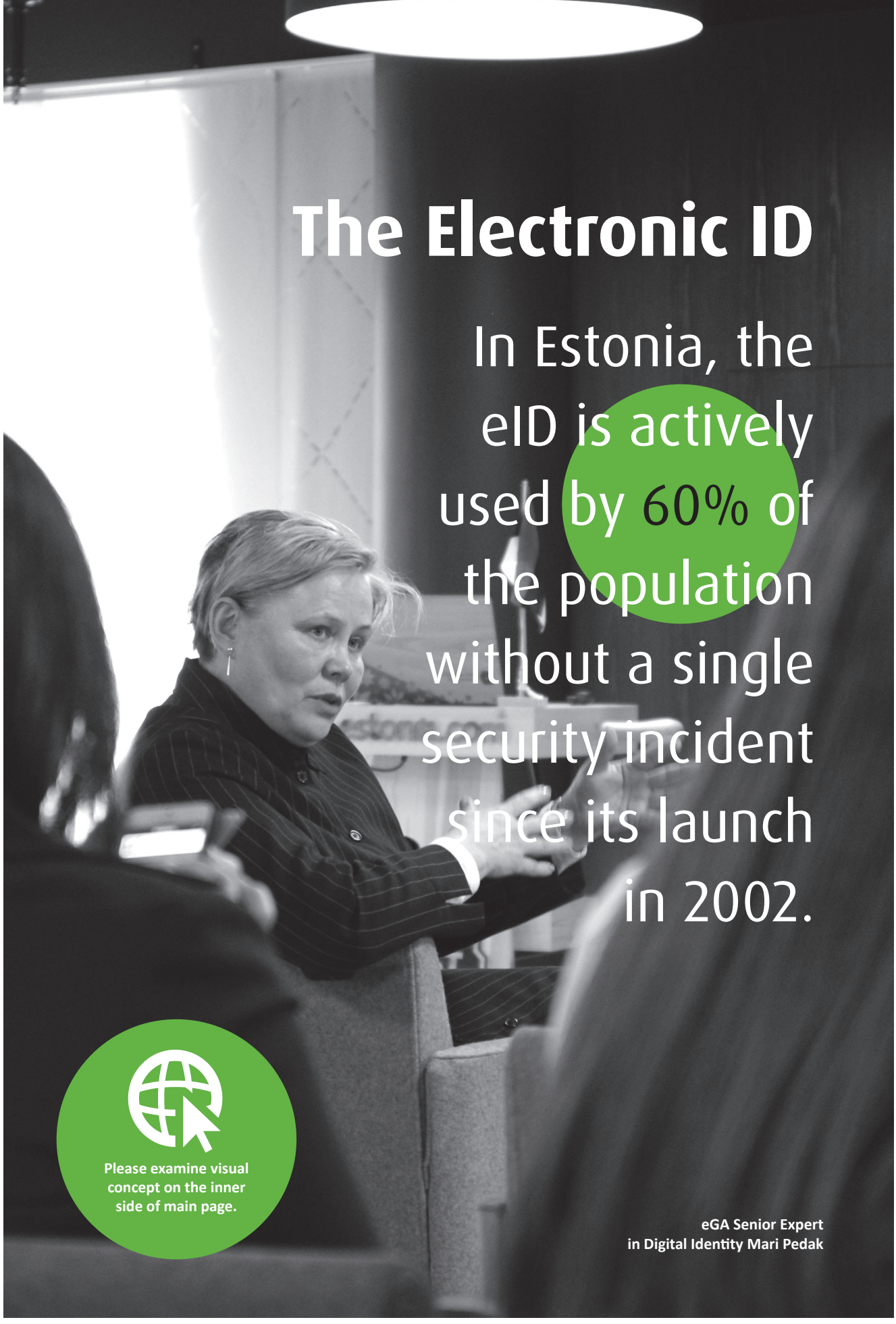
Many country leaders have come to the understanding that broadband cannot be offered to all people and companies without the intervention of the public sector. However, past lessons have taught us that excessive state intervention is not beneficial for the overall development, because it decreases the motivation of the private sector.

The public sector must have an excellent overview of broadband development and the plans of the private sector. In general, the intervention measures of the public sector should increase competition, i.e. it is necessary to avoid the situation where the principles of a free market are sacrificed for the benefit of achieving rapid results. Market intervention by the public sector should follow the principle of less is more or as much as necessary, but as little as possible.

Modern ICT regulation is built around the understanding that developments are mainly market-driven and all necessary agreements (on interconnection, access, infrastructure sharing, etc.) are made primarily through agreement between market participants. However, in order for this to work, it is important that there is a regulator with powers to intervene if and when necessary. In addition, a universal service obligation is stipulated by law in all EU Member States and many other countries, to ensure that basic services are available in all parts of the country at reasonable conditions.

In Estonia, several discussions have been held by the executive, and legislative branches, small and large operators, and local authorities. All parties have different interests, and consequently also different opinions. In order to make a public-private partnership project in broadband development a possibility, it is necessary to reduce opposition and look for opportunities for collaboration.

A reasonable option would be the drafting of the broadband development plan by an independent organisation, such as the e-Governance Academy. The plan should include proposals for the creation of the environment required for broadband development, suitable models, financing options and different support measures considering the local situation.



The Electronic ID

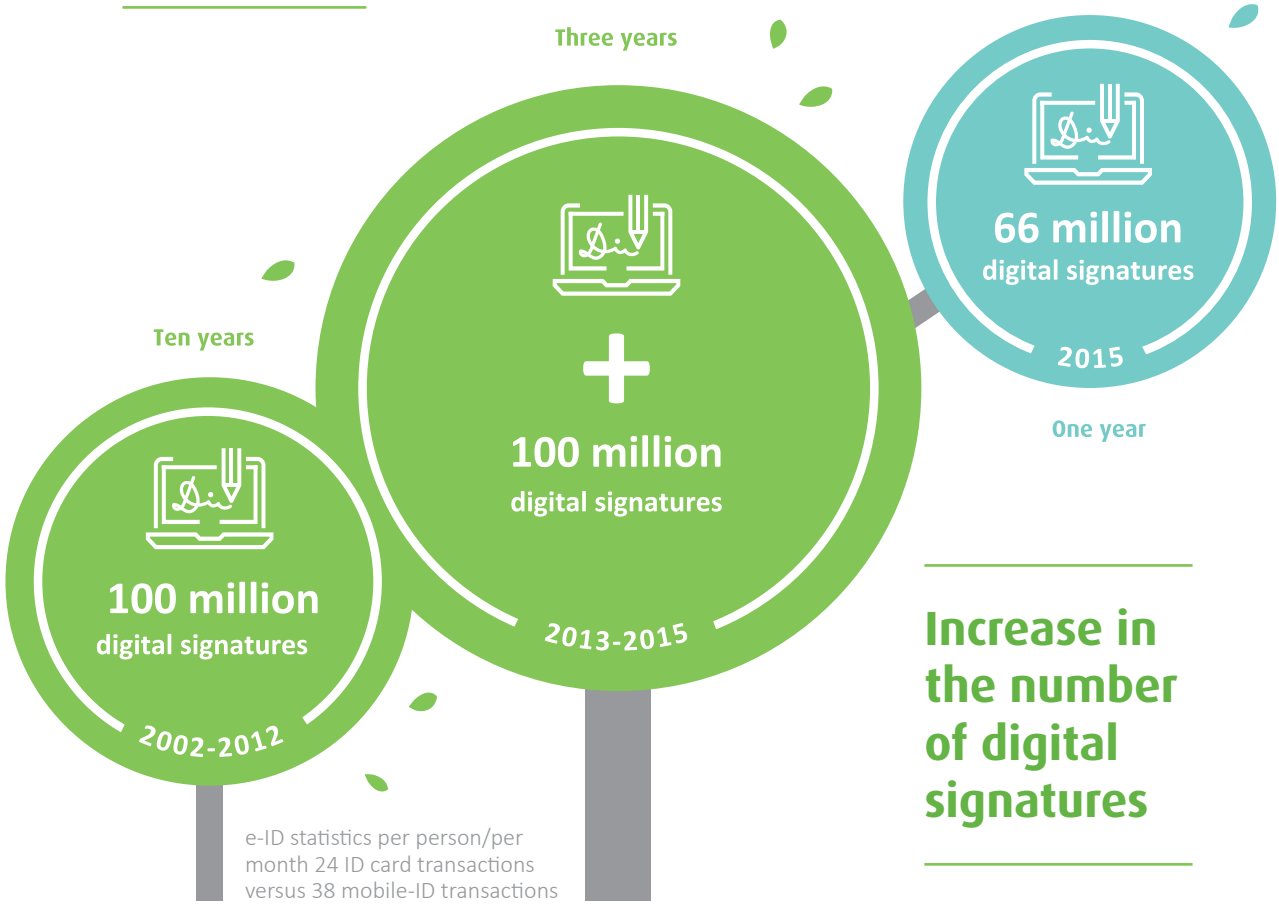
In Estonia, the eID is actively used by 60% of the population without a single security incident since its launch in 2002.

Please examine visual concept on the inner side of main page.

eGA Senior Expert in Digital Identity Mari Pedak

Estonia has a comprehensive system for electronic identification, authentication, and digital signing which includes the following elements:

- **ID-card**
- **Digi-ID**
- **Mobile-ID**
- **digital stamp**
- **residence permit card**
- **e-residency card**



Increase in the number of digital signatures

In Estonia, the use of the eID is regulated by the Identity Documents Act and the Digital Signatures Act, replaced by EU regulation eIDAS. It is essential that digital signatures are legally binding as hand-written signatures. At the EU level, in 2014 a Regulation on eID was adopted (Regulation 910/2014) which repeals Directive 1999/93/EC. Regulations are directly applicable for all Member States, and the aim of this specific regulation is to enable harmonisation to such an extent that electronic identification can be accepted in all EU Member States.

Personal Identification Code

In Estonia the identity of a person is based on a permanent individual ID called the Personal Identification Code (PIC), which was introduced in 1992. The PIC is generated in accordance with the Estonian Standard EVS 585:2007 „Personal Code. Structure", the Population Register Act and a regulation on the generation of PICs. Pursuant to the Population Register Act, the personal identification code is a unique combination of numbers formed on the basis of the person´s sex and date of birth, that allows for the identification of a specific person.

All certificates contain the PIC. The PIC is used as a primary key in the majority of databases containing personal information, both in the public and private sector.

Moreover, digitally signed files contain a certificate of the signatory (which in turn contains their PIC), which allows for a definite identification of the signatory.

The data on the ID-card (i.e. the data file and certificates) is available to every card terminal as they are not read-protected. The authentication certificate is available to the service provider upon a successful login. The digital signature certificate is available in the digitally signed document to everyone who sees the document. As a result, the PIC in the data file or in the certificate is made available with every electronic use of the ID-card.

As of June 2016, the digital documents bearing the electronic identity of Estonian residents are plastic cards (ID-card, Digi-ID, e-residency card, residence permit card) and mobile phone (Mobile-ID).

Public Key Infrastructure (PKI)

The public key infrastructure (PKI) enables secure digital authentication and digital signing. The infrastructure also provides means for secure data transfer by using encryption. Estonia uses a national PKI, meaning that the state undertakes to assure the existence and functioning of the public key infrastructure. Although a large part of the services related to the PKI are purchased from the private sector (e.g. certificate issuance, certificate validity information, distributing the public key); as well as preparing the key generation environment (e.g. chip of carriers of ID-card type, SIM card) and personalising the documents (carriers of ID-card type), the most important aspects related to the PKI are still handled by the state:

- Police and Border Guard Board: issuing personal (digital) identity documents enabling secure electronic authentication and digital signing (ID-card or another smart card).
- Ministry of the Interior: drafting legislation that determines the types and requirements for the digital identity documents.
- Information System Authority (RIA): development of software applications necessary for using the PKI (ID-card middleware including drivers, utility and client software).
- Ministry of Economic Affairs and Communications (Department of State Information Systems): determines the quality and reliability requirements of PKI services.

The Estonian eID features also the provision of a unique state-issued e-mail address allocated to each card holder. There are currently two formats personalidentificationcode@eesti.ee or firstname.lastnameNNNN@eesti.ee, where NNNN represents a sequential number to provide uniqueness if there are several citizens bearing the same name. This e-mail address is intended as a lifetime address. It is not associated with a real e-mail service but is rather a relay address forwarding mails to the holder's 'actual' address. These e-mail addresses are publicly available through Estonia's National Registry of Certification Service Providers' certificate directory.

Since **2002**

ID-Card
General Overview

The ID-card is the only mandatory ID document in Estonia. Thus far, ID-cards have been issued to more than 1.2 million active users, which makes up nearly 94% of Estonia's 1.3 million residents. This makes the Estonian system the most used national ID-card system in the world

The ID-card aso has a digital supplement called the Digital-ID (Digi-ID), which is a state issued digital document for electronic identification and providing digital signatures. Unlike the ID-card, the Digi-ID is not designed for visual personal identification; therefore, it does not carry a photo or any physical security elements – simply the person´s name, personal identification number and end of validity date. Electronically and cryptographically, it is identical to the ID card, and in electronic environments they are treated as equivalent certificates.

The ID1-shaped documents- defined by ISO/IEC 7810 standard - are based on PKI technology, and incorporate two certificates: one for authentication, and the other for digital signatures. Each private key is dependent on the use of a different PIN-code. In addition, the card also contains a single user-readable data file, replicating data from the visual layer. There is no electronically usable biometric information on the card.

Chip Features

The Estonian ID-card serves as the digital access card to all secure e-services offered in Estonia. The chip on the card carries embedded files which, using 2048-bit public key encryption, allow for it to be used as definitive proof of ID in an electronic environment. It can be used for personal identification, signing documents digitally and for data encryption functions. The ID-card requires a special card-reader, for digital signatures special DigiDoc software is also required. (Reference: eid.eesti.ee)

ESTONIAN ID-CARD

CHIP
The chip on the card carries embedded files which, using 2048-bit public key encryption, enable it to be used as definitive proof of ID in an electronic environment.

THE FRONT SIDE OF THE CARD CONTAINS THE FOLLOWING INFORMATION:
- card holder's name
- card holder's signature and photo
- unique personal identification code (national ID-code)
- date of birth
- gender
- citizenship
- card number
- date of expiry

THE REVERSE SIDE OF THE CARD CONTAINS THE FOLLOWING INFORMATION:
- card holder's place of birth
- date of issue
- residence permit details (if applicable)
- card and holder data in machine ● readable format (except for the photo and signature)

THERE ARE TWO CERTIFICATES saved on the ID card
1) a certificate for digital personal identification and data signing and encryption;
2) a certificate for digital signing, enabling the cardholder to issue a digital signature.

THE REVERSE OF THE CARD CONTAINS:
An ID card issued before 1 January 2007 is valid for 10 years and the certificates on it are valid for three years. Upon expiration, certificates can be renewed without charge. On ID cards issued after 1 January 2007, the certificates are valid for as long as the card itself, i.e. five years, and there is no need to renew the certificates.

Certificates and Validity

The ID-Card contains two certificates (standard X509v3 certificates):

1) a certificate for digital personal identification, data signing and encryption;
2) a certificate for digital signing, enabling the cardholder to generate a digital signature.

The ID-card along with corresponding certificates is issued for five years, and there is no need to renew the certificates. Digi-ID and its certificates are issued for three years. Reference: eid.eesti.ee.

The Process of Issuance

The ID-cards are issued in close public-private partnership. There are three main organisations who are associated with issuing and operating the ID-card and the associated infrastructure: Police and Border Guard Board is the government agency responsible for issuing personal identification documents to Estonian citizens and other residents, as required by the Identity Documents Act. Certification Centre (AS Sertifitseerimiskeskus, SK) functions as CA, maintains the electronic infrastructure necessary for issuing and using the card, and develops the associated services and software. Trüb Baltic AS (subsidiary of Gemalto AG) is the company that personalises the card in the territory of Estonia.

The main steps in ID-card issuing process include:

- **personal application**
- **identity verification (when applying for the first time personal appearance is mandatory)**
- **personalisation and activation of certificates**
- **issuance and handing over**

While according to the law the issuing of an ID-card may take up to a month, the Digi-ID cards are issued within 30 minutes from the service offices of the Police and Border Guard Board. (Issuance process as of June 2016) (Reference: https://www.politsei.ee)

Digi-ID – How to start?

The Estonian e-Goverenance Academy, in cooperation with its partners, offers a full-package service to pilot an electronic identity solution. Our service will take care of all the complicated processes for you, and allows you to test drive the Estonian Digi-ID solution which boasts the highest application rate per citizen in the world.

Piloting Electronic Identity

The scope of the pilot project is to introduce and explain the concept of electronic identity and its application to a selected test-group. Parties agree on the numbers of plastic cards to be issued in the framework of the pilot project, and the relevant application shall be loaded onto the chip during the pre-personalisation stage.

Subsequently the plastic card will be personalised both physically and electronically. The level of physical personalisation depends on the technical and the practical point of view. The electronic personalisation entails the generation of two asymmetric keys: one for authentication, one for digital signature. The public part of the keys shall be certified by the Certification Centre based on specific certification requests. Test certificates are loaded onto the smart card chip and also stored in the system.

The Digi-ID Pilot Package includes:

- market ready solution: the best way to find out how Digi-ID works
- duration: 2-3 months
- piloting includes:

mapping the market situation
training the test-group and service providers
compilation of Digi-ID implementation blueprint
support for PR actions
full project management

Getting started:

- local partner provides data on test-group
- choosing one e-service integration to access securely with Digi-ID or possibility to use customised demo portal for testing both authentication and digital signature
- test certificates are issued
- plastic cards are produced
- 24/7 customer support

For further information, please contact Mrs Mari Pedak
mari.pedak@ega.ee

Mobile-ID
General Overview

Originally introduced in 2007, the Mobile-ID is an electronic personal identification document that can be used for electronic personal identification and digital signatures with a mobile telephone.

In this configuration the mobile phone with its SIM card functions simultaneously as an ID card with an ID-card reader.

Since **2007**

The Mobile-ID becomes operational after it has been activated in the electronic application environment administered by the Estonian Police and Border Guard Board. Unlike the ID-card, the Mobile-ID cannot be used for document encryption, only for accessing secure e-services and generating digital signatures to documents. However, it has the advantage of not requiring a special card reader.

In 2007, the Estonian Mobile-ID solution was awarded "Best New Product" by Innovation Center InnoEurope. In 2011 the Mobile-ID was promoted to the status of national electronic ID document in Estonia, which means that the Mobile-ID can be used on an equal basis with the ID-card (Reference: eid.eesti.ee, Baltic IT&T Review" ISSN 1691-4694).

Chip Features

The Mobile-ID requires a special SIM card that enables the service. SIM cards with Mobile-ID readiness must fulfil the following requirements:

- **Javacard 3.0.4**
- **Java Transaction 0F82 Bytes**
- **Java Stack Default 01F0 Bytes**

Private keys are stored on the mobile SIM card along with a small application for authentication and digital signing. SIM cards are furnished with special Mobile-ID Applets during production (applet size is 39912 Bytes). The Estonian PKI-based Mobile-ID solution corresponds to the following security crypto algorithms: ECC, SHA2. Evaluation level: EAL4+ (Reference: SK.ee)

eGA Project Manager
Triin Rast

Certificates and Validity

The Estonian Certification Centre (SK) generates two certificates for Mobile-IDs (standard X509v3 certificates):

1) certificate for digital personal identification
2) certificate for digital signing, enabling gerenation of digital signatures

Unlike other documents, the Mobile-ID certificates are not saved on the SIM card. The Mobile-ID certificates are valid for three years, and when they expire, the SIM card has to be replaced. (Reference: SK.ee and politsei.ee)

The Process of Issuance

The process of issuing a Mobile-ID, as well as its further operation, is carried out in a close public private partnership. There are three main organisations in Estonia that are involved in issuing and operating the Mobile-ID and the associated infrastructure.

- **Police and Border Guard Board i**s the government organisation responsible for issuing identification documents to Estonian citizens and other residents, as stipulated in the Identity Documents Act.

- **Certification Centre** (AS Sertifitseerimiskeskus, SK), maintains the electronic infrastructure necessary for Mobile-ID

- **Mobile Network Operators** (MNOs, eg. Telia, Tele2, Elisa) – all leading MNOs in Estonia offer SIM cards with Mobile-ID capabilities.

Mobile-ID – Where to Begin?

The Estonian e-Goverenance Academy, in cooperation with its partners, offers a full-package service to pilot a Mobile-ID solution. Our service will take care of all the complicated processes for you, and allows you to test drive the Mobile-ID solution and generate digital signatures in any country.

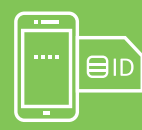
eGA Mobile-ID Pilot Package includes:

- market-ready solution: the best way to
- find out how Mobile-ID works
- duration: 2-3 months

Getting started

- local MNO provides information on SIM vendor
- test SIM-cards include SIM Applet (supported by all leading card producers)
- one e-service integration in order to test secure access with Mobile-ID
- portal for testing digital signature
- Estonian internal infrastructure is used during pilot and public testing

For further information, please contact Mrs Sandra Roosna sandra.roosna@ega.ee



The process of obtaining a Mobile-ID

- one mandatory personal appearance (+ valid ID-card)
- Mobile-ID agreement (signed with an Estonian MNO)
- SIM-cards are issued by all leading MNOs in Estonia
- card holder inserts ID-card or Digi-ID into the card reader and enters Estonian Police and Border Guard Board website for filing an application for a Mobile-ID
- the application is processed and the activation of certificates is completed on the Police and Border Guard Board website

The issuance procedure of Mobile-IDs is in line with the Estonian Digital Signatures Act and the EU Regulation 910/2014 on the Community Framework for E-signatures.

e-Residency

The Republic of Estonia is the first country to offer e-Residency — a transnational digital identity available to anyone in the world interested in administering a location-independent business online.

What is more, e-Residency enables access to secure and convenient e-services that facilitate integrity and reliability online.

NB! e-Residency is not equivalent to citizenship or permanent residency. It does not guarantee the right to vote in elections, nor does it give permission to enter Estonia or the European Union without a visa. Please bear in mind that e-Residency is a privilege, not a right, and therefore, Estonia shall screen all applicants and reserve the right to refuse applications.

First results are impressive:

- over 10 000 e-Residents from 130 countries
- over 600 new companies established by e-residents

Steve Jürvetson, Tim Draper and Prime Minister of Estonia Taavi Rõivas

Main Features

The e-Residency card is based on the Estonian Digi-ID solution, i.e. the official national digital document for personal identification in an electronic environment and for generating digital signatures. However, unlike the ID-card, the e-residency card is not designed for visual personal identification.

Electronically and cryptographically, the Digi-ID is a smart card identical to the ID-card. Therefore, when issuing a Digi-ID certificate, the Certification Centre uses the same general principles, certification policy and certificate profile as with Estonian national ID-cards.

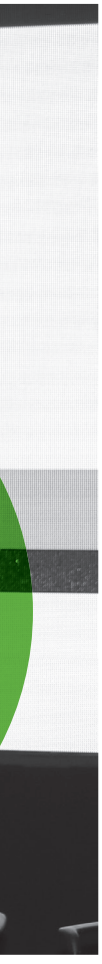
The Process of Issuance

The application for the e-Residency card can be submitted personally at Estonian Police and Border Guard Board service bureaus, at foreign representations of the Republic of Estonia, by post or by e-mail.

The decision to issue a Digi-ID card for an e-Residency applicant shall be made within 30 working days. For security purposes, the applicant must provide their fingerprint upon receipt of the card, in order to link a particular individuals to their digital data.
(Reference: Police and Border Guard Board).

Certificates and Validity

The e-Residency card and its certificates are issued for a duration of three years. The card lists the card holder´s name and issued personal identification code, along with the document number.



The Digi-ID application must include the following documents:

- **application form (online fill-out possible; or print and fill out on paper)**
- **national identity document or a copy of the document if application is submitted by post and by e-mail**
- **colour photo (min. 40x50 mm or 600x800 pixels (JPG)**
- **receipt certifying payment of application fee**
- **free-form written explanation regarding the purposes for applying for the Digital-ID and the circumstances of its use (holders of a service card or diplomatic card exempt)**
- **in case the applicant is an diplomatic officer, they must additionally provide relevant credentials**

Digital stamp

The digital stamp is a service that allows legal persons (e.g. companies) sign documents digitally.

The digital stamp confirms that the document comes from the company that has signed it (i.e. the digital document is confirmed by the institution, not by an authorised physical person.

Signatures can be attached (also in large quantities) to invoices, payment orders, confirmations, certificates, bank statements, etc. Digital stamp is available on USB crypto-stick that has an X.509 certificate (the area of application shall be determined by the name of the certificate). The issuing process and evidential value of the digital stamp are regulated by law (Estonian Digital Signatures Act), certification policy (specific to the respective certification service, and more detailed) and more general certification principles.

Advantage:
people come and go,
institutions remain.

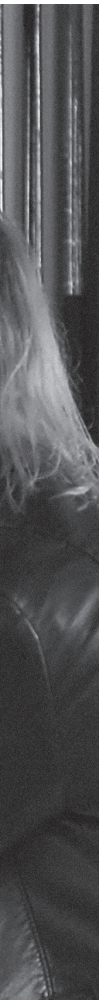
The Process of Issuance

The digital stamp certificate is issued to the authorised representative of the institution on a smart card or crypto-stick. The use of the digital stamp is similar to the ID-card, because the document is furnished with the time of giving the stamp certificate and the validity information. The digital stamp solution can be integrated into most information systems. (Reference: SK.ee)

eGA Project Manager Martin Lään and Assistant of the Management Board Evelin Sõluste

Digital Signature Tool

The DigiDoc Client, a piece of software included in the eID package, is a system that's widely-used in Estonia for sharing and digitally signing documents. Because in Estonia, digital signatures carry the same legal weight as hand-written signatures, a secure, easy-to-use platform is needed to give government agencies, businesses and private persons a way to transfer files.



BENEFITS

1

faster exchange of documents => improved cash flow

2

reduction of direct and indirect business expenses

3

security provided by timestamping and certificates => reduced risk of forgery and fraud

How it works?

Every eID user can upload any document, sign it digitally, and send it to other parties. While the users have the DigiDoc software, the e-service providers use software called DigiDocService. The DigiDocService is a SOAP-based web service which enables furnishing an e-service or an application with such funcitionalities as personal identification, digital signatures, signature identification and Mobile-ID.

Furnishing solutions with ID-card and Mobile-ID functionality is simple and allows for:

- digital signatures using an ID-card (or another smart card)
- identification and digital signing using Mobile-ID
- verification of certificate validity (identification via ID-card or another smart card)
- creation of digitally signed files
- verification of content and signature validity for digitally signed files (DigiDoc).

The basic software components used for digital authentication are publicly available to all developers. Any organisation can therefore build applications and business processes based on the eID card as the central identification device. This has resulted in widespread adoption of the functionalities of the ID card.

The Estonian Certification Centre conducted a cost-benefit analysis of digital signing, which showed that it entails remarkable financial benefits, eg. by replacing handwritten documents with digitally signed ones Estonia has saved over 200 million euros.

TRY OUT

Calculate your prospective savings:

- **Digital signature cost-profit calculator www.eturundus.eu/digital-signature**

- **Digital document cost-profit calculator www.eturundus.eu/digital-document**

These calculators are helpful tools for institutions and companies who sign contracts with their clients, partners and suppliers or exchange other formal documents (subscriptions, acts, invoices, etc). (Reference: www.sk.ee)

Customer support

The customer support is organised by the Estonian Certification Centre (Sertifitseerimiskeskus AS, SK). The main channel for all eID, and Moblie-ID related questions is the 24/7 helpline service.

The Certification Centre provides the following additional services in its customer service points:
- verification of certificates
- activation of certificates (termination of suspension)
- suspension of certificates
- revocation of certificates
- change of PIN codes

Information channels:
- Police and Border Guard Board www.politsei.ee/en
- e-Estonia website: www.e-estonia.com
- ID-card help centre www.id.ee
- Mobile-ID help centre www.mobiil.id.ee

Customer service points
- Police and Border Guard Board
- banks: Swedbank, and SEB

Main Actors

On the political level, two major Estonian ministries are involved in the development of eID:

Ministry of the Interior (MoI) is responsible for the legal framework regulating identity documents. In addition, it is also the authority supervising the Police and Border Guard Board, directly responsible for issuance and maintenance of identification documents, and for maintaining electronic identities of residents at large.

Ministry of Economic Affairs and Communications (MEAC) is responsible for the legal framework and implementation of the Digital Signatures Act and eIDAS regulation, as well as and is supervising the Informarmation System Authority (ISA), that coordinates the development and administration of the national information system, to help the state provide the best possible electronic services to citizens in a secure environment.

- RIHA, responsible for administrating the state information system, guarantees the transparency of the administration of the national information system and helps to plan national information management.
- The State Register of Certificates, functioning under the MEAC, is a supervisory body for certification and time-stamping service providers. Since the number of such service providers is quite low (1 CSP and 2 TSPs in June 2016) the register has been rather passive, functioning mainly as a registrar receiving compulsory annual audit reports from service providers.
- e-Identity Working Group was originally established under the auspices of MEAC, and comprised different stakeholders from the public and private sector. The group held meetings when necessity addressing topical issues regarding eID matters.

In addition to the public sector, the private sector also plays a significant role in the Estonian eIDMS. Both card manufacturing and certification are carried out by private companies, with almost a decade long intensive collaboration. Thus, PPP has served as an essential driving force behind the evolution of the Estonian eID.

There are two private companies that have essential role in the delivery and management of the Estonian eID:

- TRÜB Baltic AS (owned by Gemalto AG) is the company responsible for manufacturing of plastic ID-cards, and also their personalization.
- Certification Centre (AS Sertifitseerimiskeskus, SK) functions as a certification authority and maintains the electronic infrastructure necessary for issuing and using ID-cards. It also functions as an centre of excellence for electronic usage of the ID-card providing software, including a digital signature software framework, end-user support as well as support and services to e-service providers. In addition, the Certification Centre acts as a Mobile-ID technology provider in close collaboration with major local telecom operators.

SK is owned by the “big three” of the Estonian economy—two major banks (Swedbank and SEB bank) and the largest mobile network operator (MNO) Telia Eesti. This set-up allows SK to act as a unique roundtable bringing together the public sector, MNOs and the banks. This collaborative framework may definitely be credited as one of the main reasons why ID-card and Mobile-ID have been established as suitable eID tokens across all sectors. This configuration has also facilitated the comprehensive application of digital signatures.

Please examine visual concept on the inner side of main page.

X-Road has been live since 2001 with no downtime.

Description of the X-Road Environment

X-Road is the data exchange layer that forms the backbone of e-Estonia. Its creation was originally launched by the Estonian government in the 1990s in order to create a secure and standardised environment for interconnection, enabling data exchange between a multitude of different information systems, both in the public and private sector, incl. providing services to each other.

The main goal of the X-Road project was to build an infrastructure that would allow effortless access to the data in state registries without compromising the security of the data and with minimal impact to the existing systems.

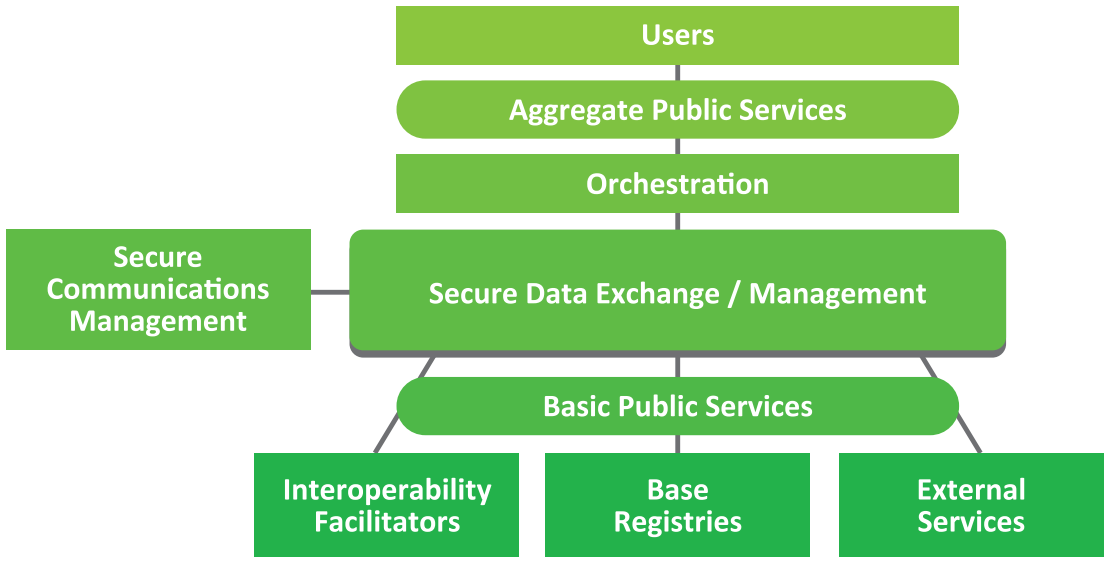
Background

The starting point was to unite various government registries – and there were many, managed and developed by different organisations, and financed separately. Registries contain mostly personal data that is in some cases or used to make high-value decisions, that are in some cases needed in real time (eg. healthcare situations). The situation was complicated by the fact that there were even more users, most of them small organisations without relevant security know-how and limited IT-budgets.

Statistical Data for X-Road in 2015.

- more than 1,700 services
- more than 900 connected organisations, public registries and databases
- more than 500 million transactions per year
- more than 1 million requests per day

Conceptual model for public services



The X-Road experience served as one of the models in designing the conceptual model for the European interoperability framework. For that reason the Estonian model matches fully with the EU conceptual model of services (see Figure above). (Ref: Estonian Interoperability Framework www.mkm.ee/sites/default/files/interoperability-framework_2011.doc)

The Population Register, maintained and developed by the Ministry of the Interior, is a database which contains the main personal data on Estonian citizens, EU citizens residing in Estonia, and aliens who have been granted a residence permit. The registry data includes names, unique personal identification codes, birth dates, places of residence, and other statistical data.

The Population Register is connected to other systems and databases via the X-Road, and allows for smooth exchange of up-to-date data. For example, when individuals apply for study allowances, discounted tickets on public transport or give their votes online, all the relevant data is retrieved from the Population Register. The system retrieves the information automatically – no need to submit extra documents or fill out online forms. Each person can access the registry with their with ID-card or Mobile-ID, and review or correct their data in the registry. (Reference. Ministry of the Interior).

The X-Road is an advanced and highly secure interoperability framework that connects all main public sector registries and databases, for example:

- Population Register
- Marital Property Register
- Succession Register
- Criminal Records Database
- e-Business Register
- European Business Registry
- e-Land Register
- Register of Constructions
- Central Procurements Registry
- Central Registry of Securities
- Ship Register
- Recreational Craft Registry

Technical Design

The technical design principles for the X-Road core technology Unified Exchange Platform (UXP) provide a distributed, secure, unified inter-organisational data exchange platform.

Distributed: UXP is a completely distributed, resilient system with distributed management. UXP does not centralise the data and does not change the ownership of the data.

Secure: Designed to satisfy the security requirements for governmental and organisational interoperability, UXP ensures the authenticity, integrity and non-repudiation of exchanged data; resulting in high availability of services and the confidentiality of exchanged data.

Heterogeneous: UXP connects information systems built on any platform. UXP does not prescribe any tools and technologies for internal use for organisations.

Reliable: UXP does not have a single point of failure. All components in the infrastructure can be made redundant for high resiliency against failures and attacks. Components that are available over a shared or public network employ protective measures against denial of service (DoS) attacks.

Federation support: UXP supports bi-lateral agreements between different UXP installations. Any single UXP installation has the capability for interoperability to another UXP installation.

Ease of implementation: UXP infrastructure deployment is fast and efficient. We offer a pilot version of UXP which can be implemented very conveniently and which offers prompt installation and review opportunities.

Ease of use: UXP is easy to adapt, all communication is based on web-services and can therefore be easily used by all developers through the use of UXP Adapter. In addition, access to all other organisations is uniform – there is only one API and one set of rules that must be followed by all developers.

Consultation and system support are available for the development of organisational procedures and legal framework. Our expertise is based on two decades of practical experience in the development and deployment of the relevant technology and auxiliary solutions. Partner organisations: e-Governance Academy, Cybernetica, Aktors, Estonian Information System Authority.

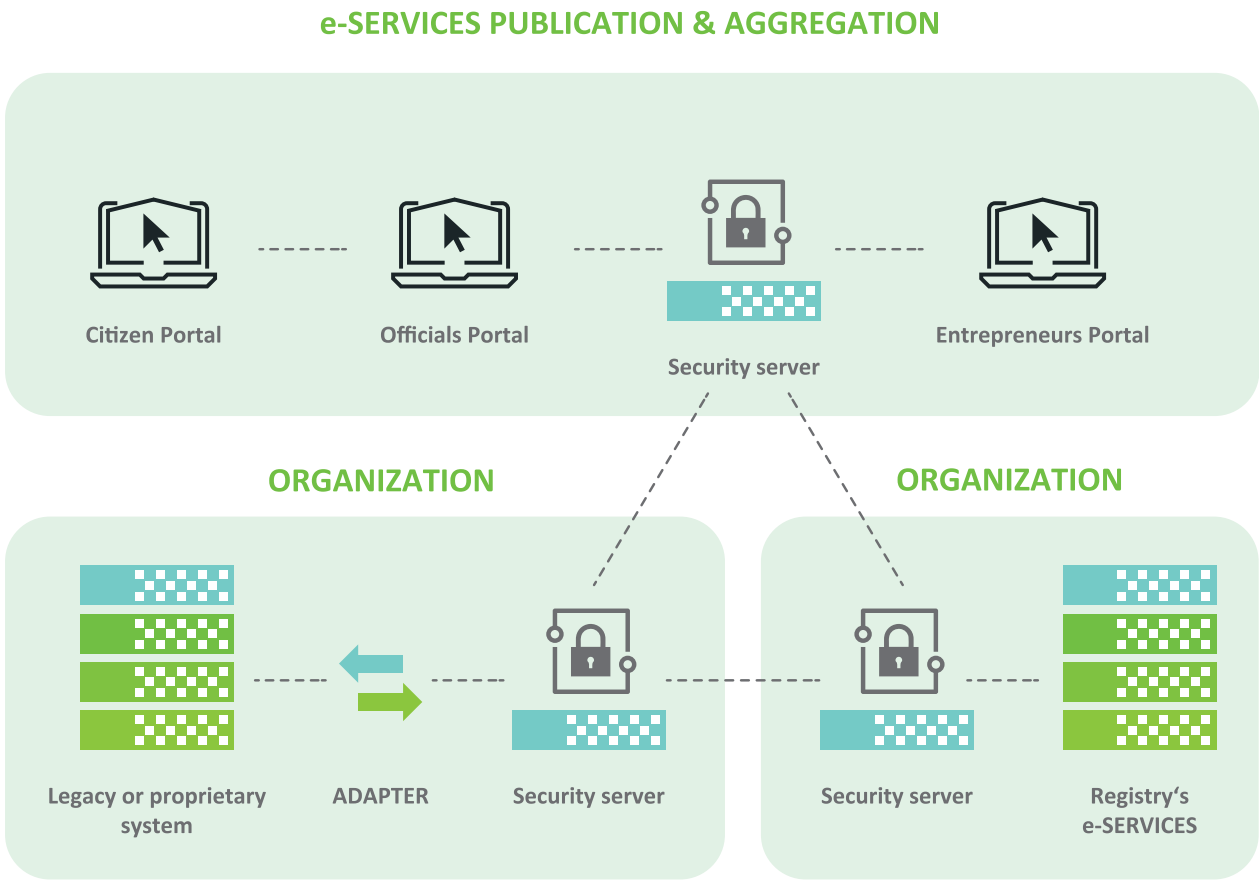
X-Road Technical Components

In the X-Road system, certified members communicate directly without intermediaries using secure peer-to-peer connections. All the messages (requests and responses) are digitally signed and time-stamped and sent over an encrypted and mutually authenticated channel.

Core Components of the Unified eXchange Platform (UXP)

The UXP Core Components form the technological basis for running the X-Road framework. It consists of the three integral components that provide the technological capability for the X-Road data exchange layer:

- UXP Security Server
- UXP Registry
- UXP Monitoring System



UXP Security Server

The UXP Security Server acts as a gateway between the organisation's information system and the UXP infrastructure. The security server relays request and response messages while providing a protective layer. All messages are exchanged via a cryptographically secure channel. What is more, the messages are digitally signed and time-stamped to ensure long-term authenticity value of the transactions.

- Security servers implement security gateways for web-services. All web-service requests and responses are digitally signed, time-stamped, encrypted and archived by security servers.
- Security servers implement organisational level access control for web-services.
- Security servers encapsulate the complexity of highly available PKI-based infrastructrure and provide developers with transparently secured inter-organisational web services.
- Security servers provide meta-services for discovering the structure of the infrastructure, including organisations and services.

UXP Monitoring System

The UXP Monitoring System receives monitoring information from the security servers and makes it available to central system administrators. The X-Road comprises local monitoring stations, each continuously collecting information (status information, error messages, and query information) from the local gateway. Status information contains detailed system information, such as CPU usage, memory usage, number of pending queries, and much more, giving the system administrator a complete and accurate overview of their server(s).

Global monitoring of the X-Road infrastructure enables the collection of statistical data about usage and will help maintain X-Road services. Analysing collected statistics can help discover and mitigate misuse. What is more, alerting X-Road members about invalid states of the security server will facilitate X-Road service availability.

UXP Registry

The UXP Registry maintains information about approved certificate authorities, approved trust services, UXP members and security servers. This information is distributed to the security servers. The UXP registry is maintained by the Governing Authority.

X-Road Governing Authority

X-Road´s operation is ensured by central governing, specifically by the Estonian Information System Authority (RIA), which serves as its governing authority. The most important task of the X-Road governing authority is to ensure the legal status of the X-Road system and the information exchanged by enforcing relevant policies. The X-Road governing authority is also responsible for steering the further development of the X-Road and ensuring its consistency and integrity.

The X-Road governing authority is also responsible for formulating the infrastructure's security policy which includes:

- security requirements for members of the infrastructure (eg. user authentication requirements)
- security categories applicable to services and information systems. Security categories allow the service providers to formally specify lists of security requirements that service users must comply with.
- list of trusted certification and time-stamping service providers.

Universal Portal

Universal portal MISP (Mini Information System/ Portal) is an application that allows organisations to execute X-Road services that are opened to them. Consumers can create and use four different types of portals in the MISP application. The portal types are the following:

Organisational information system

- one consumer organisation is linked to the portal
- user can only use e-services on behalf of the linked organisation. User must also have user
- role and query permissions given by this organisation.
- Services of X-Road producers are opened to the linked organisation.

Citizen portal

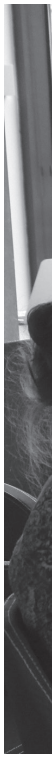
- a portal for public e-services.
- special configuration of the organisational portal where public user group is used. All authenticated users are considered to be in public user group.
- user account is not required to enter the portal and use e-services.
- authenticated user may use all e-services which are available in the portal.

Universal portal

- only one organisation is linked to the portal (the organisation managing the portal). Application of unit concept, i.e. user roles and permissions are linked to the portal unit. These roles and permissions are valid only under the linked unit, eg. in the family physician portal the portal unit is a doctor.
- e-services can only be used as a unit's representative, meaning query permissions and user role are required to be performed from under the unit.
- in order to use the portal, a new unit has to be registered by the unit representative, whose representation rights are checked using X-Road producers standard representation rights query.
- under the portal's organisation rights (while not representing any unit) only meta-services are executed.
- services of X-Road producers are opened (depending of portal configuration):
  - to the linked organisation.
  - to the portal unit organisation

Business portal

- special case of universal portal, units are registered in the Estonain Business Register
- during unit registration, check query is sent to CCR. The response may include businesses with single or unknown representation rights. Unknown representation rights mean that additional confirmations are required from other unit's representatives to set units permissions managers.




eGA development partners

Trust Services

Trust services provide certification and time-stamping services. In simpler cases, trust services can be provided by the X-Road governing agency or by any Certification Authority. Generally, certification authorities offer standard certification services:

- issue certificates for digital signature and web servers
- offer certificate validity checking services
- offer time-stamping services

X-Road Members

The X-Road members are entities that wish to communicate with each other. The prerequisite is that each member has an information system that will be connected with systems of other members through a security server. Thus, all X-Road members need to add a security server to their infrastructures and use X- Road and PKI infrastructure services for making their services available to different types of users. In order to join the X- Road community, all prospective members must ensure that they have sufficient security measures in place. The X-Roads governing authority retains the right to review security policies and operational procedures. Finally, after concluding contracts with service consumers, access rights to use the service are granted to client organisations. The access rules are always defined by the service provider and regulated by the X-Road governing authority.

In contrast to consumers, who make requests via the X-Road, data providers use the X-Road to answer requests and share data. Therefore, data providers must meet two extra requirements to use the X-Road:

- data providers must operate a registry (database), which must be registered with the X-Road governing authority (Information System Authority in Estonia).
- data providers must have an Adapter Server, commonly known as integration components.

Main Actors in X-Road

On the political level the major Estonian institutions that are involved in the X-road development:

Ministry of Economic Affairs and Communications (MEAC) is the supervisory authority of the Estonian Information System Authority (SIA), that coordinates the development and administration of the national information system, to help the government provide the best possible e-services to citizens.

- RIHA, the administration system for the state information system, serves as a catalogue for the national information system. RIHA guarantees the transparency of the administration of the national information system and helps plan national information management.

In the private sector two companies are involved in the X-road delivery and management:

- Aktors develops information systems and other specific software solutions, offering the whole package from analysis to the implementation of the system and consulting services related to software development. Aktors has been involved from the beginning in the development of several X-Road interface databases. In addition, Aktors handles the maintenance and development of the X-Road portal MISP.

- Cybernetica: researches, develops and manufactures software solutions, light signaling and telematics products, maritime surveillance and radio communications systems; investigates and applies the theoretical and practical security solutions. Cybernetica is focused on spreading its expertise on UXP technology, currently enabling e-Government services for more than 35 million people across continents. Integrated management system of Cybernetica is certified according to the standards ISO 9001:2008 and ISO 14001:2004.

X-Road Community

The community was created in 2013, and meets twice a year. They discuss issues related to the

X-Road, and seek solutions to these issues. The community includes developers, administrators and business process managers that want to be involved in the development of X-Road.

How to start?

Why use the X-Road solution?

- X-Road is a major step towards the Information Society
- X-Road offers best practices from Estonia and Europe in the utilisation of new technologies
- X-Road provides secured and top quality e-Services to citizens, government agencies and the private sector

Currently, the X-Road is used as the official government interoperability framework in Estonia, Azerbaijan and Finland. In addition, the Estonian e-Governance Academy has helped several countries (eg. Namibia, Tunisia, Palestine, Faroe, Haiti, Ukraine, Kyrgyzstan, etc.) to implement and adjust X-Road to their needs.

The implementation process comprises the following activities:

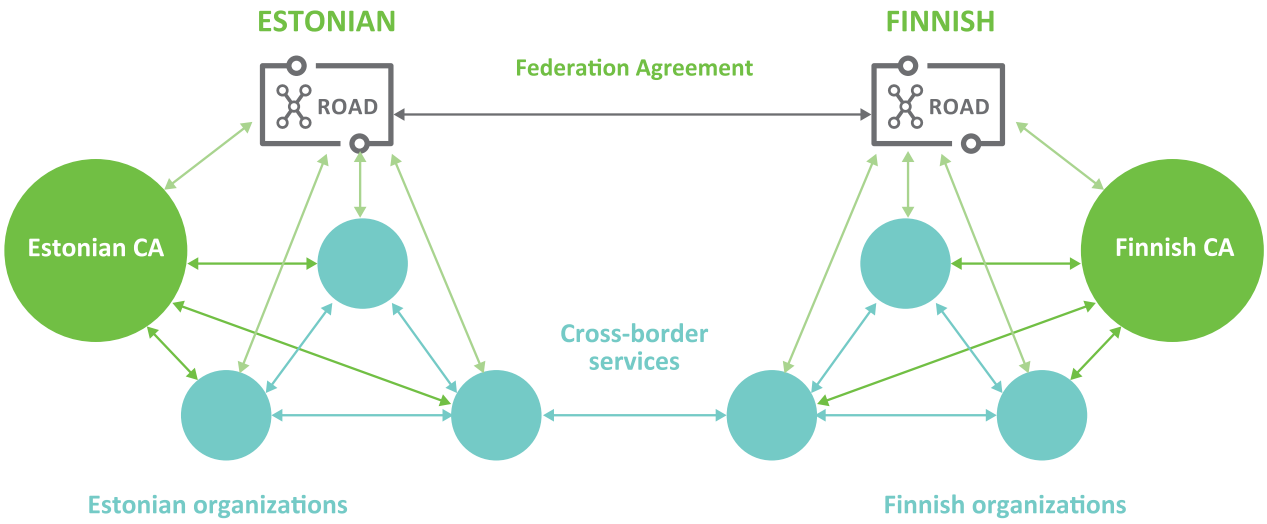
- creation of the central agency/governing authority
- establishing legal status
- setting up technical systems
- creation of e-services

Prerequisites for X-Road

- unique identifier per entity
- eID framework
- technical and regulatory framework for digital signatures
digitised registries
- regulatory framework for electronic data exchange (to ensure uniform data exchange)
- trusted and legitimate governing authority procedures and regulations with sufficient resources

For more information, please contact Mr Uuno Vallner uuno.vallner@ega.ee

Ongoing: Federation EE-FI



e-Government Legislation

eGA Member of the Management Board Hannes Astok and Founder of e-Governance Academy Ivar Tallo

e-Governance does not entail a comprehensive system of specialised legislation. Actually, it might even be dangerous to have too many regulations, because it runs the risk of creating a parallel system of governance, and might lock in technologies when they would actually need flexibility in order to facilitate on-going development.

The regulations should address the nature of transactions, and the sensitivity of data, while leaving the technology itself relatively untouched. The essential legal work lies in analysing existing legislation and identifying gaps as well as areas where law may pose obstacles to the development of e-governance. However, certain aspects, such as electronic identification and digital signatures, need special regulation because these are the concepts that have no equivalents in the non-virtual paper-based world. In addition, special focus should be on data protection legislation because electronic data is generally perceived as less secure.

Therefore, it is essential to engage legal experts early in the planning process in order to avoid regulatory obstacles, and also prevent situations where late implementation of regulations could hinder the application of e-services. Over-regulation should be avoided and paradoxically, the risk is greater if the legal analysis is postponed to a later stage. The most pressing matters that need to be solved in first order are ICT legislation and competition law, in order to ensure access to the internet, but also the online protection of rights. However, this does not necessarily need to take the form of new law, but should preferably be solved via legal discussions.

Estonia does not have specific e-governance legislation, but there are a number of legal acts that have an effect on e-governance. This overview outlines the most important acts, the different steps that need to be taken, as well as the assistance that the Estonian e-Governance Academy can provide in this process.

Basic Principles

The following principles outline the key elements related to the legal side of e-governance:

- avoid over-regulation, because it entails the risk of creating parallel governance structures
- it is essential to review existing laws to ensure that e-governance methods are applicable
- it is important to legally determine the responsible authority (i.e. for carrying out reforms, monitoring the quality and accessibility of services and for receiving complaints, etc.)
- stipulation of data protection rules and also a system of enforcement
- the law must establish a secure form of online identification
- information and communication technology (ICT) law as well as competition law (sector specific and/or general) is important to ensure that proper access to the internet is secured
- e-governance can be an important tool for ensuring better access to information and facilitating democratic participation, but the technology should be seen primarily as the tool and not the determining factor for how to structure such access and participation

Public Information Act

The act covers national and local government agencies, and other legal entities both in public and private law, that are responsible for the delivery of public services in areas such as education, health care, social or other public services. People have the right to make inquiries, and the holders of relevant information are under obligation to reply. In addition, they are also obligated to maintain websites and post relevant information online. These entities are also required to ensure that the information is not 'outdated, inaccurate or misleading'. Currently, this act also regulates the subject area that was previously covered by the now defunct Databases Act. From the perspective of

e-governance the Public Information Act regulates:

- management of the national information system (by Information System Authority)
- data exchange layer of the information system X-Road
- security measures for other information systems

Digital Signatures Act

This act bestows equivalent legal status to both digital and handwritten signatures, and stipulates a requirement for all public institutions to accept digitally signed documents. It also includes a special chapter regulating governmental supervision over certification and time-stamping service providers. For a more detailed overview, please refer to the subsection on Public Key Infrastructure. This act is superseded by the EU regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market (eIDAS).

Archives Act

The act stipulates the principles for collecting, evaluating, archiving, preserving, and accessing archival documents, as well as the general regulation for archiving activities. What is more, it lays out the guidelines for private records entered in the archives' register and the transfer of ownership of private records entered in the archives' register. The Archives Act applies to electronic documents as well as to documents in any other forms.

Population Register Act

The act sets out the principles for one of the main cornerstones of the digital society – the unique personal identification code. Pursuant to this act, the Estonian identification code is a unique lifelong 11-digit code that is mandatory for everyone working and living in Estonia, also e-residents. The ID code is a fundamental element of the electronic authentication process. In addition to electronic transactions, the same code applies in all other contexts where personal identification is necessary, i.e. each person has their own unique code.

Identity Documents Act

This act establishes a mandatory identity document, and regulates the issuance of identity documents to Estonian citizens and aliens by the Republic of Estonia. In addition to other functionalities, the identity document can also be used for electronic transactions, as explained above.

Electronic Communications Act

The purpose of this act is to create the necessary conditions for promoting the development of electronic communications networks and services while ensuring the protection of the interests of users of such services. The act stipulates requirements for: publicly available electronic communications networks and services; and also state supervision over compliance with the requirements. It serves as sector-specific legislation to the Competition Act.

Information Society Services Act

This act draws on the EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. It establishes the requirements pertaining to information society service providers, as well as the organisation of supervision and liability in case of violations.

Personal Data Protection Act

The regulations provided in this act are in full compliance with the EU Data Protection Directive 95/46/EC. The act protects the fundamental rights and freedoms of persons in the course of processing of their personal data, all in accordance with the right of individuals to obtain freely any information that is made available for public use. The EU is in the process of amending its data protection legislation, with the General Data Protection Regulation adopted in April 2016. The new regime is better suited for electronic data. However, the personal nature of the data, not its form, is still the determining factor. Independent oversight, and clear provisions regarding responsibility for data processing, remain the cornerstones of this protective system.

Public Procurement Act

This act includes legal provisions facilitating the further development of electronic solutions in public procurement (e.g. e-Auctions, Dynamic Purchasing System, eCatalogue,s etc.).

State Secrets and Classified Information of Foreign States Act

This act ensures the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure, and becoming accessible to persons who have not been granted access to such information.

Emergency Act

This act provides the legal framework for crisis management, including preparation for an emergency and resolving an emergency, as well as ensuring the continuous operation of vital services. This act also regulates the declaration, the resolving and the termination of emergency situations, and the use of the Defence Forces and the Defence League in resolving an emergency, performing rescue work and ensuring safety.

How to start?

The e-Governance Academy offers assistance in analysing and formulating necessary legal regulations.

The first step is to conduct a comprehensive review of existing legislation, which should preferably be carried out by local legal experts under the supervision of eGA´s legal expert. The main goal of this analysis is to highlight areas in need of legal modifications in order to facilitate smooth transition to
e-governance (e.g. regulations on digital signatures, electronic documents, interoperable databases etc.). Ideally, this analysis should be carried out concurrently with the planning of applicable technologies because the regulations should complement the technological solutions. The outcome of this comprehensive legal analysis is an overview of relevant legislation, highlighting necessary changes, the means to achieve them, and offering suggestions for legislative modifications.

The following areas of law need to be reviewed with regard to e-governance related matters:

- administrative law (incl. administrative procedure)
- competencies of government institutions

data protection legislation (protection of privacy)

- contract law
- regulations on access to information
- ICT law (eg. internet service provision)
- competition law (incl. general/sector specific, • including licenses and authorisations)
- public procurement law
- criminal procedure law (rules on evidence)

The key factor determining successful transition to e-governance is the establishment of a governing authority responsible for different aspects of e-governance. The competence of this agency must be set out in law to avoid ambiguity and disputes. eGA experts (legal and institutional) are on hand with knowledge about the best international practices. We recommend arranging a seminar with
e-governance legal experts in the early stages of transitioning to digital society.

For more information, please contact Mrs Katrin Nyman-Metcalf katrin.nyman-metcalf@ega.ee

Institutions and Organisations

Government Institutions

Estonian Government Office:

Supports the government and the Prime Minister in planning and implementing policies, and facilitating good governance practices. Responsible for ensuring that draft legal acts proposed by the government are constitutional and in conformity with other legislation.

- **e-Estonia Council:** coordinates the development of Estonian digital society and e-governance, specifically the implementation of national digital agenda. Establishes expert committees, and working groups or commissions studies in the field of ICT policy.
- **National Security and Defence Coordinaton Unit**: responsible for coordinating national security and defence, including cyber security.

Ministry of Economic Affairs and Communications (MEAC)

is responsible for developing the information society, and supervising relevant government agencies

Information System Authority (ISA) main areas of responsibility:

- Public Key Infrastructure (PKI)
- Administration System for the State Information System (RIHA)
- Data Communication in Public Administration (ASO)
- State Portal eesti.ee
- Data Exchange Layer X-Road
- Document Exchange Centre (DEC)
- IT Infrastructure

Raising Public Awareness about the Information Society

- Critical Information Infrastructure Protection (CIIP)
- Management of security incidents in .EE computer networks CERT-EE
- IT Baseline Security System ISKE

Technical Regulatory Authority

- improves the security and reliability of the electronic communication products
- oversees certification service providers and time-stamping service providers
- adopts ETSI (European Telecommunications Standards Institute) European Standards
- manages Root-CA (EE Certification Centre Root CA)

The Estonian Internet Foundation

- maintains the database of the country-code top level domain name

Enterprise Estonia

- promotes regional policy, and provides counseling, funding and training for businesses
- manages the e-Estonia brand, incl. web page on our e-governance and
- e-services, and the e-Estonia showroom- an executive briefing hub

Estonian State Infocommunication Foundation (RIKS)

- provides communication-related services to government agencies
- provides operative, radio and maritime communications, and telephone services

Ministry of Education and Research

is responsible for the development of the national IT education strategy and the integration of IT in all levels of the Estonian educational system

National Archives

- establishing principles, standards and guidelines for digital records
- develops and implements the digital archives to their full potential

Information Technology Foundation for Education (HITSA)
- promotes the development of ICT-related education in Estonia
- oversees the operation of the Estonian IT College, and the Tiger Leap development programme for implementing IT in basic and general education

Ministry of the Interior

is responsible for developing identity management policies (incl. electronic identity), and coordinating national crisis management activities, incl. cyber crises.

Police and Border Guard Board
- oversees the national system for identification
- documents, and maintains electronic identities of residents at large
- investigates cyber crimes and terrorism
- utilises digital forensics

Estonian Internal Security Service
- investigates offences related to internal security, incl. collecting information and implementing
- preventive measures

Centre for Information Technology and Development Centre
- oversees the activities of the Population Register

National Foundation for Civil Society (KÜSK)
- supports NGOs in capacity development by providing funding
- funds projects promoting democracy

Ministry of Justice

is responsible for the development of national legislative policy, and administration of national registries, e.g. commercial registry

Centre of Registers and Information Systems
- oversees the development and management of national registries and information systems

Deputy Secretary General for Communications and State Information Systems Taavi Kotka

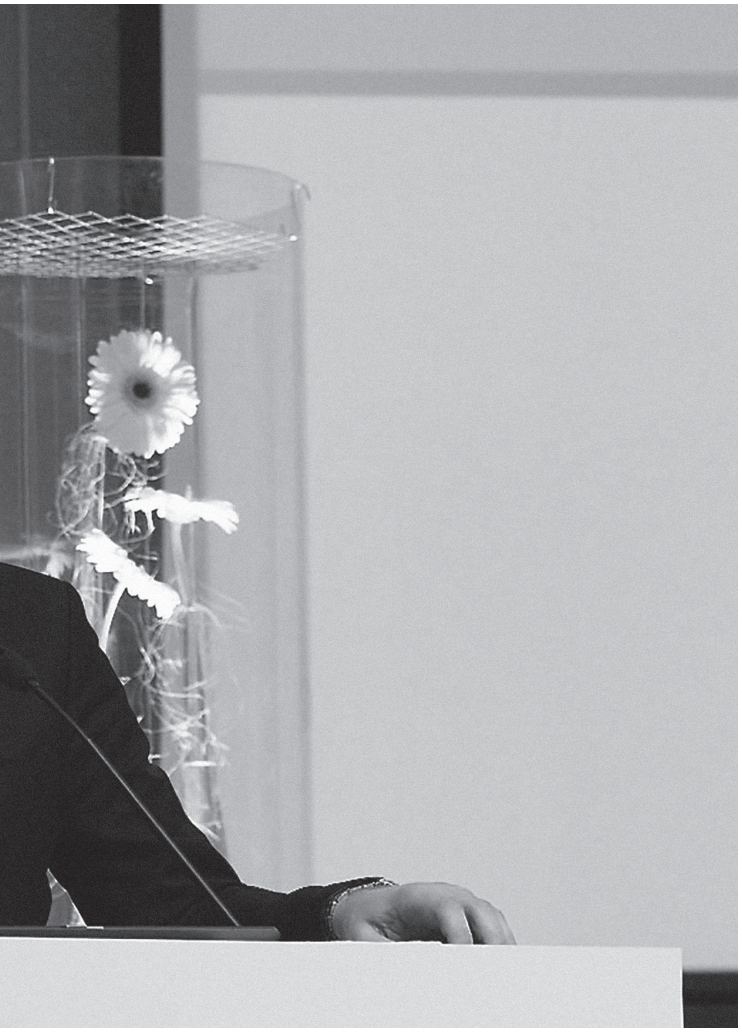
Data Protection Inspectorate
- independent organisation, supervises public and private sector entities in respect to data protection rights and obligations.

Ministry of Defence

is responsible for organising national defence by deterring attacks against Estonia and ensuring that Estonia is capable of defending itself against external threats.

Estonian Information Board
- manages the electronic system for classified information

Estonian Cyber Defence League
- volunteer organisation of IT security experts, programmers, lawyers and management specialists from the nation's top IT companies, banks, ISPs and defense forces, tasked with assisting the government during cyber attacks



Non-Governmental Organisations

eGA
- establishes and disseminates knowledge and best practices in the fields of
- e-governance, e-democracy, open information societies and national cyber security

Look@World Foundation
- promotes the use of Internet and ICT in education, science and culture, e.g. projects on ICT-skills , safe usage of ICT, and ICT-related after-school activities

Estonian Association of Information Technology and Telecommunications
- voluntary umbrella organisation uniting Estonian IT and telecommunications companies aiming to promote their mutual co-operation in Estonia's development towards the digital society

Academic Institutions

University of Tartu
- national university, and the leading centre of research and training in Estonia
- belongs to the top 3% of the world's best universities

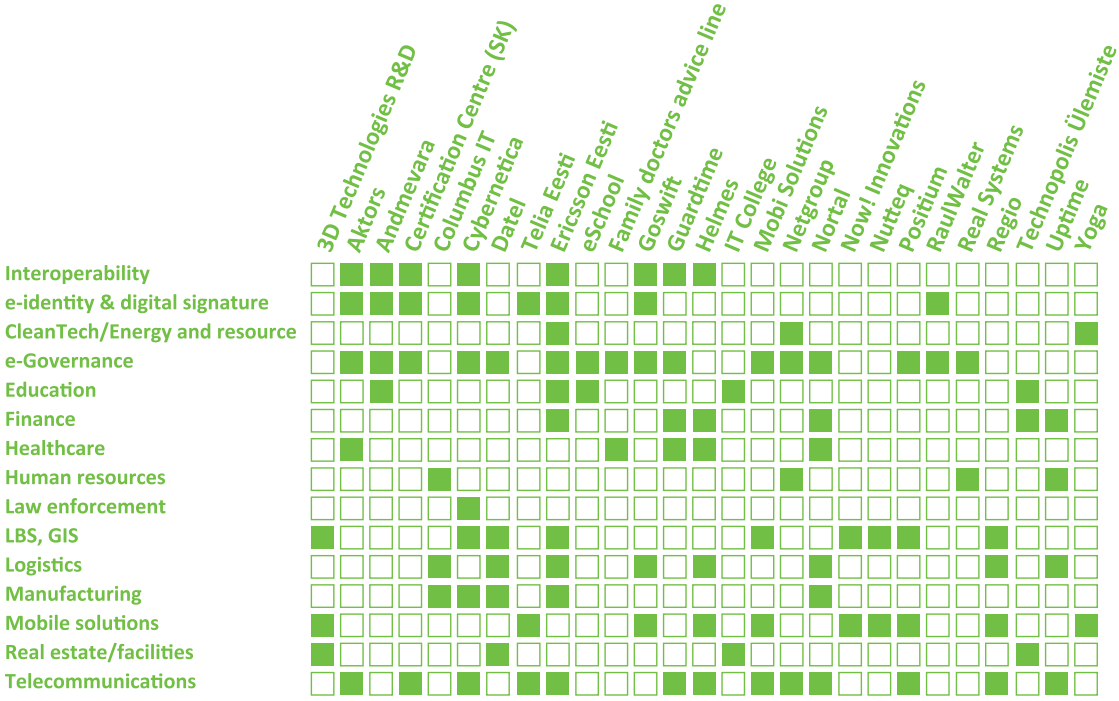
Tallinn University of Technology
- the flagship of Estonian engineering and technology education
- creates and values that secure Estonia´s development in a globalised world by generating synergies between natural and social sciences, thus enhancing the development of society

Tallinn University
- the largest humanities university in Tallinn and the third largest public university in Estonia
- its interdisciplinary focus areas are educational innovation, digital and media culture, cultural competencies, healthy and sustainable lifestyle and society and open governance

The Estonian Information Technology College
- the leading provider of applied higher IT education in Estonia, bringing together
- high-tech know-how and the practical needs of the information society
- 1/3 of the academic staff come from IT companies or government agencies

Business Entities

In this section you will find a list of companies that are important players both in the domestic and foreign markets, equipped with cutting-edge expertise and specialised teams. They are ready to become your reliable partners in the areas of e-governance. In order to find a suitable business partner from Estonia, please begin by choosing the field of competence from the left column, and then selecting the matching company in the upper row:



Reference: www.e-estonia.com

eGA Head of e-Governance Trainings Annela Kiirats

Knowledge Development

In Estonia, a variety of ICT education programmes have played an essential role in the success and widespread utilisation of the country's eID system for various transactional processes, as well as overall growth in the number of people using different e-services.

Over the years, Estonia has launched several different projects and programmes in order to improve accessibility to the Internet and increase the relevant motivation and capabilities among all age groups, especially the elderly people (i.e. 55+). The ICT education targeting the younger population is mainly provided by schools, whereas elderly people have had the opportunity to obtain basic ICT user skills and get user support for example at post offices, regional offices of government agencies and local municipalities.

The main partner organisations participating in ICT knowledge transfer projects have been Look@World and Tiger Leap Foundation. In addition, the Ministry of Economic Affairs and Communications initiated a special programme titled "Awareness-Raising for the Information Society", which aims to raise awareness about the benefits of the information society; promote active participation in information society policy making; improve the effectiveness of policy making in the ICT area; contribute to making public administration more transparent and accountable; increase accessibility to ICTs and boost active use among all segments of the population.

The programme comprised trainings offered by different partners, incl. banks and the Tax Office which promoted the popular use of e-services through the utilisation of the electronic ID-card. The programme´s core activities include the cultivation of positive attitudes towards innovation and new technologies in general, more specifically:

- promotion of the eID possibilities
- government information portal eesti.ee and other online public services
- introducing citizens to the possibilities of the state information system
- increasing awareness about online security issues

ICT in General Education

In 1997, with the establishment of the Tiger Leap Foundation, and the launch of its Tiger Leap Program (1997-2000), Estonia began facilitating the use of ICT in general education, and as a result all Estonian schools now have:

- a broadband connection
- consistent and practical ICT methodology training for teachers at different levels
- possibility for teachers to use VLEs (virtual learning environments) to create electronic study materials.

According to Eurydice's Key Data on Learning and Innovation through ICT at school in Europe, Estonia has established national strategies covering training as well as research measures in all areas of ICT in schools, e-learning, and digital/media literacy. In primary and secondary schools ICT is approached as a general learning tool that can be utilised in all other subjects. Public-private partnerships for promoting the use of ICT are also widely encouraged. In addition, in secondary schools ICT is also taught as a separate subject.

With regard to the use of ICT, the majority of teachers in Estonia have been using ICT in class activities for almost a decade, and in general, the use of ICT by Estonian teachers is well above the EU average. As a result, Estonia ranks first among the leading group of countries at all grades on this indicator (Reference: www.schoolnet.com Survey of Schools: ICT In Education).

e-Governance and Cyber Security Programmes in Estonian Universities

University of Tartu

- International Master's Programme (MSc) in Cyber Security (joint programme with Tallinn University of Technology)

Tallinn University of Technology

- International Master's Programme (MSc) in Cyber Security (joint programme with University of Tartu)
- e-Governance Technologies and Services (MSc)
- Technology Governance (MA)

Tallinn University

- Politics and Governance (BA)
- Information Society Technologies (PhD)
- Information and Communication Science (PhD)

IT College

- Cyber Security Engineering
- Information Systems Analysis

e-Democracy

The development of democracy in Estonia has been similar to other post-communist countries, characterised by rapid institutional development and a somewhat slower development of civic society. However, Estonia is exceptional in its technological development which has been faster than in most other post-communist countries (Reinsalu and Dobnikar, 2012).

The benefits of e-democracy lie in the support and enhancement of democracy, democratic institutions and democratic processes by means of technology. It is complementary to, and interlinked with traditional democratic processes, so as to widen the choices available to the public for participating in political processes.

The benefits of implementing e-democracy are most evident for example in i-voting, that has been used in Estonia since 2005. Estonia is the first country in the world to use online voting as an alternative to the traditional voting procedure. It enables people to vote from anywhere in the world by using their electronic identity card.

In the early stages of developing e-democracy the role of ICT was relatively weak. However, the constantly growing popular use of the Internet and available e-services have improved democracy. The Internet is also a great tool for educating people on democracy, e.g. helping people stay up to date with what is happening in their government. Recently, researchers have concluded that ICT has the potential to reach the disengaged parts of the population and bring them closer to society and politics. (Ref: Alvarez, R., Hall, T., and Trechsel, A.)

Other areas of e-Democracy:

- **e-Participation**
- **government-to-citizen G2C**
- **citizen-to-government C2G**
- **citizen-to-citizen C2C**
- **grass-root activists and social networking**
- **political campaigns**
- **online media**
- **i-Voting**

eGA Head of e-Democracy Domain
Kristina Reinsalu

Estonian e-Democracy

TIMELINE:

1996 Tiger Leap Foundation

This NGO played a significant role in improving access to the Internet and developing new capabilities among the general population through the use of new technologies.

2001 Look@World Foundation

This NGO serves public interest by supporting education, science and culture via encouraging and popularising the use of Internet and ICT. Look@World, together with the Tiger Leap Foundation, helped increase the e-literacy of Estonians and as a result also Estonia´s overall competitiveness.

2001 TOM

A civic participation portal called "Today I Decide" (TOM, acronym based on the Estonian name) launched by the Estonian State Chancellery in June 2001, and incorporated into the
e-participation site osale.ee in June 2008. This public participation portal allowed citizens to engage directly with legislative and policy-making processes either by proposing new legislation or by suggesting amendments to existing laws. By launching TOM, the Estonian government was one of the pioneers in the field of e-participation. However, in reality, only relatively few activists took part in TOM and actual virtual debate took place in other informal forums.

2005 i-Voting

Internet voting, or 'i-voting', is a system that allows voters to cast their ballots online via an Internet-connected computer, from anywhere in the world. I-voting has been approached with the aim of establishing the criteria by which to classify the different views on Internet democracy (Reference: Kristina Reinsalu. The implementation of Internet democracy in Estonian local governments)

2007 www.osale.ee

("participate.ee" in Estonian)
The successor to citizen participation portal TOM was launched in 2007, and is now the central consultation-participation portal for the Estonian Government. The portal, managed by the State Chancellery, is connected to the inter-ministerial electronic documentary system EIS. It aims to facilitate wider participation of citizens and civic organisations in politics, and also to draft legislation through discussions and consultation in accordance with relevant development plans. The portal is still operational, although several studies have been critical and consider osale.ee a failed
e-democracy tool.

2010 www.petitsioon.ee

A participation platform created by the Central Confederation of Owners, Estonian homeowner lobby group, for popular launching of online petitions. It enables raising a petition by paying a usage fee which currently stands at 30 EUR. Authenticity of

TIMELINE:

signatures is proven by an electronic ID-card in addition to identification by e-mail address or Facebook profile. Because the NGO that created and manages the platform has not taken responsibility for making the petitions official (i.e. forwarding them to the addressed institutions) it is difficult to evaluate the actual impact of this tool. Nevertheless, in some cases the impact is clear and it correlates with the number of people signing the petition. For instance, the petition called Harta 12 initiated in 2012, which managed to garner 18,210 signatures (more than any other petition so far), has had a tangible outcome: it was the key driving force behind starting the Rahvakogu (The People's Assembly) process described and analysed in the next section.

2012 Rahvakogu

The People's Assembly was initiated by the Estonian President and active NGOs with the aim to improve the functioning of democracy in Estonia. The Assembly combined modern communication tools with traditional face-to-face discussions. In three weeks, the website received close to 2,000 proposals from citizens, and the top 15 ideas were presented to the Parliament with seven of those having now been adopted as laws (incl. three were implemented fully and four were modified or combined with other laws) (Toots, 2015; Navarro and Font, 2013).

2013 Participatory Budgeting

Participatory budgeting (PB) is an innovative way to manage public funds, and to engage people in issues of local government. Tartu was the first city in Estonia that opened up its budgeting process for citizens and experimented with participatory budgeting pursuant to the scenario designed by the eGA. From the beginning, electronic participation was open to all in order to provide an opportunity to contribute to the development of e-democracy. Citizens of Tartu were given a chance to decide for themselves how their city should spend 1% of the annual investment budget next year. This was done by presenting their ideas online or by sending a letter/e-mail to the Tartu public relations department. After eligible proposals were selected, the residents had the chance to vote for their favourite projects and the most popular proposal received funding from the city of Tartu.

2016 www.rahvaalgatus.ee

The Draft Act on Public Initiatives and the e-platform www.rahvaalgatus.ee were born in the process of the People´s Assembly organised in 2012. This public participation platform enables citizens to compile and send public initiatives (which must have at least 1.000 digital signatures) to the Estonian Parliament. What is more, the platform provides an opportunity to follow whether the submitted proposal will become a draft act.

Open Government Partnership

The Open Government Partnership (OGP) is a global effort to make governments more open, accountable, and responsive to citizens. People all over the world want their governments to be more transparent, effective and accountable, with institutions that empower people and are responsive to their aspirations.

OGP was launched in September 2011 when the founding eight governments of Brazil, Indonesia, Philippines, Mexico, Norway, South Africa, United Kingdom, and United States formally adopted the Open Government Declaration and announced their national action plans. Since then, the partnership has grown to 64 countries representing a third of the world's population.

The Estonian Government is committed to working towards an open and empowered society where the citizens' voices are heard and civil society initiatives are included in the political process. The Estonian national action plan covers activities in the areas of developing public (e-) services, accessibility to national information assets (data), engaging citizens in policy-making, and preventing corruption and conflicts of interest.

In April 2014, eGA launched a new project called "Open Government Partnership in Local Governments" which aims to increase the awareness and capacities of Estonian local governments for implementing open, transparent and participatory governance, while also to improving e-democracy at the local level.

We believe that it is necessary for local governments to include specific activities related to open governance into their action plans, and to create a joint open government partnership platform for sharing experiences and best practices. To that end, a network of front rank local governments has been formed and activated. This network shall work in close cooperation with local civic organisations, and establish key principles of open government for local governments and design specific action plans.

How to start?

eGA promotes the balanced development of e-government, wherein e-democracy receives due attention along with e-administration and e-services. We provide policy advice, training, and consultancy to public authorities and civil society organisations who want to enhance the transparency, accountability and civic engagement of their governments.

For more information, please contact
Mrs Kristina Reinsalu
kristina.reinsalu@ega.ee

Focus areas of training and consultancy:

- impact of ICT and other technological developments on democracy
- development of transparent and reliable e-services
- drafting an e-democracy policy
- tools and practices for online engagement and online participation
- development of e-communities
- Estonian experience with e-participation platforms
- i-Voting and good practices in online voting

e-Governance Academy (eGA)

The e-Governance Academy (eGA) is a think tank and consultancy organisation founded for the purpose of creating and disseminating knowledge and best practices related to e-governance, e-democracy, cyber security and the development of an open information society. eGA is an independent and mission-based non-profit, non-governmental institution. In the course of its operation eGA has always maintained high standards of integrity and performance required for these efforts.

eGA offers training and consultation services to leaders and stakeholders regarding the use of information and communications technology for the purposes of increasing government efficiency and improving democratic processes. What is more, eGA assists in the implementation of e-government technical solutions.

EGA was jointly established in 2002 by the United Nations Development Program (UNDP), Open Society Institute (OSI) and the Government of Estonia. It is governed by a supervisory board composed of representatives from the Office of the President of the Republic of Estonia, Republic of Estonia Government Office, Ministry of Foreign Affairs, Ministry of Economics and Communication and internationally recognised e-governance experts.

Over the years eGA has successfully undertaken and completed contracts with such distinguished partners as the Open Society Institute, UNDP, World Bank, USAID, Estonian Government, European Commission, and numerous other international organisations and companies.
Since its inception, EGA has collaborated with a wide variety of organisations and government agencies encompassing more than hundred international projects in more than 60 countries, such as Moldova, Armenia, Ukraine, Georgia, Tunisia, India, Namibia, Kyrgyzstan, Sao Tome & Principe, Cayman Islands and many others.

e-Governance Academy – Your Partner in Implementing e-Governance and Open Government

In Brief

- active since 2002
- more than 60 countries consulted
- more than 3,000 participants (public officials) in trainings and consultations
- more than 50 ICT projects on the national, local and organisational levels
- network comprising more than 100 experts from governmental organisations, academic research institutions, and private companies

eGA's Core Competencies

e-Governance for central governments: We help improve the awareness and skills of government leaders in all aspects related to e-governance by focusing on relevant policy and planning issues, organisational and management frameworks, legal regulations, ICT implementation budgeting, and basic concepts of e-government interoperability and architecture.

e-Government for local and regional governments: We demonstrate how local and regional governments can play an active role in the development of e-administration and e-democracy.

e-Democracy and e-Participation: We provide assistance in achieving more transparent, accountable and participatory governance.

Cyber security policies and frameworks: Through training and technical assistance, we enable governments to understand the modern risks of the digital society and develop national cyber security policies and strategies.

Interoperability: We support the implementation of interoperable e-service frameworks, proven to provide necessary flexibility and versatility in existing decentralised IT solutions.

eGA's offers the following services:

- consultancy
- training
- research
- implementation of e-governance solutions

For more information, please contact us:
e-Governance Academy Foundation

Arvo Ott (PhD)
Chairman of the Management Board
Area of Expertise: Central government, interoperability
P: +372 508 8901 / E: arvo.ott@ega.ee

Hannes Astok
Member of the Management Board
Area of Expertise: Policy planning, local government development, interoperability
P: + 372 5091366 / E: hannes.astok@ega.ee

Annela Kiirats
Area of Expertise: e-governance trainings
P: +372 525 8623/ E: annela.kiirats@ega.ee

Mari Pedak
Area of Expertise: Digital identity
P: +372 515 6761 / E: mari.pedak@ega.ee

Raul Rikk
Area of Expertise: Cyber security
P: +372 5647 7520 / E: raul.rikk@ega.ee

Kristina Reinsalu (PhD)
Area of Expertise: Local e-governance, e-democracy
P: +372 528 1392 / E: kristina.reinsalu@ega.ee

Publication composed by Sandra Roosna, Raul Rikk
Design and copywriting by Optimist Group
Involved experts: Arvo Ott, Uuno Vallner, Katrin Nyman-Metcalf, Annela Kiirats, Mari Pedak, Kristina Reinsalu, Liia Hänni, Anu Vahtra-Hellat, Siret Schutting, Raul Kaidro.
This publication was developed in cooperation with SeedForum Estonia and Norway Grants program.

References:

Alvarez, R., Hall, T., and Trechsel, A. (2009) Internet Voting in Comparative Perspective: The Case of Estonia. PS: Political Science and Politics, 42(03):497–505).

Harjo, O. (2016) Lairiba arenduse mudelid.

Reinsalu, K., Dobnikar, A. (2012) e-Democracy in policies and practices in transition society – country cases from Slovenia and Estonia, Paper proposal for European Conference on e- Government 2012, 14-15 June, Barcelona, Spain

Vassil, K. (2015) h p://valimised.err.ee/v/riigikogu_valimised_2015/valim- isuud-ised/927b20d9- 118d-4d08-8961-a72e69593f11 (Accessed 17 January 2016, in Estonian)

Certification Centre website
Cybernetica website
Digital Agenda 2020, Ministry of Economic Affairs and Communications
EU Digital Agenda Scoreboard
Enterprise Estonia, e-Estonia showroom website
Freedom House report "Freedom on the Net 2015"
The Estonian eHealth and eGovernance System

The European Schoolnet Academy, Survey of Schools: ICT In Education (2014)
Police and Border Guard Board portal

eGA has trained over 3 000 officials from more than 60 countries