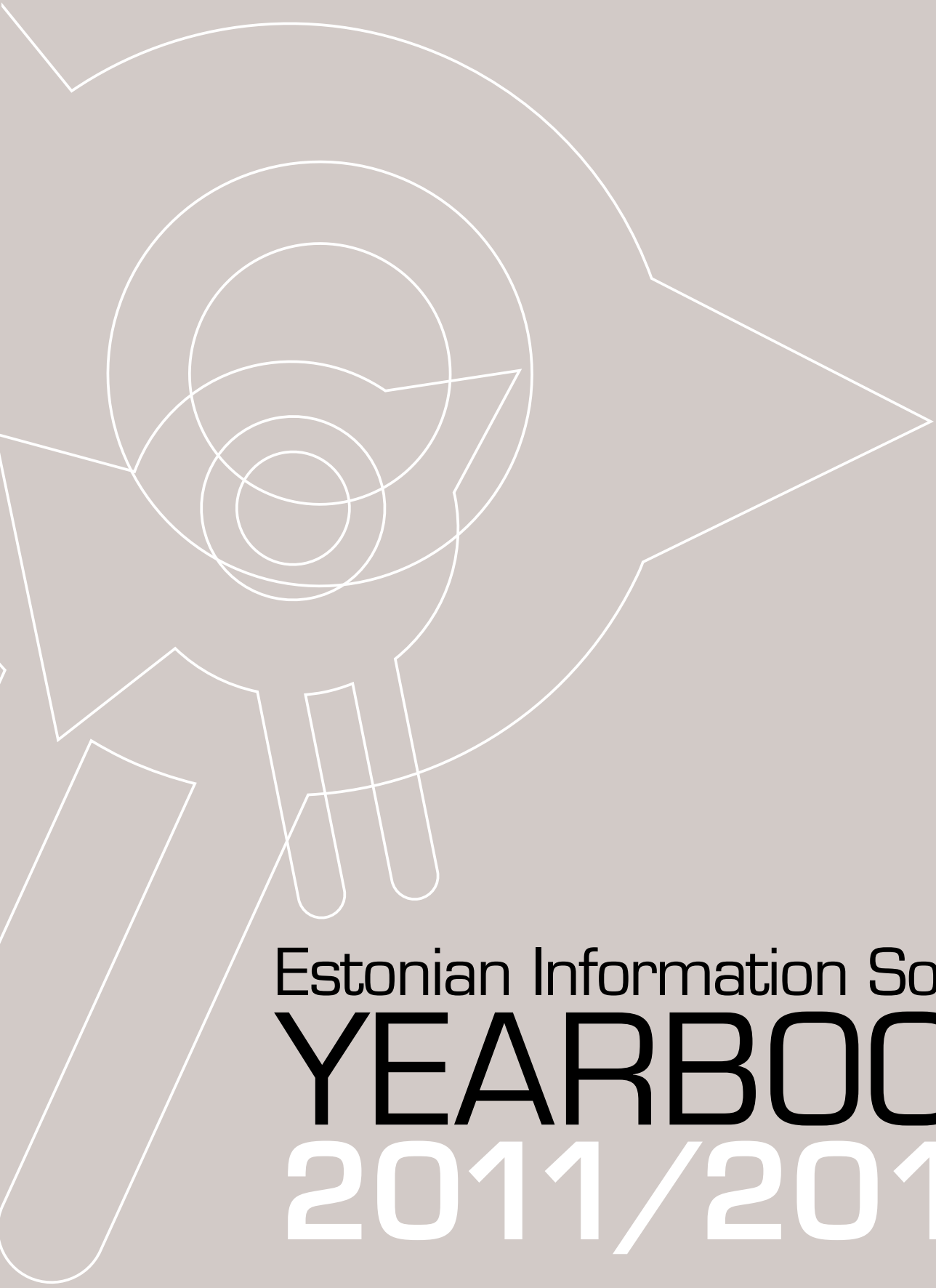
European Union
Regional Development Fund

Investing in your future



Estonian Information Society YEARBOOK 2011/2012

MINISTRY OF
ECONOMIC AFFAIRS AND
COMMUNICATIONS

Estonian Information Society
YEARBOOK
2011/2012

This publication has been funded by the EU Structural Funds programme „Raising Public Awareness about the Information Society“.
Compiled by Department of State Information System (RISO), Ministry of Economic Affairs and Communications.

Information Society yearbooks are available on:
www.riso.ee/en/ITyearbooks

Layout and design by Eva Unt, Director Meedia OÜ
Illustrations by Triinu Lille
Edited by Karin Kastehein, Director Meedia OÜ
Translated by A&A Lingua OÜ

ISSN 2228-3374

Contents


Internet
world
awareness
sector
Card
field
access
legal
Mobile-ID
study
programme
people
society
making
anniversary
competitiveness
more
launched
function
electronic
conference
democracy
eGovernance
working
ICT
possibilities
place
allows
media
changing
use
data
goal
across
during
open
first
age
Estonia
annual
service
Census
public
bring
system
information
project
over
population
candidates
comment
aimed
procurements
best
development
Ministry
Centre
authority
solutions
communications
Foundation
Cabinet
experts
study
areas
time
international
computer
best
election
during
cabels

A brief chronology of information society 2011 – July 2012

January 2011

A survey is published by the Praxis Center for Policy Studies and the eGovernance Academy at the behest of the Ministry of Economic Affairs and Communications regarding the possibilities of use of digital TV and mobile telephones for providing public services. http://www.riso.ee/et/files/DigiMobi_uuring_2011_final.pdf (in Estonian)

February 2011

The electronic public procurements environment is launched, consisting of an information website and public procurements register, that allows all operations related to public procurements to be conducted electronically in one place.
https://riigihanked.riik.ee

The state begins issuing mobile-ID certificates. Mobile-ID is an alternative to the ID card and enables electronic identification and digital signing by mobile phone. Mobile-ID can also be used for electronic voting at elections.
http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/mobiil-id
(in Estonian)

Garage48 is held: over one weekend, developers of Internet services come up with public services of benefit to society. The winner is 112 Mobile – a mobile and web service that can be used to contact emergency responders without making a call.
http://garage48.org/blogger/garage48-public-services-ideas-in-process

March 2011

Elections for the Riigikogu (Estonian Parliament) are held. For the fifth time, Estonians can vote for candidates electronically. The share of Internet voters sees continued growth, this time reaching 24.3% of all voters. For the first time, mobile-ID is one of the options for authentication, making voting especially convenient, as no ID card reader connected to the computer is required.
http://www.vvk.ee/valijale/e-haaletamine/e-statistika (in Estonian)

The Estonian Development Fund starts the Futututuba blog devoted to future trends. Foresight experts bring readers coverage of ideas from world-leading think tanks and research centres. http://www.futututuba.ee (in Estonian)

April 2011

The Government Office adopts use of the new information system for draft legal acts (EIS), which allows bills to be tracked as they make their way toward becoming law.

Documents in the information system can be retrieved and opinions on documents can be submitted during the public comment period. EIS can also be used by drafters to submit a draft legal act to the participatory website http://www.osale.ee for public comment before the endorsement process.
http://eelnoud.valitsus.ee (in Estonian)

A study conducted by the American human rights organization Freedom House ranks Estonia #1 in the world for Internet freedom. Estonia is followed by the US, Germany, Australia and Great Britain.
http://www.freedomhouse.org/report/freedom-net/freedom-net-2011

May 2011

The Estonian version of the open office software site LibreOffice meant for public use is launched, with Estonian-language user support and containing a wealth of interactive study resources. http://www.libreoffice.ee (in Estonian)

An analysis of the Riigikogu elections' online campaign is released. It examines how much political parties and individual candidates used the Internet, including social networks, to organize their campaigns during the run-up to the elections.
http://www.ega.ee/et/node/853 (in Estonian)

June 2011

The Estonian Informatics Centre is restructured into a national authority. The new functions of the Estonian Information System's Authority (RIA) include performing regulatory supervision of the security of vital service providers and the development of new information systems. http://www.ria.ee.

Estonia's electronic environment for filing annual reports wins first place at the World Summit Awards (WSA) 2011, an international competition recognizing creative use of digital media. The environment's interface makes it convenient for companies to enter and send data by providing a specific place, format and method for entering all required data. https://ettevotjaportaal.rik.ee

July 2011

The Environmental Board opens its e-services portal. The first electronic service offered to customers is a facility for compiling and filing declarations of environmental charges. https://eteenus.keskkonnaamet.ee (in Estonian)

August 2011

The first part of EstWin, a project to bring high-speed Internet to Estonia's rural areas, is completed. All of Estonia's cities – in particular, towns with a population of 1,000-10,000 – are now connected by fibre-optic cables. By 2015 Estonia should have a fully developed fibre-optic trunk network built so that 98% of households, companies and institutions are no farther than 1.5 km to a network connection point. To attain this goal, the Estonian Broadband Development Foundation will have to replace over 6,000 km of optic cables and establish over 1,400 network connection points. http://www.elasa.ee

September 2011

Tallinn hosts the international e-governance conference ICEGOV 2011. This major event, held under the aegis of the UN, brings together practitioners, entrepreneurs and academicians in the field of e-governance to discuss developments in the field and to share experience. The Estonian organizer of the event is the eGovernance Academy. http://www.icegov.org

The annual information society conference organized by the Ministry of Economic Affairs and Communications focuses on copyright in the digital age, and is titled "Õigus luua, õigus tarbida" (Right to create, right to consume). It discusses rights, obligations and opportunities related to use of digital content in a world of changing technological possibilities. http://infoyhiskond.eesti.ee (in Estonian)

October 2011

The information technology and telecommunication conference "From vision to solutions 2011" is held. The main topic is open data and competitiveness – it focuses on the necessity of freedom of movement of data and on business possibilities in this field. http://www.visioonistlahendusteni2011.ee (in Estonian)

The role of the public sector and its experience in social media are discussed at the seminar "Public authorities in the social media – friend or uninvited guest?" http://www.ega.ee/et/node/896 (in Estonian)

November 2011

The new and improved state portal eesti.ee is opened. The main keywords of the new version are usability and personalization. Searching for information and services has been made easier, and greater emphasis has been laid on availability of information in English and Russian. http://www.eesti.ee

The Internet and computer training project Ole Kaasas! (Come Along!) ends its three-year run, during which 100,000 people in Estonia gained new computer knowledge under the leadership of the look@world (Vaata Maailma) Foundation. In addition, the program introduced possibilities for using smart work possibilities at home and in the office, and 35 Ole Kaasas! computer clubs across Estonia were founded.
http://www.olekaasas.ee (in Estonian)

The Ministry of Economic Affairs and Communications creates a department for the development of information society services, with the aim of improving the quality and usefulness of public services developed in Estonia.
http://www.mkm.ee

December 2011

One of the pillars of e-governance in Estonia, the data exchange layer X-road, celebrates its 10th anniversary. The X-road is the means by which all of the state's public electronic solutions and key private sector e-services reach the public in a secure fashion. http://www.ria.ee/x-road

A study commissioned by the Ministry of Economic Affairs and Communications from Ernst & Young Baltic, "The Role of Green ICT in Enabling Smart Growth in Estonia", is published. The study assesses the level of awareness of green ICT areas and their potential in Estonia. The results form the basis for measures developed in the framework of the Estonian-Norwegian Green Industry Innovation programme.
http://www.mkm.ee/public/Inno_18_GreenICT.pdf

January 2012

The 10th anniversary of the issuing of the first ID card is marked. As of the beginning of 2012, 1.2 million people hold a valid ID card, of whom 85 percent are Estonian citizens and 15 percent foreign nationals. In ten years time, 72.6 million digital signatures have been given, and close to half of ID card holders have used the document electronically.
http://www.id.ee

The ICT Demo Centre, a joint project of Estonia's ICT companies, turns three. The Centre was established to increase the profile of Estonia as an e-state on the international arena and to accelerate the export of local ICT services and experiences. http://e-estonia.com

Estonia sets a world record for participation in an electronic census. A total of 62% of the population provides information for the Population and Housing Census online, beating Canada's respective figure by eight percentage points. http://www.stat.ee/phc2011

February 2012

Public debate over copyright in the information age and the ACTA (Anti-Counterfeiting Trade Agreement) becomes more vocal in Estonia. An Estonian Internet freedom manifesto is developed in this period. The goal of the paper is to initiate discussion in society on the topic of fundamental rights of Internet users. http://mottehommik.praxis.ee/uued_teesid (in Estonian)

The Estonian Information Technology Foundation (EITSA) starts implementing a national programme on higher ICT education and research and development in the field. Its goal is to raise the quality of Estonia's higher education in ICT as well as its international competitiveness and R&D capability in the field. http://www.eitsa.ee

March 2012

The Association of Information Technology and Telecommunications spearheads an "IT Night" where hundreds of active-minded young Estonians across the country come up with ideas how to make school life more exciting through IT. The event is part of the project designed to popularize IT specialities, called Kõik on IT, a play on words meaning literally, "Everything is IT".
http://startit.ee/it-oo-2012-valminud-tood (in Estonian)

On 14 March, the Estonian ID card reaches 500,000 unique electronic users.

April 2012

Estonia joins the Open Government Partnership, aimed at supporting democracy, economic development and cooperation with NGOs.
http://www.opengovpartnership.org

A 3D virtual model of Old Town Tallinn is launched, allowing people to see the capital's cultural sights and its food, drink and accommodations providers in a new way.
http://3d.tallinn.ee

May 2012

The e-democracy conference "Demokraatia muutuste keerises" (Rapidly Changing Democracy) is held. Among other things, the conference discusses what constitutional democracy must be like in an information society and how people see their role in a democratic system. http://infoyhiskond.eesti.ee (in Estonian)

The Cabinet forms an Information Society Council, replacing the Estonian Informatics Council that has served since 1996, and updates its functions and composition. The council's functions include presenting positions and advising the Cabinet in important matters pertaining to development of information society.

President Toomas Hendrik Ilves, the head of the European Union's working group on e-health, presents an overview of the working group's report, entitled "Redesigning health in Europe for 2020". The working group led by the Estonian president includes healthcare experts, patients, representatives of medical, pharmaceutical and ICT industry, legal experts and policy makers from various countries.
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/453&aged=0&language=EN&format=HTML&guiLanguage=en

June 2012

Estonian Public Broadcasting's mobile app ERR is declared overall winner of the competition "Estonia's best m-service 2012" and winner of the entertainment and media category. It can be used to access all Estonian Public Broadcasting livecasts of television and radio programming as well as access an on-demand archive.
http://www.m-konkurss.net/eng

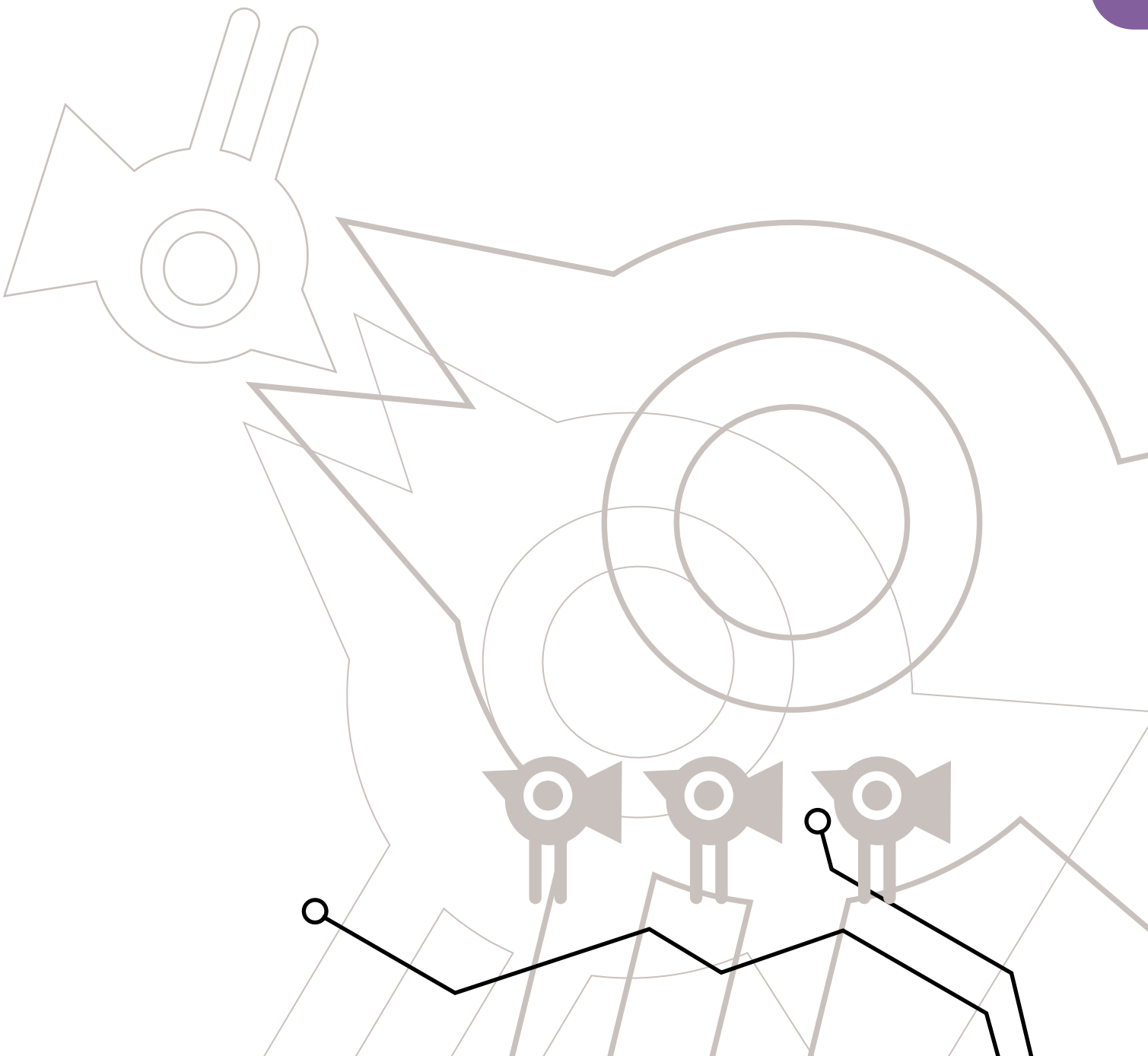
In the framework of the EU Structural Funds programme "Raising Public Awareness about the Information Society", the eGovernance Academy completes its guidelines for developing web-based communication at local governments. The guidelines focus above all on making use of existing technical solutions more effective, addressing

both local governments' service portals and social media platforms. http://www.ega.ee/files/Soovitused%20kohalike%20omavalitsuste%20veebi-suhtluse%20interaktiivsuse%20t%C3%B5stmiseks.pdf (in Estonian)

July 2012

An application round for funding projects aimed at making public data open to re-use is launched. Assistance is provided for transforming information systems so that information is available in machine-readable form over the Estonian open data site opendata.riik.ee. http://www.ria.ee/36610 (in Estonian)

The proposal to prepare the information society development plan 2020 enters the stage of consultations. The goal is to agree, in partnership with private and third sector, how to best use ICT to raise Estonia's competitiveness and improve people's well-being. http://ww.infoyhiskond.eesti.ee (in Estonian)



CHAPTER 1
OPEN DATA

No country in the world can afford to disregard the topic of open data. Such data has become a part of our everyday life – already now, public sector institutions generate various kinds of data in digital form – a tantalizing source of raw input for all sorts of new services and products. Open data refers to machine-readable data that is available to everyone to use freely and publicly, with no restrictions on use and distribution. In fact, Estonia's Public Information Act obliges the public sector to make information available to the public either through websites, document registers or databases. This chapter looks at the topic of open data and the principles governing the domain both in Estonia and in other countries.

Open data – a step toward the Internet of the future

UUNO VALLNER
uuno.vallner@riso.ee
Ministry of Economic Affairs and Communications

The principle of open data and open government became buzzwords at the dawn of the 21st century. Since that time they have become areas that impact all of society. Open data is the first stage in moving toward the so-called Internet of Things and an interlinked world. Movement of data is seen as a way of dealing with "big data" in the future.

Here in Estonia, too, the goal could be a "linked Estonia" – an interoperable Estonian-ICT-developed network of individuals, organizations, devices, knowledge, information systems and linked data. Creating it will require a breakthrough on such fronts as high-speed data networks and smart devices, interoperable information systems, knowledge networks, semantic networks, linked data, open government technologies (open standards and data, free software).

Open data for re-use

Public sector institutions generate, collect or retain a large quantity of data and information, such as statistics, spatial data, economic figures, environment data, archive materials, books and art collections. Today these resources are to a very great extent digitized and represent a major asset for development of new products and services where they are used as raw input. There is particular interest in re-use of dynamic data in public sector registers.

According to a study commissioned by the European Union[1] if the public sector information in the EU's 27 countries moves toward greater openness and easier access, it will be possible to achieve economic benefits translating into around 40 billion euros per year. The market for re-use in Europe is growing 7 to 40 percent a year. Vice-President of the European Commission Neelie Kroes has called open data "new gold"[2]: "If oil was black gold, re-use of data could be new gold for Europe." Opening public sector data will allow the private sector to mash them up with other data and create new commercial services with value added. The public sector could focus on its main activities and discontinue competing with the private sector. But presenting data in a re-usable form will mean expenditures. Based on the European Commission study, 1.4 billion euros of public sector investments would increase Europe's GDP to 140 billion euros. Thus every cent invested will increase a country's GDP by a euro.

Open data: a rediscovered gold mine

The topic of data re-use is not new. It began to be talked about in the late 1950s. During the Soviet era, the Information Institute re-used one million records a year[3] of reports on magnetic media. The first instance of re-use of a register in re-independent Estonia was the technological solution for the State Gazette developed in 1995-1996. WordPerfect office software was used in

this case to publish it on paper. The WordPerfect files were converted into SGML (XML is a derivative of SGML), digitally signed and opened via ftp server for free public use. The more active re-users of legal acts were the Government Office's document management system, the State Gazette's online database, IBS search system and EstLex. In recent years, many countries have discovered that opening data is a path to economic stimulus and they have launched extensive projects that support re-use of data:

- The European Commission's policy on open data[4]
- Study commissioned by the Commission: "Towards a pan EU data portal – data.gov.eu"[5]
- Principles of open data in Great Britain[6]
- Principles of W3C open data[7]
- Recommendations of the Open Government Data development group[8]
- US and UK. Recommendations to the OECD with regard to open data policy[9]
- OFKN Open Data manual (legal affairs, social affairs, technology)

Many countries, regions and local governments have created frameworks for re-use and websites that simplify re-use:

- European open data directory: http://publicdata.eu
- US open data directory http://data.gov
- UK open data directory http://data.gov.uk
- Australian open data directory http://data.gov.au
- Canadian open data directory http://data.gc.ca
- Kenyan open data directory http://opendata.go.ke
- Norwegian open data directory http://data.norge.no
- Dutch open data directory http://data.overheid.nl
- New Zealand open data directory http://data.govt.nz
- Italian open data directory http://data.gov.it
- French open data directory http://data.gouv.fr
- Swedish open data directory (initiative of an individual) http://www.opengov.se
- Philadelphia area open data directory http://opendataphilly.org
- Helsinki Region Infoshare http://www.hri.fi/en
- CKAN open data directory repository http://thedatahub.org

Although opening data for re-use will result in additional expenditures, politicians have recognized the strong influence it will have on national economies and have started actively investing into the creation and development of open data. On his first day in office, US President Barack Obama signed a memorandum on an open and transparent government under which the public sector opened its data for re-use. By autumn 2011, the US open data directory consisted of 390,000 data sets.

What is open data?

Open data and data sets. Data published for re-use is called open data. This term covers machine-readable data that is freely available for everyone over websites and which is not protected by patents or restrictions on use or distribution. If legislation does not specify a fee for obtaining the data, the open data can be obtained free of charge and without access restrictions.

Formats that can be opened and modified by freeware applications are also well-suited for re-use.

The Public Information Act[10] makes it obligatory to release to the public, via a government department's website, document register and databases, the department's unrestricted information. In addition, the public sector has the obligation of releasing information in response to requests for information. Here we take open data to mean information that is presented to the public in proactively opened formats. But in general, no request for information need be submitted for downloading open data.

Publication of officially generated data has several important objectives, the most specific one being the interest of individuals, companies and the third sector to merely view existing data or use it in software developments to generate value added in some field.

All data generated by both government departments and local governments and the public use of which is not expressly prohibited and which contain data other than personal data is subject »

» to being made public. With regard to data that consists of both personal data and other data, only the latter part is made public.

In the context of open data, data that comprise an integral whole is called a dataset. This includes contract texts, regulation texts, collections of metadata on correspondence, budget and statistics files, databases converted to open format or open network services that issue data from registers. It is not reasonable to treat individual agreements and regulations as a dataset, unlike individual databases. In the case of some datasets, it is sufficient for the user to have access to the data (for reading or copying) while in the case of others there may be a strong interest to re-use the data. Below, the fields are arranged (pursuant to the OECD's 2006 analysis) according to their re-use value in ascending order:

- culture (libraries, archives, museums, broadcasting)
- politics (press releases, strategies, green books)
- education (lectures, textbooks and study materials)
- science and research (research at universities, institutes and public sector)
- legal information (court, legal acts, patents, trademarks, rights and obligations)
- nature (biology, ecological, geological and geophysical information, information on energy resources)
- agriculture, forestry, fishing
- tourism, accommodations and entertainment
- traffic, transport
- social information (statistics, demographics, health, education)
- business and the economy
- meteorology, environmental information
- spatial data

Technically, the dataset published may be a collection of human-readable text files (such as a collection of legislation or regulations, official notices or contracts) or machine-readable data (such as a database of files exported to csv or xml format or a web service that allows all data to be searched for and downloaded in json or xml format).

A dataset is, in the technical sense, a collection of human-readable text files

The user must be able to do the following:

- browse and search public datasets for a dataset of interest;
- download a dataset found as a whole or, via the search system offered by the services, in parts without having to negotiate for rights or obtain passwords. In an exceptional case, a fee may be charged for the downloading of a dataset;
- to continue to use the database freely, with the right to download it into one's computer and using it in applications (in free and paid applications) without having to pay (additionally) for it or needing permission to do so.

A public sector institution that creates and publishes a dataset has no obligation to offer data users additional amenities such as conversion to a suitable format, building special network service, translation etc. Nor do officials have the obligation to ensure that data is correct or up to date. Instead, the publisher has to explain in brief the nature of the data and document the expected frequency of the updates.

Licence and fee for dataset. An open dataset must have a licence that allows it to be used, processed and distributed free of charge and without restrictions, either free of charge or for a fee – at the user's discretion. Specifically, we recommend that a creative commons licence be selected as the licensing option[11]. Above all, from this list, we recommend CC by 3.0 licence[12]. This means that in licensing a work, the licensor is the author or the copyright holder, but the licensee is the public at large. You have the right to copy a work (reproduce it), distribute, perform and direct it at the public, and to adapt, arrange and develop it otherwise, including derivative works, on condition that the author is credited.

Open data is published advisably for free download, but the publisher has the right to charge a fee for loading the data in cases set forth in legislation.

Principles for publishing datasets. When publishing data, a compromise between two objectives must be found:

- convenient usability and comprehensibility of the data for the data seeker and the downloader,
- simplicity of publishing data and minimizing the work expenses for the publisher.

To do so, the first task is to find the easiest, simplest and most rapid way of publishing the existing data as such and only then to examine

Tim Berners-Lee format level scheme on a "five-star mug" http://www.cafepress.com/w3c_shop

ways of creating user friendliness for information seekers and downloaders. In other words, updating data, converting and other operations are to be tackled only once the dataset has been published.

Data can be updated and converted by a third party as well, who in turn receives the right to share the data free of charge of for a fee. The open dataset conforms to the following requirements[13]:

1. **Integrity.** All public data shall be made available. This includes all data not subject to personal data restrictions etc.
2. **Comes from original source.** The data has been gathered from the original source without modification, preserving their original format and level of detail. As with databases, it is not permitted to take data from a secondary database.
3. **Up-to-dateness.** The dataset was published as rapidly as possible to preserve its up-to-dateness.
4. **Availability.** The data is available to as wide a circle of users as possible with as wide a range of use as possible.
5. **Machine-readability.** The data has an understandable structure and can be automatically processed.
6. **Avoidance of discrimination.** The data is presented publicly, no need to register or seek access privileges in order to obtain it.
7. **Use of open standards.** The data is presented in an open format that is not the exclusive property of any one company or person.
8. **Free licence.** The data is not under copyright, patent, trademark or business secret protection. Reasonable privacy and security restrictions are permitted.

How to publish?

In what format? The main principle here is that it is much better to publish data in an inconvenient coding than to not publish them at all on the consideration that it is planned at some unspecified time to improve the coding. Secondly, a published data set can always later be published in a new, better code.

We recommend evaluating the user-friendliness of formats and coding formats based on Tim Berners-Lee's five-star system principles[14] – the more stars the user-friendlier format. The distribution of formats given Estonia's circumstances could be the following:
* data is available online in any format (e.g. .jpeg, .pdf, .doc, .docx, .xls.). Data cannot be separated from the file or it is presented in formats oriented at proprietary software;
** data is on the website in open format (e.g. .txt, .html, odt), but in unstructured form;
*** data is presented on the website in open and free format (e.g. .csv, .xml, ods files);
**** the objects in the data are identified by URIs[15];
***** the data are linked to other data using URIs.

Publishing of data sets is best done in formats that can be opened and processed using freeware applications. This includes .odt format document files as well as some of the most »

» common formats for structured data, like .csv, .json and .xml.

Formats that can be opened and modified by freeware applications are also well-suited for re-use.

Situation in Estonia

In Estonia as well, there is now considerable political will to make public sector information more reusable. And thus the government's programme[16] in the section on "From E-state to I-state" has a subsection devoted to open data entitled "Putting the state's e-resources in the service of citizens and companies". The government programme promises the following explicitly:

- we will make the state's spatial data public in modifiable form – this will give citizens and companies the possibility to develop purposeful services on the basis of government data;
- to increase transparency and inclusion and stimulate the private sector to develop new applications, we will make public data – i.e. state and local government data machine-readable;
- we will set the aim of making databases created collaboratively between private and public sector available to companies and individuals for development.

Estonia is home to an open data community[17], and it has a page on Facebook. A movement called Garage48 is active in preparing services, and their motto is "less talk, more action". The Association of Information Technology and Telecommunications initiative is also to be reckoned with their 2011 conference "From vision to solution" focused on obstacles to developing new e-services.

In Estonia, the availability of public information can be rated exemplary. As the fairly liberal Public Information Act[18] makes it obligatory to release to the public, via a government department's website, document register and databases, the department's unrestricted information, more information than in most other countries is subject to being made public. For instance, every public sector institution must release information on their structure, salaries, document register, reports, statistics, budgets, development plans. The Public Information Act distinguishes between 32 types of information to be published. Considering that Estonia has 2,000 public sector institutions and each one of them should publish an average of ten datasets, the volume of reusable information is at least 20,000 datasets.

But unlike most countries, the public sector is not required to publish information in reusable form. The published datasets are not always in open formats. The primary formats used are PDF and MS Office (proprietary software) oriented formats. Thus this is predominantly one-star data.

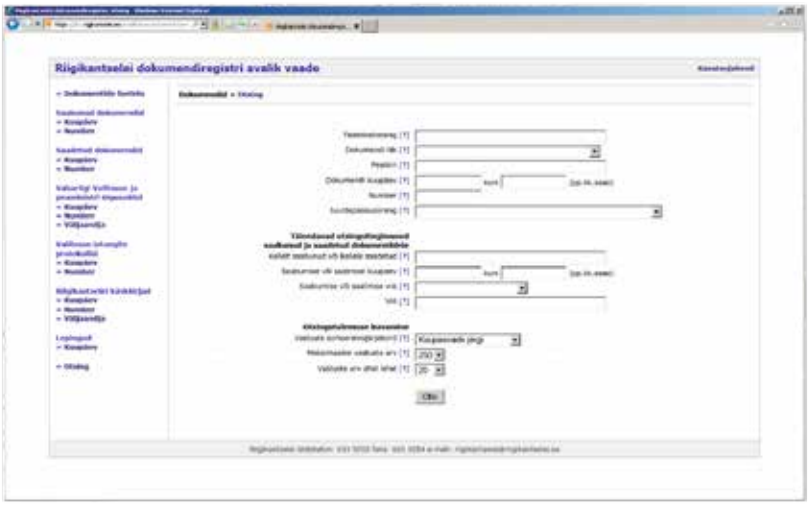
Public sector information is stored in databases. But public databases and their open service interfaces are unspecified and thus hard to re-use. There is no legal requirement that descriptions of such registers and their services be published in the state information system's management system (RIHA). For instance, the Government Office's document register has been realized in model fashion, its output is xml data, but the data and the search interface as well as the option of saving output as in xml format has not been described to potential users. Submitting to the document register the query: https://dhs.rigikantselei.ee/avalikteave.nsf/contractsbydate?open&path=2011/12|Detsember, we get the response in the following form:

<document noteid="NT0017AE7E">
<field name="date">30.12.2011</field>
<field name="docid">L11165</field>
<field name="subject">Trükiste kujundamine ja trükkimine</field>
<field name="documenttype">Töövõtuleping</field>
<field name="contractstartdate">30.12.2011</field>
<field name="contractenddate">20.01.2012</field></document>

But the Government Office document register is a positive exception to the rule. Most registers of this type output HTML text that cannot be processed directly for re-use.

Public services will not do away with the need to download. For the most part, Estonian public services lack search result download facilities, to say nothing of mashup options.

Pursuant to the Public Information Act, the data processed in a database must be publicly available, if there are no access restrictions on them established by or deriving from law. But personal data in a database is not to be published unless there is an obligation to do so under law. Thus speed camera data, and incidents registered by the police, among other categories of information, should be public, as long as the personal data is redacted. Estonian public sector has mainly disregarded this requirement and the public part of registers that contain personal



Sample query to the Government Office's document register

data have been left unpublished, to say nothing of their presentation in a reusable form.

The options for re-using public data from registers that contain personal data are modest.

Estonian open data is scattered in institutions. The most important generators of open data:

- Land Board – geoportal: http://geoportaal.maaamet.ee
- Environmental information centre: http://www.keskkonnainfo.ee
- Statistics Estonia: http://pub.stat.ee/px-web.2001/dialog/statfile2.asp
- National Library digital archives DIGAR: http://digar.nlib.ee
- National Archive digital archive.

One route to making availability of open data simpler and better organizing presentation of open data would be the open data repository currently in pilot stage, http://opendata.riik.ee.

1 http://epsiplatform.eu/content/review-recent-psi-re-use-studies-published

2 Speech by Neelie Kroes "Data is the new gold" 12.12.2011: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/872&format=HTML&aged=0&language=EN&guiLanguage=en

3 Uuno Vallner. Retrospektiivsed otsisüsteemid (Retrospective search systems). Tallinn, Estonian Information Institute, 1985 (in Estonian)

4 http://ec.europa.eu/information_society/policy/psi/index_en.htm

5 http://ec.europa.eu/information_society/policy/psi/docs/pdfs/towards_an_eu psi_portals_v4_final.pdf

6 http://data.gov.uk/opendataconsultation

7 http://www.w3.org/TR/gov-data

8 http://www.opengovdata.org

9 https://usoecd.cms.getusinfo.com/data.html

10 https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv (in Estonian)

11 http://creativecommons.org

12 http://creativecommons.org/licenses/by/3.0

13 http://www.opengovdata.org/home/8principles

14 http://lab.linkeddata.deri.ie/2010/star-scheme-by-example

15 http://en.wikipedia.org/wiki/Uniform_resource_identifier

16 https://valitsus.ee/UserFiles/valitsus/et/valitsus/tegevusprogramm/valitsuse-tegevusprogramm/Valitsusliidu%20programm%202011-2015.pdf (in Estonian)

17 http://www.opendata.ee

18 https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv (in Estonian)

Open data repository

UUNO VALLNER
uuno.vallner@riso.ee
Ministry of Economic Affairs and Communications

TANEL TAMMET
tammet@staff.ttu.ee
Tallinn University of Technology

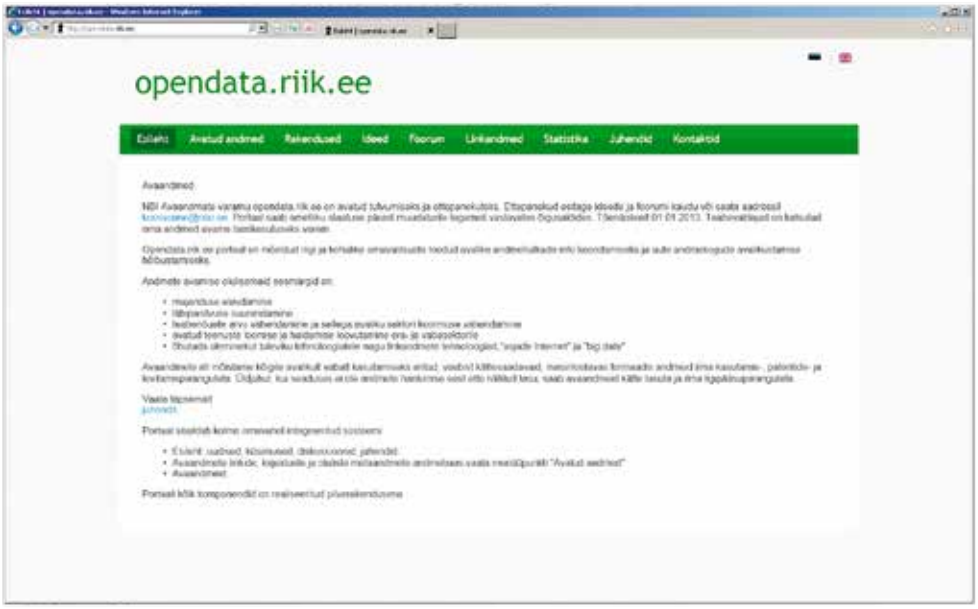
ALEKSANDER REITSAKAS
aleksander.reitsakas@aktors.ee
Aktors OÜ

To improve availability of open data and coordinate posting of open data, a pilot interface has been developed for an open data repository at http://opendata.riik.ee. Metadata for the public sector's open data should be uploaded there. Public departments and agencies can also upload data sets here if they so choose.

Repository for open-source data

From the standpoint of open data, what Estonia's public sector needs the most are changes in legislation as well as organizational and technical principles. With this in mind, project Open Data Framework was launched for 2011-2012. A procurement was held to develop infrastructure for supporting making data open and for laying the organizational, technical and semantic preconditions for going open. The following were the planned outcomes of the procurement:

- developing a website at opendata.riik.ee (beta) as Estonia's information gateway for access to and use of open data;
- creating infrastructure for publishing data (repository; beta);
- specifying, in cooperation with open data communities, the preliminary organizational, technical and semantic requirements for open data;
- the cloud solution CKAN was recommended to power the central repository (http://ckan.net);
- the cloud-based Drupal search engine was recommended as the front-end system (http://drupal.org);
- Apache SOLR was recommended as the search engine



Front page of the pilot application of the open data website

(http://lucene.apache.org/solr);
- interfaces that support RDF and SPARQL standards were required;
- a LAMP platform was required;
- interoperability with other repositories was required;
- it was assumed that institutions could establish their own repositories, but the central repository had to be capable of picking metadata from them;
- it was presumed that institutions could load datasets directly to the central repository.

The pilot version of the central open data site can be found at http://opendata.riik.ee. The site consists of three integrated systems:

- A site for news, questions, discussions and manuals where manuals and news can be posted, questions brought up and discussions on the open data topic can be held.
- A CKAN-based database of open data links, specifications and key metadata (see http://ckan.org), which can be linked to from the menu item Open Data on the site's upper menu bar. The following can be retrieved from this database:
  1) open data can be searched and downloaded: without access restrictions;
  2) new open data can be added (registration and user privileges from administrator required).
- A repository for datasets, which is one of the possible places where a government department can save open data.

Technically, preconditions have been created for developing open-data infrastructure. But technical solutions are not enough. It will be necessary to staff and train a team to be capable of administering and developing infrastructure and performing supervision; their activity should also encompass public sector data generators as well as open-data communities that develop services.

How to publish?

In what format? The main principle is that it is much better to publish data in an inconvenient encoding than to not publish them at all on the consideration that it is planned at some unspecified time to improve the encoding. Secondly, a published dataset can always later be published in a new, better encoding.

In the context of open data, we recommend evaluating the user-friendliness of formats and coding formats based on Tim Berners-Lee's five-star system[1] principles, which are described in the previous article. Publishing of datasets is best done in formats that can be opened and processed using freeware applications. This includes .odt format document files as well as some of the most common formats of structured data, such as .csv, .json and .xml.

Formats that can be opened and modified by freeware applications are well-suited to re-use.

The use of **one-star formats** for opening data is to be avoided. But on the other hand publishing »

»» them as such is certainly better than not publishing them at all.

Two-star formats are used primarily for data where all that users need is access to the data. Re-use means, above all, viewing and cutting and pasting of data. To ensure development of services, the open data should be presented in a three-, four- or five-star format.

Three-star formats. Three-star data should advisably be in one of the following formats, depending on whichever is more convenient for the data publisher. From the user standpoint, there is not much of a difference between these formats, but it would likely be most convenient to use .json.

- csv files. The documentation must specify the alphabetical encoding, whether comma/semicolon is used as delimiter and whether a period or comma is used as the decimal point. Files should advisably have a header listing the names of the fields. And certainly the official[2] csv format should be used as the basis, along with nuances as regards quotation marks etc (see http://en.wikipedia.org/wiki/Comma-separated_values).
- json files. Same requirements for language encoding standards.
- xml files.

Preconditions have been created for developing open-data infrastructure.

Four-star formats. The principles are the same as in the case of three-star data, but the primary difference here is that globally unique identifiers – URIs or uniform resource identifiers – are to be used to identify objects. The use of uniform identifiers makes it much easier to use data across different systems.

To adopt URIs, a dataset prefix is to be added to each object-identifier during data export, for instance http://institution.ee/nameofdataset/objects/, where the full URI would be http://institution.ee/nameofdataset/objects/45321 and 45321 the object's original ID in the dataset. If the IDs are not unique for their own data set (which is the most usual situation) the easiest would be to express URIs during export in a form where the name of the relevant table is added instead of "objects", for instance http://institution.ee/nameofdataset/naturalpersons/.

Once objects have begun to be presented as URIs, it would be suitable, besides use of csv/json/xml, to express data in the form of RDF - as entity-attribute-value triplets[3].

As data can be appear in various syntaxes in RDF, we advise using one of the following two:

- Microdata[4], which is for encoding data into html to be read by humans: information can simultaneously be easily parsed by humans and is also readily machine-readable.
- RDFa[5], which is analogous to and has the same objectives as Microdata, but is slightly more complex.

Data in Microdata format can always be converted into RDFa with little trouble. The next question after the Microdata/RDFa issue is the selection of field names – the names of object properties. There are two main approaches.

- The simplest way would be to express pairs of table/field names of the original dataset in the form of URIs, for instance: http://www.institution.ee/nameofdataset/nameoftable/nameoffield, an example being http://www.institution.ee/permitrecipients/naturalpersons/dob (www.institution.ee/permitrecipients/naturalpersons/dob).
- A slightly more complicated but potentially also more useful alternative would be to use, instead of the table/field name in the original system, the more general and common property name, if there is one. Schema.org is a suitable collection for searching for names. Note that if no suitable name is found, users will find it very easy later on to convert exported names to a form suitable for their purposes, on condition that they can understand the meaning of the exported field name.

The topic of ontologies should be addressed as well in discussing how field names should be expressed. They may be viewed as rules for converting/classifying field names; for instance if we want to say that our field name in the form of the URI http://www.institution.ee/permitrecipients/naturalpersons/dob is precisely the same thing as schema.org's Thing>Person>birthDate.

From this view, the ontologies for publishing data are not a directly relevant or complicated topic;

rather, they are more of a useful tool for application developers who mash up data from different sources. With regard to exporting data upon publishing, it would be expedient to write ontologies oneself either for documenting one's field names or to convert a subset's existing field names to schema.org names.

Five-star formats. One way of linking data URIs is to use, instead of the identifier used in databases, a de facto more universal global identifier – the URI. Let us suppose that the state agrees on (or that the Population Register and Business Register adopt the use of) a format for personal identification codes and Business Register codes consisting of http://prefix1.ee/prefix2/personalIDcode and http://prefix3.ee/prefix4/companycode. In such a case, the five-star representation of personal and company codes would be through URIs where prefixes/URI formats are not the company's own but, rather, the formats more broadly agreed upon. The same goes for names of database fields – names of object properties.

How should a dataset be published in practice? There are three main technological ways of publishing data.

- For human-readable files, the directories containing the files are packaged, a short content description is added and the packaged directory (directories) are uploaded in freely downloadable form advisably on the institution's website, http://<asutuse domeeninimi>.ee/avaandmed (http://<institution domain name>.ee/opendata) or in the opendata.riik.ee directory.
- In the case of data in databases, export the database content into a text format structured as xml or csv or json files etc and then implement the simple package-and-upload-to-web-server method. If the database contains personal data not subject to disclosure, the fields are simply not exported.
- As an alternative, the data in the databases may be published as a free web service that can be used to find and download the entire content of the dataset or a filtered partial set. Network service can be SOAP service, but the most preferred ones are simpler, for instance json-based REST services, as well simply csv format-issuing services with get or post input parameters.

The data must be described in reasonable manner, i.e. a person with no previous experience with the dataset but who understands the field and the technology must, with reasonable exertion, be able to understand the purpose, structure and content of the dataset.

The dataset must include description of the principles for updating the dataset and the planned frequency of the updates. The publisher of the dataset has no direct obligation to regularly update the dataset – it is important to record the update plan (or lack thereof) in writing in comprehensible fashion.

The datasets published by the institution must be easy to find. To do so, at least two means of publishing the existence, descriptions and download links to the data must be used.

- A special directory on the institution's own website, /avaandmed (/opendata), such as http://www.institution.ee/opendata.
- National consolidated open data site/repository http://opendata.riik.ee.

1 http://lab.linkeddata.deri.ie/2010/star-scheme-by-example/

2 http://en.wikipedia.org/wiki/Comma-separated_values

3 http://en.wikipedia.org/wiki/Resource_Description_Framework

4 http://en.wikipedia.org/wiki/Microdata_%28HTML%29

5 http://en.wikipedia.org/wiki/RDFa

Open Spatial Data

KRISTIAN TEITER
kristian.teiter@maaamet.ee
Estonian Land Board

What are spatial data?

Simply put, spatial data are data with a geographic location and form. Such data are also called geodata, geoinformation and location data. As a rule, spatial data are presented and used in the form of a map that can be considered the spatial data output of a database. For instance, one of the outputs of the topographic data administered in the Topography Database of Estonia is topographical maps, but the data themselves can be used and made available online in xml format.

Fields that account for the principal use of spatial data are environmental protection, planning, construction, logistics, transport, the military and statistics, to name a few. More and more potential is seen in location, and the use of spatial data in different walks of life is seeing explosive growth.

Address data is also spatial data. It appears that, thanks namely to address data, a number of database administrators have recently been surprised to learn that their database contains spatial data.

Publication and re-use

Compared to Europe and the rest of the world, spatial data that can be treated as public information are public in Estonia. The Land Board, being the largest state map producer and administrator of spatial data, published cadastral unit data, administrative boundaries and topographic basic maps back in 2001 via the Web-based map server (http://geoportaal.maaamet.ee/). In 2008, Web-based map services (WMS) were added to the public map server; the Land Board's maps can be accessed through these services using various GIS/CAD software. The map server and services are very popular, with a total of 500,000 visits per month.

A second example we can cite is the Environmental Information Centre, whose website displays all sorts of environment-related spatial data. One example is the forest register's web service.

The difference between publication and re-use is mainly the fact that published spatial data can be viewed, queried, searched and, to a limited extent, downloaded as an image and printed. The possibilities for using spatial data in re-usable form are unlimited and as a rule they can be downloaded as databases in the suitable format. Making spatial data available specifically in re-usable form creates the preconditions for the private and third sector being able to use public sector information for developing new and interesting services and applications.

With regard to availability of reusable spatial data, Estonia presents a variegated picture. Some re-usable spatial data covering all of Estonia are easily available; there are other kinds that are difficult to access for several reasons. Availability of data varies both from one agency to the next as well as within a given agency.

Conformity to open data principles

The following is my subjective assessment of the conformity of Estonia's spatial data situation to selected open data principles. But the fact that these are spatial data does not have particular importance in this situation. Rather, the technological capability of database administrators,

legal regulations, historical customs and other factors have influenced the situation.

One principle is that data have been gathered from original sources without processing and they have retained their original form and level of detail. This is a principle that was more problematic in the case of spatial data 10-15 years ago, but today it is generally no longer an issue. It took time before spatial data users understood that it was in their own interests for spatial data from information holders to be from the original source and up to date. Paradoxically, the implementation of open data policy in Estonia could make the situation even worse. In using applications developed by third parties, end users no longer have a direct link to the data generator – the original source. Nor do they know how different the spatial data visible to end users are compared to data that the developer pulled from the original source. While it is true that developers of open data policy are concerned about whether all interested parties – developers and creators of value added – can access data, including spatial data from the original source, it has not in any way been determined what happens to the data after the developer processes them and resells them. It will be likely left up to the market – and end-user awareness – to regulate the area.

Principles worth mentioning include machine-readability, up-to-dateness of data and use of free standards. These are principles where conformity can be ensured largely using technical means. In Estonia, many databases that include spatial data were established only 20 years ago, they can be administered in machine-readable form, not as scanned sets of historical documents. This is a big difference and advantage compared to Western Europe, where states have had to spend noteworthy sums on digitization and vectorization of maps. To ensure up-to-dateness of spatial data between the information holder's database and the place where the spatial data will be available in re-usable form, the state's open data consolidated site to be established will likely be an aid, allowing the data user to be sure that the data he or she downloaded are identical in the information holder's database. A more troublesome question is whether the data in the information holder's database are up to date and reflect reality.

In the case of open data, importance is placed on the principle that the data be presented in an open format that is not the exclusive property of any one company or person. A propos of the needs of spatial data users in Estonia, we should mention that users wish to obtain data in a format compatible with their GIS/CAD software. Converting spatial data from one format to another is an inconvenience that causes dissatisfaction even if the software enables conversion. Estonia makes use of both proprietary GIS software from specific manufacturers and freeware GIS programs, the latter being less common. Thus open spatial data should be available in the formats that are predominantly used, including in some producer-centred and closed as well as open format.

Open data policy will be effective if it proved possible to unify access, release and terms of use and fee-charging principles for public data in re-usable form nationwide.

As the last group, we can mention open data principles dealing with rights, restrictions and availability of the use of the data. For many reasons these aspects are regulated quite inconsistently in Estonia. The Public Information Act establishes a single set of principles for publishing data. With regard to spatial data, the Spatial Data Act governs questions of availability, the Act reflects the principles of the INSPIRE directive. The Spatial Data Act obliges information holders to make the spatial data they administer available via services (including download services) that conform to specific requirements, and in a format that likewise conforms to specific requirements. At the same time, the Act leaves the terms and conditions and procedure for distributing information – i.e. user privileges and licensing matters – open and empowers the minister in whose area of government a given database resides.

In large part, matters pertaining to use of data are governed by the relevant legal acts. The principles that pertain to requesting data from data sets and conditions for use of data are set forth in many legal acts, and it is difficult to orient in this landscape. »

Money

Should public information be available free of charge in re-usable form to all or should people pay for it? How much should the fee be? These questions are at the centre of passionate debate in Estonia and throughout the European Union and are also salient among information holders administering spatial data.

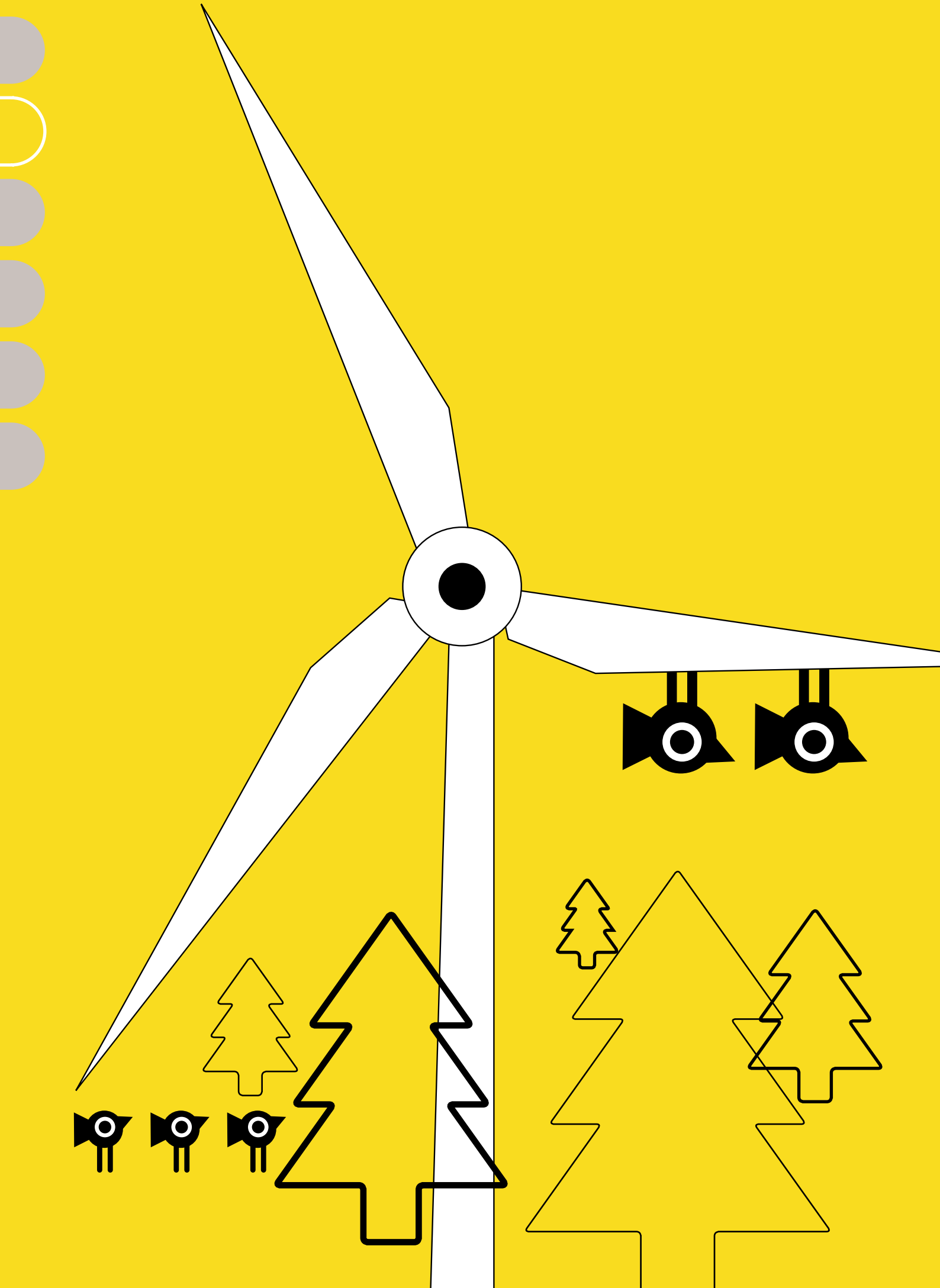
For public sector information holders, spatial data from other information holders are available free of charge in Estonia. The situation varies greatly in terms of fees for data for the private and third sector. If we generalize (and do not distinguish what the fee is being charged for exactly – provision of service, issue of spatial information or other services) we can say that the fee and fee levels vary by data set. For instance the Spatial Data Act establishes fees for Topography database, but there is no fee charged for certain environmental data, such as Forest Register data, which can be freely downloaded from the Environmental Information Centre page. Or, for instance, address data are free of charge for all in re-usable form from the Land Board site, but the State Fees Act establishes a fee for releasing cadastral unit data.

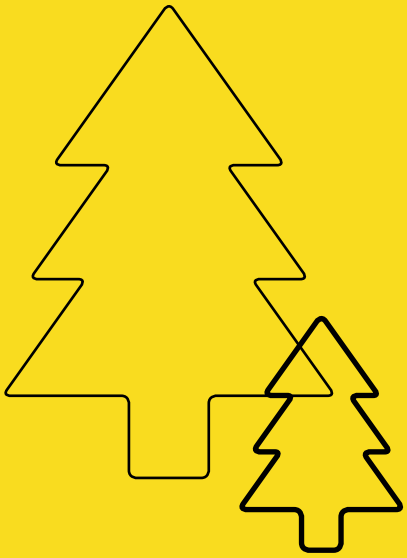
Such a situation has developed over quite a long time and it is not only typical of spatial data but all public sector data. We can speculate that in the case of certain databases, a monopolistic status is sensed and the authorities are reluctant to forgo the possibility of charging a state fee. In the case of certain databases, it is in the interests of the information holder and the state to make the data more widely usable in society – in such a case they would be free of charge and available in as simple a manner as possible.

The situation in different European countries also varies. Much depends on the extent to which information holders receive state budget funding and how much they need to earn the money themselves. A telling example is the wording, pertaining to fees, of the draft act supplementing the PSI directive. It appears there is an attempt to find a compromise between opposing interests and the result is a wording that is open to many interpretations.

Conclusion

Open data policy will be effective if it proved possible to unify access, release and terms of use and fee-charging principles for public data in re-usable form nationwide. Currently much effort is spent establishing technical infrastructure to promote greater availability of re-usable data. But this is not enough and presumably no huge changes will take place in regard to availability of data in re-usable form. Whether this is progress or stagnation depends on the viewing perspective. Spatial data have at least become more open over the last few years and this trend will continue.





CHAPTER 2
GREEN IT

We are facing a situation where natural resources keep on decreasing and become more difficult to access even as countries need more and more of them to continue their growth. Raising the economy's competitiveness will require more intelligent and resource-efficient production and use of smarter technologies. The OECD considers ICT a key enabler of sustainable economy and has indicated that while the ICT sector generates 2 per cent of the world's carbon dioxide, it can alleviate the negative impact of the remaining 98 per cent. This chapter gives an overview of the results of a survey conducted to map Estonia's green ICT potential and looks at plans for implementing the recommendations issued in this regard. The chapter also gives an overview of developments in the private sector: the ambitious Smart Vormsi initiative on that western island, and the ELVIS project – the timber industry's electronic waybill project.

Green ICT as enabler of environment and resource conservation

KRISTIINA KITSIK
kristiina.kitsik@mkm.ee
Ministry of Economic Affairs and Communications

In late 2011, the Ministry of Economic Affairs and Communications in cooperation with Ernst & Young Baltic conducted a study for mapping the level of awareness of green ICT areas and their potential in Estonia.

Green ICT is a concept that has developed in the early 21st century. It is a combination of ICT solutions and environmental conservation. In the big picture, green ICT is engaged in two main areas: environmental sustainability of ICT equipment and solutions (making ICT greener) and raising sustainability in other walks of life through ICT solutions. Earlier environmental conservation topics were considered purely green-movement topics but today, with ICT solutions developing, they are becoming increasingly intertwined with businesses' everyday activities. The reason is the fact that ICT helps bring about savings on resources in work processes. It also represents a business opportunity for companies developing new products and services.

A study entitled "The role of green ICT in enabling smart growth in Estonia"[1] reveals that Estonian enterprises realize the role of ICT solutions and, using green ICT, seek ways of making manufacturing processes more efficient and environmentally friendly. The adoption of such solutions is largely motivated by the desire to save money, although conservation as such is also considered important.

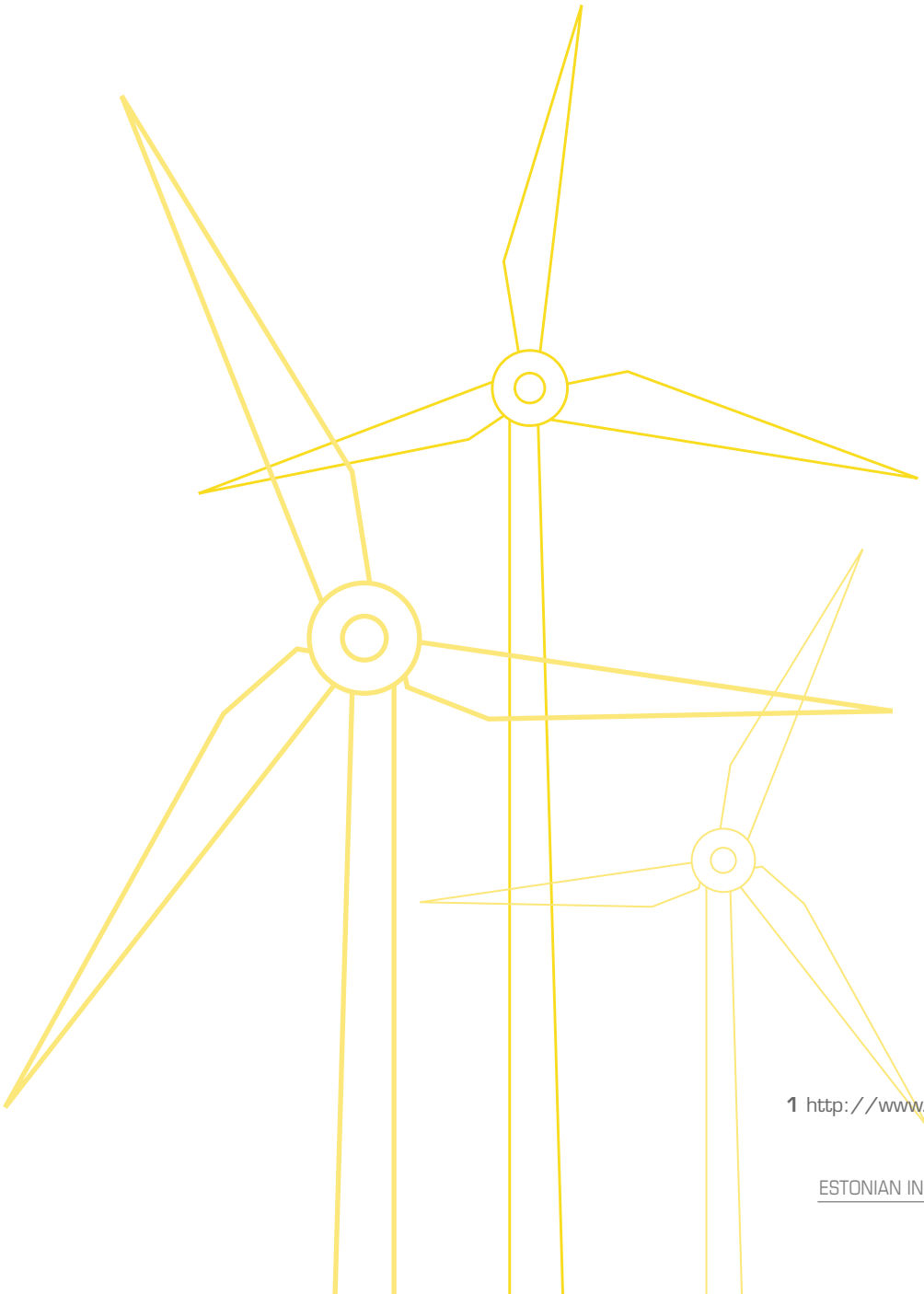
Green ICT solutions can be found in many walks of life. An example of building energy efficiency is the smart house solution devised by an Estonian company, Yoga. The company estimates that the design will allow the heating costs for the building to be reduced by as much as 30%. In the field of transport, ICT is used to optimize itineraries. Estonia's biggest telecoms companies, EMT and Elion, are piloting solutions where residual heat from server rooms is used to heat surrounding offices and homes. An active community on a western island is behind the Smart Vormsi project designed to improve the living environment for the islanders (see p 32).

In addition, resource savings are provided by the replacement of services that require paper copies and in-person office visits with online services and software solutions. Although the state sector has had an active role in this area (ID cards, X-road, e-health, e-school, electronic tax returns) there are also good examples from the private sector, such as Internet banking and mo-

bile parking, green ICT solutions that have been in use for over 10 years.

In spite of some good examples, it must be noted that in large part the use and development of green ICT solutions is still in the pilot stage in Estonia. Companies polled were asked what obstacles they saw to wider use of green ICT. As could be expected, the greatest obstacle cited was monetary restrictions (about 85% of respondents) – development of technology and innovation are costly. Often intelligent green ICT solutions require greater start-up investments and the savings tend to be realized in the maintenance costs. It was also noted that there are no reliable methods for determining the return on green ICT solutions. Thus companies often take a wait and see position with regard to green ICT. Public sector authorities are facing a similar problem; due to the Public Procurement Act they are forced to save on acquisition costs.

The study conducted by Ernst & Young and the Ministry of Economic Affairs lists policy recommendations for surmounting the obstacles hindering the development of green ICT. The study results were used as a source for the ministry's programme for supporting green ICT solutions.



1 http://www.mkm.ee/public/Inno_18_GreenICT.pdf

Using ICT solutions to support eco-innovation

KRISTIINA KITSIK
kristiina.kitsik@mkm.ee
Ministry of Economic Affairs and Communications

The previous article discussed a study commissioned by the Ministry of Economic Affairs and Communications from Ernst & Young Baltic, "The Role of Green ICT in Enabling Smart Growth in Estonia"[1], the goal of which was to determine the level of awareness of green ICT areas and their potential in Estonia. Among other things, the study made policy recommendations to the government. These are the primary ones.

There should be more focus on raising ICT awareness. Although Estonia is in the vanguard in ICT compared to other countries in the neighbourhood and can show good examples of solutions in use, it can be argued that in fact there is little awareness that much can be saved on resources by developing or outsourcing new ICT solutions: energy, time, money, materials etc.

How to raise awareness:

- Creating a publicly usable ICT solutions and products database.
- Offering (e.g. from Enterprise Estonia and the Development Fund) more business consultations, the goal of which is to identify the potential of green technologies and green IT.
- Citing examples of solutions already in use.
- Recognizing entrepreneurs at enterprise competitions with a special prize for green ICT.

Supporting cooperation with stakeholders and between companies engaged in focus areas. Cooperation would increase synergy and strengthen the companies' competitiveness.

Solutions:

- Carrying out more joint public and private sector projects.
- Integrating the green ICT topic into clusters or contributing to the inception of a green ICT cluster.
- Determining detailed opportunities for cooperation and the benefits to be realized.

Financial support for green ICT solutions. This in turn would accelerate the adoption of the solutions in companies and society.

A new programme being developed – "Green Industry Innovation[2]" – will help resolve these problems. It is being funded from the Norwegian financial mechanism 2009–2014 and is being developed in close cooperation with programme partner Innovation Norway.

Two strategies on the state level served as a basis for designing the programme: The Estonian RDI strategy 2007-2013 and the 2012-2013 implementation plan for the Information Society Strategy 2013. But it also proceeded from the need to use ICT for saving resources and for new smart solutions.

A general goal of the programme is to increase Estonia's environmental, economic and social

sustainability, developing smart IT solutions that would help save on resources. This means that Estonia should start to use all of our key resources better, above all so that they would last for hundreds of years. Smart IT solutions will contribute well toward this purpose. They will help optimize the processes and make them more efficient.

As part of the programme, it is planned to support companies, non-profits and foundations. Support will be offered precisely for developing innovation business ideas in the field of environmental conservation and for entering the international market. Above all, the criterion is a given organization's desire to develop new or existing solutions, not the organization's legal form. What we want to see is that ICT solutions are used to achieve resource savings in fields set forth in the following state strategies: transport and logistics, energy, industry and manufacturing, e-health.

In short, as a result of the programme, the number of new and innovative ICT solutions in use should increase and resource savings should grow. Cooperation between entrepreneurs should also develop, and turnover – especially export turnover – should increase.

If the volume of new (or improved) services and products built by Estonian companies on smart ICT solutions increases, this will be sure to support the sustainable development of society. Through new solutions or improved old ones, the competence and capability of Estonian companies will also increase and this in turn will lead to better competitiveness.

Good competitive advantages will result in an opportunity to make better offers on the local and international market. To be more competitive on international markets, companies must engage in more cooperation with companies both in Estonia and other developed countries. For this reason, the programme will also promote cooperation between Norway and Estonia. We find that we have much to learn and transpose from each other. We also believe that cooperation will allow us to enjoy success on third-country markets.

We will be implementing the programme in cooperation with Enterprise Estonia, which is in the area of government of the Ministry of Economic Affairs and Communications, and whose primary role is to dispense assistance and consultation to companies.

The programme has been divided into small grant scheme and open calls.

The small grant scheme is meant to prepare applications for the open call. The following activities are supported: search for project partners from Norway; executing mapping, studies, analysis and expert assessment; developing and testing ICT solution strategies by sector; initiating cooperation network or other forms of cooperation in each sector; involving consultants and experts in developing IT solutions planned in companies.

Applying for financing from the small grant scheme is not a prerequisite for submission of an application for the open call.

The open call is for major projects already being carried out. Above all, we are looking for projects that will produce resource-effective solution with commercial potential both in Estonia and abroad.

The budget for the entire programme for 2012-2015 is around 7 million euros.

1 http://www.mkm.ee/public/Inno_18_GreenICT.pdf

2 http://www.eas.ee/et/ettevotjale/innovatsioon/norra-eesti-koostoeoeprogramm-green-industry-innovation

Smart Vormsi brings renewable energy and telework to island

INDREK PETERSOO
indrek.petersoo@ericsson.com
Estonian Association of Information Technology and Telecommunications

The goal of MTÜ Nutikas Vormsi (Smart Vormsi) is to make the island of Vormsi independent energy-wise, developing a modern living environment and promoting the local economy. The leaders of the project hope to export their experience to other countries as well.

The Smart Vormsi concept has five aspects: smart Vormsi inhabitants, smart economy, smart living environment, mobility, and availability of public services on the island.

The founders of the non-profit association established in December 2011 are Vormsi municipality, Net Group OÜ and Volta AS. Partners in cooperation include the island's residents, other companies in Estonia, the Tallinn University of Technology and the Ministry of Economic Affairs and Communications. The non-profit welcomes all interested parties who want to contribute to the island's development as a unique centre for smart solutions.

Independence from undersea power cables

Board member for Smart Vormsi Mr. Priit Kongo sees the island in future as a place where renewable energy is generated and used. "Currently Vormsi gets electricity via a submarine cable. The situation satisfies the island's needs, but we are looking at the future with the long term in mind – the price of energy may fall only periodically, while the overall growth trend will soon reach a critical point. That is why we are looking for other solutions in the field of renewable energy," said Kongo.

Making the island independent energy-wise means relying on solar and wind energy. It would also allow each household to be a producer and sell surplus energy to others.

Although the cost of the equipment needed to generate wind and solar energy is largely the same, Kongo says the best choice would be a combination of the two. The wishes of the Vormsi community will determine which model is chosen.

"We are focusing more on solar panels. Our data indicates that from March to October electrical needs could be covered by solar energy if there are a sufficient number of solar panels in place. Using a smartphone app, every microproducer could keep track of how much their panel generated in a certain period, and how much their household consumed and sold to the island's grid. Such a system will require the existence of a Smart Grid," said the board member.

Kongo says the project's coordinators have too few real measurement data about the possibilities of wind and solar energy. A good resource on the team is Tarmo Kadakas, an entrepreneur from West-Estonia and renewable energy leader who has experience measuring profitability of solar and wind energy over a longer period.

This March, Smart Vormsi signed a cooperation memorandum with the Tallinn University of Technology. The use of modern technologies being developed at this institution is seen a possibility for developing the island's energy cooperative. The cooperation memorandum offers students possibilities for research and development. In addition, a representative of the university will take part in the work of the advisory board of Smart Vormsi, and it is planned to take part jointly in international projects.

Vormsi is seen by state power company Eesti Energia and the Distribution Network Imatra Electricity, as a place to test interesting renewable energy solutions. The Association of Estonian Information Technology and Telecommunications and companies from a number of other fields are also connected to the project.

Services to become more available

Smart Vormsi will help to make several vital services available for island residents and stimulate the local economy by promoting internal tourism.

"We envision the renovation of Hullo village centre on the principle of smart buildings, where everyday functions - above all ones related to electricity and heating – can be controlled by smartphone or computer. A smart building does not have to result in economic benefits, but simply bolster the overall support system," said Kongo in describing the strategy for the island's central site.

Smart Vormsi will make telemedicine available for locals, meaning that they will not need to travel in person to opposite corners of the country to consult with a specialist. Local schoolchildren will also be able to make wider use of opportunities for online learning.

"Telework positions are also planned for the island. Although not all companies are ready for this, the field of IT in particular is very flexible. If you can come to Vormsi for a family holiday in summer and also be able to manage business back home via HD quality videoconferencing tools and enjoy decent office space, that is a compelling argument for choosing a spot for a second home and it would allow vacationers to stay for longer periods. This in turn will increase demand for accommodations places, food and drink establishments and entertainment venues and locals will be able to offer tourism on a broader footing. Such an integral solution would raise the standard of living for the whole island," Kongo said.

> The Smart Vormsi concept has five aspects: smart Vormsi inhabitants, smart economy, smart living environment, mobility, and availability of public services on the island.

Vormsi municipality is seeking growth in the permanent population and it will have to prepare a housing plan for this purpose. "We will try to determine where it would be wise to develop real estate on Vormsi. A large part of the land belongs to descendants of former owners and many of these descendants do not reside in Estonia," said the board member.

In 2012, it is hoped to reach the first milestones on the way to a smart future. We will also start developing the smart building and renovation of Sviby harbour, which could also lead to additional smart services," said Kongo regarding the first steps to be taken.

In future, the leaders of Smart Vormsi hope to export their experience to other countries. Kongo says the world has few islands that are self-sustainable energy-wise – like Denmark's Bornholm and Samsö and Jeju in South Korea.

ELVIS – transition from paper to electronic consignment notes in the timber industry

MÄRT RIDALA
mart.ridala@elion.ee
Elion Ettevõtted AS

The project known as ELVIS is a good example of how a unified IT system can be implemented to organize movement of information between companies and institutions. As yet there are few such success stories but such systems are the future!

What is ELVIS?

Truck drivers carrying timber have to have a waybill that shows the owner of the timber, the transporter and consignee. The purpose of the system is to ensure traceability of timber. Up to 2011, the only option for such a waybill was a paper sheet in triplicate. The electronic version of the waybill launched at the end of last year allows the entire process to become electronic and database-driven.

The situation today

By August 2012, companies in the forestry sector had actively adopted the electronic waybill system. It is used to transport an average of 8,500 cargoes a month and over 180 companies have joined. Many larger companies such as RMK (State Forest Management Centre), StoraEnso, AS Lemeks and Horizon Pulp & Paper have practically given up paper waybills. It is planned to introduce electronic waybills for other types of forestry products, such as wood chips. A key addition in 2012 was a mobile app – now business can be transacted remotely, in the truck cab.

Advantages of the electronic waybill

The electronic information system ensures that adequate information is available. The timber owner, transport firm and recipient can track how the delivery is proceeding, getting a live update on the situation without having to call the driver. Besides the real-time information, statistical and historical data are also recorded. Transport charges can be calculated

on the basis of the data in the system, and the forest owner can be paid for the timber.

Electronic paper or development of an entire process?

When developing any information system, the first thing is to answer the question of whether the goal is simply to computerize the current process or whether it should be improved as well. Merely replacing paper with electronic records is always the simplest, but the real benefits come only when the process is improved. In the case of the e-waybill, it was decided at the outset of the project to do something more than just replace pieces of paper with computerized versions. The goal set was to increase the breadth of the overview and increase the efficiency of the operations on all sides. The decision made the project more complicated, longer and more costly but it has also translated into more post-implementation benefits for users.

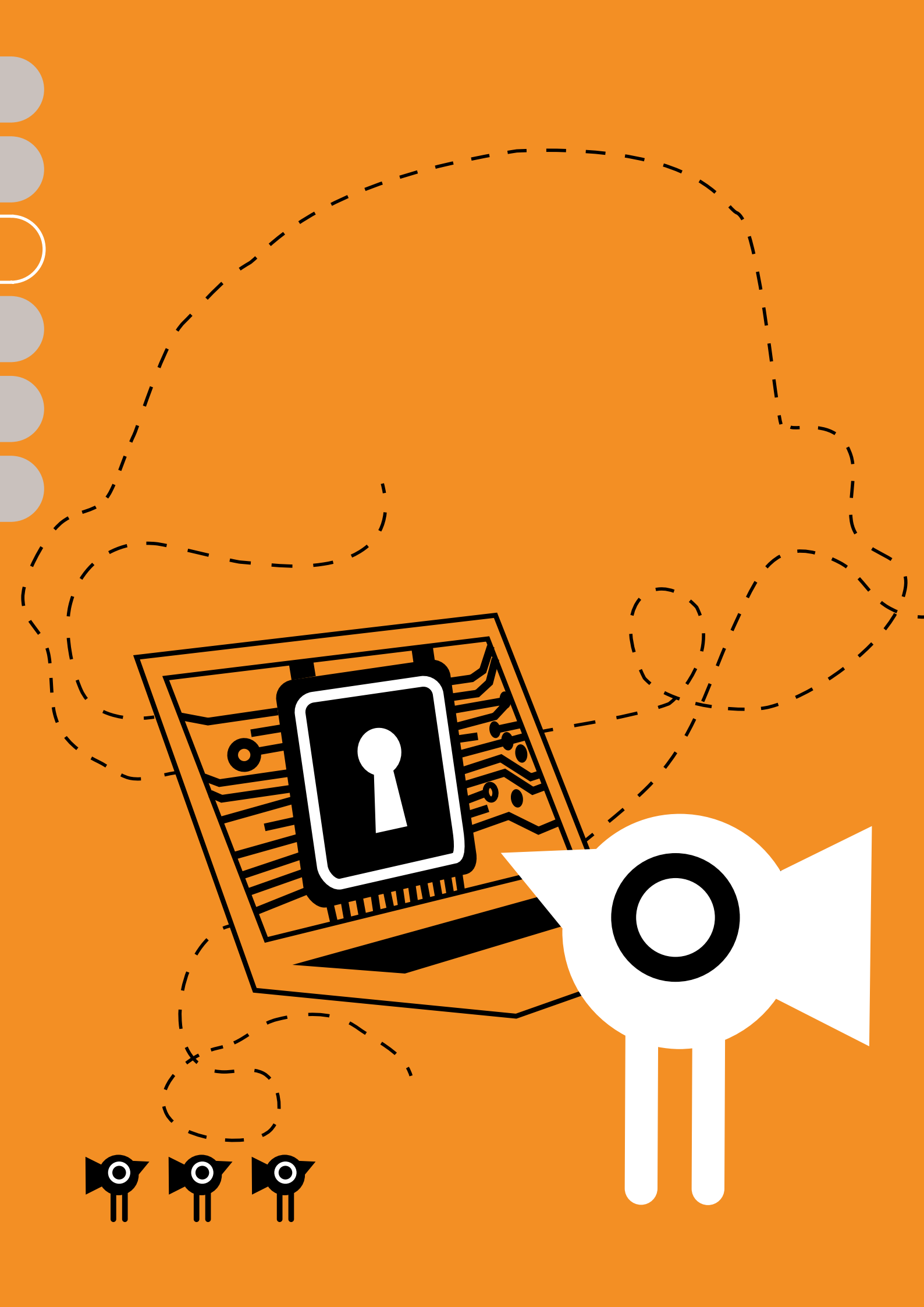
When developing any information system, the first thing is to answer the question of whether the goal is simply to computerize the current process or whether it should be improved as well. Merely replacing paper with electronic records is always the simplest, but the real benefits come only when the process is improved.

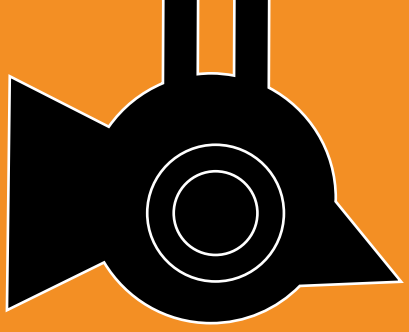
Key to success

It is many times harder to implement a system involving several companies than within a company. It means diverging interests or, often, lack of interest. Within a company, one manager is in place and that person decides whether and what to do. But if there is more than one company, consensus must be forged. Thus the role of the Forest and Wood Industries Association and of the e-waybill project group led by StoraEnso Estonia logistics director Mait Marran is especially important for this project. Only thanks to their consistent work was it possible to get every player – from transport company, forest owner, sawmill operator to police and Environmental Inspectorate – to work together.

Elion's role in the project

Elion's role in the project was different from ordinary IT hosting service. Usually the service recipient and service provider agree on the specific parameters for the system and the price of the hosting, but in this case, Elion is offering e-waybill operation service. That means that Elion's fees come from the e-waybill fees paid by the system users and that besides hosting, Elion is also in charge of developing the system, training, providing user support, integrating information systems and providing consultation to customers. That is a big touchstone for Elion but today the service has proved to be justified.





CHAPTER 3
CYBER SECURITY

In using opportunities that information technology has to offer, we consider it fairly natural to consider the risks as well as the amenities. The risks include cyber attacks against companies and government agencies, which potentially affect the lives of many, or activities that pose a risk to children online. The cyber security field is constantly changing and our increasing dependence on information systems means that domestic and international cooperation is ever more important. Neither should we forget that a secure Internet is up to each individual Internet user to help to create. This chapter gives an overview of the cyber security strategy and related activities, the new information security interoperability framework, organization changes in ensuring cyber security, and efforts to promote safer use of the Internet among children through the project “Smartly on the Web”.

Cyber security

HELENA RAUD
helena.raud@mkm.ee
Ministry of Economic Affairs and Communications

Cyber security and related elements made their first appearance in state-level rhetoric in 2007 when cyber attacks hit Estonian government and private sector websites.

In 2008, the government adopted the first cyber security strategy for the period 2008–2013. This was undoubtedly triggered by the 2007 cyber attacks; however, five years ago, the Estonian information society and dependence on technologies were already advanced to the extent that the role of the state in developing a more secure online society could not be ignored.

The cyber security strategy set forth four goals for the state:

1. Estonia makes widespread use of a graduated system of security measures for ensuring national cyber security.
2. Estonia is a country with very high information security competence and awareness.
3. The secure and widespread use of information systems is supported by proportional legal and regulatory environment.
4. Estonia is one of the leaders in international cooperation for making cyber security more effective.

2012 marked five years since those landscape-changing cyber attacks – it is now time to review the set goals, analyze what has been done and set new goals. As the preparation of the strategy for the new period is at an early phase, I will first provide a brief overview of the fields that we have dealt with in the context of cyber security.

Security of information systems – the government regulation "System of security measures for information systems" was adopted already on 20 December 2007, and it laid the groundwork for implementation of security measures in government bodies. To ensure even better coordination and incident reporting, the government, in 2012 established a regulation on the "Information security management system", which required government bodies to appoint information security managers. Pursuant to the regulation, the information security managers engage in cooperation with persons responsible for processing of personal data, verifying compliance with the information security guidelines, evaluating the strength of information security at institutions. They also participate in the work of the institution's development or IT council and in information system development projects, provide consultation in information security risk assessment, develop new security measures or improve existing ones, implement procedure for administering security incidents at the institution and notify CERT-EE of relevant security incidents.

The process of organizing the legal framework on cyber threats has been dealt with actively since the beginning of the strategy period. Changes to the Penal Code and the Emergency Act fall into this period, as do an amendment, adopted in 2012, to the Defence League Act, which constitutes the basis for the activity of the Defence League's cyber defence unit.

Exercises – the role of exercises in testing cyber security regulations is noteworthy as non-functional legislative or deficient decision-making mechanisms would have a significant effect on resolution of crises stemming from cyber threats in all vital service sectors.

In January 2012, a unique cyber exercise took place in Estonia, called "Cyber Fever 2012", during which the Cyber Defence Unit of the

Defence League developed the scenario and organized a Cabinet level training day for top civil servants and ministers. Institutions and organizations have organized cyber exercises from time to time, but Cyber Fever was the first for the government and its crisis management committee.

International functions – in the online, borderless world, it is important to develop uniform principles and views on cyber risks and minimize risks effectively. Estonia has been active in both bilateral and multilateral cooperation. Undoubtedly Estonia's biggest contribution has been made in international organizations, such as the EU, NATO and the OECD.

In 2011, representatives from the Ministry of Economic Affairs and Communications and the Estonian Information System´s Authority participated actively in the planning and executing of the first EU-US cyber exercise "Cyber Atlantic 2011", organized by ENISA. Besides mapping technical solutions, the goal was to introduce cyber experts from all EU member state and US and EU institutions at the technical and policy planner levels.

Similarly, in 2012 Estonia is closely involved to the planning of the EU exercise "Cyber Europe 2012", which is taking place in Athens in late autumn.

As a small country that has taken on the obligation of maintaining a high level in ensuring cyber security, we are happy that the opening remarks from the representatives from the exercise coordinator, the director of ENISA, and the representative of Ministry of Economic Affairs and Communications of Estonia, will be broadcast from Tallinn.

In addition to the exercises, 2012 is a landmark year for the EU due to the initiation of the preparation of the pan-European cyber strategy.

From organizational changes to a new strategy – 2011 saw the largest organizational change in organizing cyber security. Namely, the Ministry of Defence handed over control of the cyber strategy and Cyber Security Council coordination to the Ministry of Economic Affairs and Communications. Insofar, as it is the Ministry of Defence that coordinates transnational cyber security in many of our partner countries, one could ask why the change was made.

We can answer from the practical and communication-related aspect: it was due to the fact that cyber threats and communication infrastructure used by many ordinary citizens, as well as the state, are predominantly in the hands of private companies. Regulation of the continuous operation of communication services is in the area of administration of the Ministry of Economic Affairs and Communications. Just as important is the role of the Ministry of Economic Affairs and Communications in organizing continuous operation of other vital services (such as in the energy sector) or the fact that the Information System's Authority, reorganized in 2011, and CERT (part of the former) are under the jurisdiction of the Ministry of Economic Affairs and Communications.

Estonia has been active in both bilateral and multilateral cooperation. Undoubtedly Estonia's biggest contribution has been made in international organizations, such as the EU, NATO and the OECD.

With regard to future plans, we can say that the most important task is the drafting of the second cyber security strategy that will be initiated in 2012 and prepared in 2013 and related further review of the legal framework pertaining to cyber security.

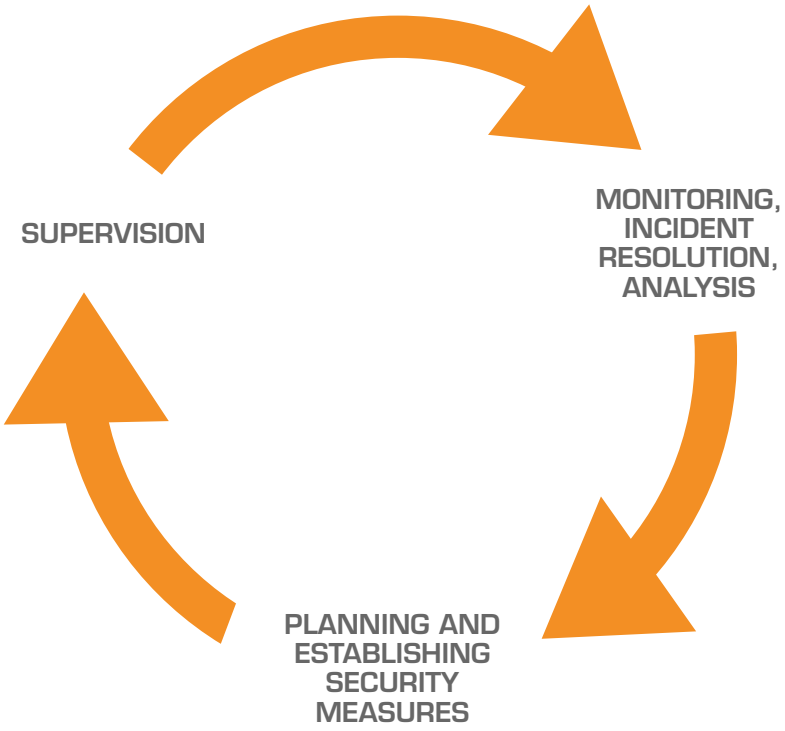
For the first time, the Ministry of Economic Affairs and Communications will begin to be responsible for the coordination of preparation of the strategy, but our partners from other ministries, government bodies, private sector and academic circles will also have an extremely important role. It is premature to talk about new strategic goals, but we hope, and work toward, making Estonia's second cyber security strategy even more broad-based, and take into account possible cyber threats in conformity to development of our information society and without imposing too many restrictions.

Role of the Estonian Information System's Authority in ensuring Estonia's cyber security

TOOMAS VAKS
toomas.vaks@ria.ee
Estonian Information System´s Authority

Starting from the early 2000s, the development of the Estonian state has been closely connected to the development of information technology. As a country with a low population, one of the lowest population densities in Europe, contribution to the development of information technology and communications sector has been a logical and inevitable step. Without modern information technology, many of the public and private sector services that we have grown accustomed to would be impossible or very expensive due to lack of the necessary human resources. We could cite the example of such information-intensive services as state and private registers, information databases, media, banking and so on. In Estonia's case it is very important that services be available outside larger cities and towns. This would allow a multitude of essential transactions and operations to be conduced in low-density areas. In the last few years, dependence on information systems has grown in fields that are not directly related to information processing. Manufacturing equipment control systems (ICS and SCADA) are increasingly integrated with Internet systems, and equipment that is controlled online has made inroads into our everyday lives. Heating equipment and backup generators equipped with remote control and monitoring systems and alarm and security equipment are just some examples.

The topic of risks has inevitably appeared on the agenda. The discussions became especially salient after cyber crime picked up in the early part of the first decade of this century, and naturally the 2007 cyber attacks turned a whole new page in this discourse. Society's dependence on government and public information systems and the associated risks also led to the need to use a more integral and effective approach to controlling such risks, and thus a new authority – the Estonian Information System´s Authority (Estonian abbreviation RIA) was established in the jurisdiction of the Ministry of Economic Affairs and Communications, one of the primary tasks of which is ensuring cyber security in Estonia. The functions of the RIA in this field are to perform supervision over the information system used to provide vital service and permanent implementation of security measures for related



The primary means used by the state to ensure cyber security.

information assets; organizing activities related to the state information system and security of Estonia's critical information infrastructure; dealing with security incidents in Estonia's computer networks and naturally also taking part in developing policies, strategies and development plans related to its area of activity.

Three Information System´s Authority departments handle cyber security: the critical information infrastructure department (KIIK), the information security incident handling department (Computer Emergency Response Team for Estonia, CERT-EE) and the supervision department (JVO) – their activities are coordinated by the deputy director general for cyber security. The primary areas of activity:

- organizing critical information infrastructure protection, including preparing risk analyses and developing security measures needed for protection of critical information infrastructure;
- coordinating implementation of information security standards (including the three-level baseline security system for information systems, ISKE) in state and local government institutions and persons under private law that execute public functions as well as developing information security recommendations for this purpose;
- handling security incidents in Estonian computer networks and reported to the network, forwarding warnings for preventing security incidents and raising users' security awareness, including preparing reports on incidents in Estonian computer networks and the spread of malware;
- developing strategies and policies related to cyber security;
- supervising permanent application of security measures for information systems used to provide vital services and information assets related thereto;
- cooperation with other government bodies, local government units, foundations, non-profit associations, entrepreneurial and consumer organization and other relevant institutions and international organizations, as well as providing consultation to government bodies in resolving problems in the field;
- representing the state in international relations in accordance with procedure set forth in legal acts.

RIA did not have to start from scratch in its cyber security operations. The information security incident handling department (CERT-EE), which has been in operation since 2006, and the critical information infrastructure department estab- »»

» lished as part of the Estonian Informatics Centre a few years later had created a very good footing for this. The specialists from these units are professionals internationally recognized in their field, and their knowledge and initiative have allowed satisfactory capability to be retained in the cyber security field also in conditions of the recession. Estonia has succeeded in founding very good cooperation between private and public sector, establishing a security committee that would be quite unusual for other countries. This community exchanges daily operational information on incidents and security risks in the cyber security field.

Increasing the security awareness of government agencies, government and corporate vital service providers and that of the public has been one of the main national priorities in the cyber security field. In 2011, 32 cyber security training events were held in the "Smart e-state" training series taking place in the framework of the EU programme "Raising Public Awareness about the Information Society". A total of 966 people took part in the trainings. International cooperation must be considered very good as well; thanks to great exchange of information, this has pre-empted and prevented security incidents and made protection measures more effective.

In 2011, the three-level baseline security system (ISKE) was updated and a number of risk analyses in fields of importance for the state were completed.

After RIA was established, a search for additional cyber security specialists was mounted in order to staff the supervision department and find additional forces for CERT and KIIK. It is a pleasure to be able to say that in spite of the high demand for cyber security specialists on the Estonian and international workforce market, a number of internationally recognized specialists have been hired by government authority and joined the RIA team.

The everyday work of 19 RIA staff and officials is connected namely to ensuring cyber security.

The keywords for 2011 in the cyber security field were the following:

- The "E-factor" – ensuring cyber security is indispensable in Estonia, as many state and private sector services depend completely on IT.
- International cooperation in the field of cyber security is very intensive and the development and establishing of international regulations has begun as well.
- A proposed amendment to the Emergency Act – termed the "servers bill" – initiated discussion in society regarding the information technology interdependence of vital services.
- Mobile devices and social media have changed people's behaviour and security risks.
- The risks of ICS/SCADA systems have brought security risks from information security into everyday life.
- Implementing supervision of implementation of security measures for vital services' information systems.

In 2012, we see our biggest tasks being monitoring and analysis of cyber security risks, notification of such risks in an adequate and timely manner and implementation of countermeasures. Even more attention must be devoted to retaining and developing capability for the resolution and prevention of incidents and effective international cooperation.

To sum up, it is not possible to exclude risks related to information systems, but it is possible to keep them under control and reduce losses. To control risks, they must be understood and the risk level, impact and probability must be assessed accurately. The greatest threat in the cyber security field continues to be lack of aptitude, negligence or carelessness on the part of technology users and their inability to apprehend technological progress and related risks.

Estonia: Building a safer global cyberspace

LUUKAS KRISTJAN ILVES
luukas.ilves@ria.ee
Estonian Information System´s Authority

The global situation

The need for international cooperation in cyberspace is evident. Cyberspace is global and no country is a cyber-island, but cyber security today is in the same phase of development as maritime security in the 18th century: bad guys operate across borders with impunity, non-state and state-sponsored actors are hard to tell apart, attackers are at a technological advantage over defenders, and the economics of asymmetric cost and benefit favor a growth in insecurity.

2011 marked the year in which cyber threats and vulnerabilities could no longer be ignored on the world stage. The slow and steady leaking of documents by Wikileaks, crackdowns by governments, and retaliations by 'hacktivists' like Anonymous for trying to silence Wikileaks; the Arab Spring, which showed the potency of social media as an organizing tool to bring down governments; the constant litany passwords and credit card data theft; the apprehension of high profile cybercrime groups like Rove Digital in Estonia; major data breaches at the EU, IMF, UN and many defense ministries and companies; the follow-up to Stuxnet, the even more potent Duqu virus.

On a national level, most governments have woken up to the threat. Many nations released national cyber-security strategies, including Germany, the UK and US. NATO adopted a new Cyber Defense policy in June of 2011. The EU and US are coordinating policy in a number of working groups. The OSCE is working to develop Cyber-CBMs and CSBMs (Confidence (and Security)) Building Measures. 2011 year was capped by a major international conference in London whose goal was to develop joint norms in cyberspace, whose follow-up is occurring this year in Budapest. The UN is beginning a further round of discussions to reach a global consensus on norms of behavior in cyberspace. Estonia is among 15 countries contributing to the group of governmental experts. In all of these forums, Estonia has been a highly active participant, usually among a small group of countries shaping the policy consensus.

The tenor of the conversation is changing, however, as talks in international organizations and with partners become more technical, and as multilateral and bilateral cyber-cooperation grows in depth and scope. Thus far, Estonia has been able to maintain policy and leadership in this area; continuing to do so will challenge a small country with an even smaller public sector.

Estonia: strategic goals

The basic tenets of Estonia's international cyber security engagement have not changed from the positions articulated in the 2008 National Cyber-security Strategy: »

- Adopt a broad stakeholder approach that includes governments, the private sector, civil society, international organizations, experts. The Internet cannot be regulated by the neat rules of the Westphalian system.
- Develop and disseminate legal and behavioral norms for state behavior in cyberspace, including norms derived from the law of armed conflict.
- Treat the fight against cybercrime as a linchpin in minimizing interstate cyber-conflict. Cybercrime is a fearsome phenomenon unto itself, but also enables state sponsored espionage and attacks to linger in a gray area without clear attribution or censure by the international community.
- Maintain the liberal and inclusive practice that has so far characterized Internet governance, ensuring that the web remains a tool for freedom and is not over-securitized.

In practice, Estonia has emphasized openness, transparency, information sharing, and a cooperative approach in all its activities and relationships. As a small country, Estonia can only realize its own cyber security in a broader framework.

In the area of cyber security, Estonia does not suffer from a lack of global visibility. Estonia has been a global cyber security leader since the 2007 attacks, with a consistent international policy and technical agenda.

Coordinating Estonia's international activity is a challenge. Even small Estonia has a long list of actors with cyber security responsibilities and an international presence. On a policy level, the Ministry of Economic Affairs and Communications has the lead, but other actors include the Prime Minister's and President's offices, Ministries of Defence, Internal Affairs, Foreign Affairs and Justice. On an operational level, the Estonian Information System's Authority, Defence Forces, and various branches of the Police.

Technical cooperation

International conferences and NATO and EU strategies alone will not keep Estonia safe from foreign cyber attack. International cooperation in cyberspace must develop more effective operational capabilities. A country of Estonia's size particularly needs to rely on EU and NATO capabilities, as well as those developed jointly with other countries. While Estonia and like-minded countries have excellent informal cooperation, the challenge has been to formalize this while maintaining and growing deep trust.

A good example of focusing on technical cooperation with clear deliverables is Abusehelper, a joint project that includes the Estonian, Finnish and Belgian CERT-s that automatically processes incident notifications and helps countries cut down on the rate of malware infection and botnets in their domain.

NB-8 and bilateral cooperation

Greater regional integration is not an option, but a requirement. Estonia's regular cyber security contact is closest with its neighbors Latvia and Lithuania (the Baltic 3) and Finland, Sweden, Denmark, Norway and Iceland (the Nordic 5). These countries are highly interdependent in cyberspace, with banking, telecom and energy sectors that are increasingly integrated, including in a physical sense (through power lines and fiber optic cables). A large-scale cyber attack against critical services in one country will leave citizens and businesses suffering in all.

The NB-8 (the N-5 and B-3) have a similar set of cyber threat assessments and domestic arrangements, a focus on protecting critical infrastructure, and resource constraints. All have relatively low rates of malware infection and criminal activity in their domestic cyberspace. There is already frequent N-5 and B-3 technical cooperation, and Estonia's ultimate goal is to achieve a uniformly high degree of cyber security that would allow a merger N-5 and B-3 activities in this area.

Estonia works closely with many other bilateral partners. Estonia's public sector IT security guidelines are based on Germany's federal IT Baseline Protection Manual. Estonian and US authorities work closely on combatting cybercrime, most recently in the high-profile takedown of the spam and adware company Rove

Digital in November 2011, the largest cyber security-related arrest and prosecution anywhere to date. Various Estonian government agencies, including the Information System's Authority, also work on capacity building and training with foreign partners, particularly in South-East Europe and, increasingly, the Middle East and North Africa.

International institutions

In addition to its national expertise, Estonia also draws upon and supports the international institutions present in Tallinn. The NATO Cooperative Cyber Defence Center of Excellence (CCD CoE) has a large Estonian staff and works with the Estonian Defence Forces and Cyber Defence League on joint programs and exercises. The EU Schengen IT Agency opening in Tallinn in 2012 will further grow the international expertise resident in Tallinn.

Exercises

Estonia is a highly active participant in multinational Cybersecurity exercises. Estonia has taken a strong role in designing EU and NATO exercises like Cyber Europe and Cyber Coalition, and along with the CCD CoE host regional exercises like Baltic Cyber Shield and Locked Shields, and invites foreign observers to its various domestic technical and tabletop exercises. Recent exercises include the Cyber Fever 2012, a two-day cabinet level table top exercise conducted by the Estonian Defence League's Cyber Unit.

Gray clouds on the horizon

There are also, however, gray clouds on the horizon. One worrying international trend is the increasing securitization of cyber security. The international network of CERT-s that grew out of the academic world in the 1990s was flexible, decentralized and very open, without formal information sharing arrangements. But, as cyber security has become a more prominent national issue, states are treating cyber security as a military and intelligence matter, and focusing their capability development in organizations and legal structure that complicate international cooperation instead of encouraging it. NATO and the EU have not achieved the same level of cooperation and joint operational capability that they have in areas of defence, law enforcement or counter-terrorism cooperation. Many Allies or Member States are simply reluctant to entrust so core a concern to international organizations.

A further difficulty arises from the relative novelty of cyber security, which has resulted in a different division of labor in every country between ministries of defence, internal affairs, and economy, and between CERTs, law enforcement, intelligence agencies, and the military. All of this makes implementing international cooperation at times confusing and difficult.

In the area of cyber security, Estonia does not suffer from a lack of global visibility. Estonia has been a global cyber security leader since the 2007 attacks, with a consistent international policy and technical agenda. As cyber security gains more attention internationally, however, we now face the difficulty of implementing this agenda in circumstances of increasing competition. The expectations and pressure on the Estonian government, policymakers, agencies, technical experts will not remit.

Information security interoperability framework, version 2

JAAK TEPANDI
jaak@tepandi.ee
Tallinn University of Technology

The boundaries between the real and the virtual have become blurred. Our well-being, property and lives are determined to an increasing extent not just by the laws of the physical world but by those of cyberspace. The latter are only now taking shape. The information security interoperability framework is one of the regulatory measures that attempts to shape a secure cyber environment.

The boundaries between the real and the virtual have become blurred. Our well-being, property and lives are determined to an increasing extent not just by the laws of the physical world but by those of cyberspace.

Starting in 2007, four official versions of the framework have been published. The most recent of them is version 2 (www.riso.ee/et/koosvoime/infoturbe-raamistik-2011.odt (in Estonian)), which takes into account the changes that have taken place in the interim in Estonia, the European Union and the entire world, recognizing, above all, the importance of protecting critical information infrastructure and security risks related to adoption of new technologies (e.g. mobile communications devices and smart devices).

As with the physical world, a number of regulations must be implemented to keep the cyber environment secure. Thus the information security interoperability framework and the Cyber Security Strategy 2008–2013 are in harmony with and linked to each other, even though they each have a different target group, orientation and content. The term cyber security covers all operations involving electronic information, media and services that affect national security. Cyber security strategy is aimed above all (but not only) at national defence and institutions related to critical information infrastructure. This is based above all on reducing the vulnerability of the cyberspace of the state as a whole and covers a number of fields related to state secrets.

The information security interoperability framework sets out the general principles for the func-

tioning of information security in Estonia. It is intended for establishing a unified set of standards for the public and private sector with regard to ensuring domestic information security, including developing and administering the IT solutions used to provide public services. The framework does not deal with matters related to state secrets.

Version 2 of the information security interoperability framework deals more thoroughly than its predecessors with protection of critical information infrastructure. In doing so, it proceeds from the position of the e-society and public sector – specifically, from what companies and institutions should consider in connection with protection of critical information infrastructure and what the cyber security aspects of information system interoperability are.

Critical infrastructures consist of physical and information technology systems, networks, services and resources that, if disrupted or destroyed, would have a major impact on public health, safety, security, quality of life or functioning of government. Critical infrastructures span many economic sectors, including banking and finance, transport and marketing, energy, public utilities, health care, food supply and communications and key government services.

The regulation of the Minister of the Interior "Guidelines for preparing a continuous operation risk analysis" defines vital services. These are services that are essential for organizing vitally important public operations, health care, safety, security and people's economic and social well-being. The Emergency Act states that "providers of vital services are obliged to ensure the permanent application of security measures for information systems used to provide vital services and information assets related thereto".

In the course of implementing the information security interoperability framework, a need for additional security requirements for state and local government databases could become evident from an analysis of vital services.

In taking into consideration the needs of other data users, particular attention should be paid to possible links with critical infrastructure (e.g. its assets, service or systems). If there are such links, they should be taken into consideration in choosing security classes, levels and measures for the systems.

Critical infrastructure services often occur in chains of dependence. For instance, an entire range of component systems and services are needed for functioning of vital services. If an institution or company is one component in such a chain, this must certainly be considered. Additional security requirements should also be weighed if an organization's systems could impact the functioning of the Internet infrastructure or they are related to SCADA control systems.

Additional security requirements should be taken into account in subcontracting agreements, including for service providers' server rooms and other infrastructure.

Cooperation for promoting safer Internet use among children

KERLI KUUSK
kerli@lastekaitseliit.ee
Estonian Union for Child Welfare

Children and adolescents are active users of new media technologies and partake of the new opportunities offered by Internet social environments, online games, mobile communications etc. But it is important they know how to use these technologies without posing a risk to themselves or others and where to get help and advice if needed. **For the purpose of promoting safer use of the Internet in Estonia, the Estonian Union for Child Welfare coordinated a project in September 2010 called "Targalt internetis" (referred to here as Smartly on the Web)**, implemented by the Police and Border Guard Board, Tiger Leap Foundation, the Ministry of Social Affairs and Estonian Advice Centre. The goal of the project is smarter use of the Internet among children and parents and preventing the spread of illegal content. The project has three activity areas: training and awareness raising, combating the spread of illegal content in the framework of a Web-based hotline www.vihjeliin.ee, and providing counselling through the children's helpline 116111. Here is an overview of the project in the framework of project activity from January 2011 to May 2012, materials prepared for promoting safer Internet use among children and information where to find them.

Training and awareness raising

The training and awareness raising work is coordinated by Tiger Leap Foundation, which organized a number of training and information events for children, parents and teachers. In early 2011, extensive training activities were launched in schools and kindergartens across Estonia. Fifteen trainers, who hold lectures and workshops in Estonian and Russian, passed on instruction about online safety to 9,194 pupils, 1,176 parents and 1,157 teachers, visiting 150 schools and kindergartens. Information on the training and contacts of trainers are available at www.targaltinternetis.ee. Through the workshops, teachers receive encouragement and information as to how to discuss these topics with students in lessons. Besides the information events in schools, four online courses on Internet safety were aimed at teachers, dealing with issues related to computer security, social networks and Internet safety. A total of 80 teachers participated.

As Estonian children are among the youngest in Europe in starting Internet use, it is important to work with kindergartens as well. The Tiger Leap Foundation, in cooperation with Audentes private

school, organized study events for older classes in kindergartens, where children received basic instruction on the Internet and computer interaction. Together with teachers children filled in thematic worksheets and watched educational cartoons.

An International Safer Internet Day is celebrated every year on the second Tuesday of February. In 2011, the theme was "It's more than a game, it's your life." In Estonia on this day, the Tiger Leap Foundation held a conference for teachers. The main topic of the event was Estonian children's online behaviour. Teachers and parents were introduced to possibilities how they could change children's risk behaviours and promote positive online content. At the conference, young Internet users talked about their experience in using the Internet and what support they expected from adults. In addition, a two-week campaign on popular websites was held for young Internet users. During the campaign they could test their knowledge of Internet safety. More than 7,500 children took part in an online quiz.

In 2012, the theme of Safer Internet Day was "Discover the digital world together – safely", which encouraged participants to think about how adults and children can support each other in the virtual world to keep anyone's privacy, reputation or health from being threatened and to keep online activities a positive experience. A year earlier, a conference for teachers and social workers was held but this time the decision was to focus on families. The Safer Internet family day took place in Lindakivi cultural centre in the Lasnamäe district of Tallinn – this community centre being a popular place especially among Russian-speaking segment of the population. Visitors could take part in a number of workshops and listen to lectures in both Estonian and Russian; children found things to do trying out educational games developed by the awareness centre of the project and competing on Xbox 360 games. Interactive workshops hosted by partners the look@world foundation, Limpa.ru and EMT were aimed at adolescents. A counselling café welcomed visitors; quizzes and a prize drawing were held. In the cinema, the youngest participants experienced the fun of Rabbit Juss's adventures in the Internet world or followed the Sheeplive cartoons. Information points for Smartly on the Web, the hotline and helpline were open. Web policeman Andero Sepp shared his experiences and good advice.

To publicize Safer Internet Day in 2011, a special supplement to Märka Last (Notice the Child) magazine was published in cooperation between Õpetajate Leht (Teachers' Weekly) and the Estonian Union for Child Welfare. In 2012, a supplement was published inside the pages of Postimees. The supplements can be found on the project website.

In cooperation with Estonian Public Broadcasting, Tiger Leap Foundation organized a thematic program on 2 October 2011 televised on ETV2, entitled "The New Reality", where three documentaries were shown: Growing Up Online (USA 2008), Digital Nation (USA 2011) and Life 2.0 (USA 2011). The studio experts who commented on the film included the project advisory board members and trainers as well as a member of a youth panel. In October, as part of the Smartly on the Web project, a youth day was held at Solaris Centre, offering entertainment and information on Internet safety. Youth day saw a total of around 400 teens and adults participate, taking tests and solving crosswords, listening to lectures and playing Kinect games.

The website www.targaltinternetis.ee provides links to all of the educational and information materials prepared during the project: training material for teachers, lesson plans for various age levels (e.g. passwords, privacy, fake user accounts, computer overuse, cyberbullying etc, posters „Netinipid" (Net tips) and „Seisa enda eest" (Stand up for yourself), tests, crosswords, cartoons, information materials for parents etc). The Sheeplive cartoons proved especially popular, which deal with risks and threats that children can encounter online and provide advice on how to avoid them. »

As the Internet transcends national boundaries, content uploaded elsewhere is also available in Estonia. Thus international cooperation between hotlines in different countries is important to stop the spread of illegal content.

» Children who are just starting to use the Internet have three Rabbit Juss cartoons to watch, where the Internet and safe behaviours such as creating a secure password are explained to them.

The website also has a new online game, Nastix (www.targaltinternetis.ee/nastix), which is primarily to help children age 9-14 learn the principles of safe Internet use. Together with the game's character Nastix, players learn how to introduce themselves to others online, what information to give and not to give; what privacy is and how to understand it in the context of the Internet; students also learn to create and recognize a secure password; it also teaches them what to think about when setting up a new user account. In the game, Nastix's computer has fallen prey to viruses and the object of the game is to disinfect it, and a mobile user in trouble also receives assistance. Separate mini-games were also developed on the topics of as cyberbullying and social networks.

In the case of communications related to Internet use, people above all ask for advice on what to do when their child has been exposed to websites with harmful content (violence, pornography, suicide); what to do in the event of cyberbullying or if a stranger tries to interact with the child online.

Hotline www.vihjeliin.ee

In January 2011, the Estonian Union for Child Welfare in cooperation with the Police and Border Guard Board set up the web-based hotline www.vihjeliin.ee, which aims to stop the online spread of content that violates the rights, dignity and physical inviolability of children. Internet users who notice illegal content (sexual exploitation and abuse of children, child trafficking, human trafficking etc) can report it through the website. Also other materials unsuitable for juveniles can be reported to the site. The information can be forwarded to the website www.vihjeliin.ee anonymously using a simple form.

The analysts of the hotline evaluate the content of the received reports on the bases of Estonian legislation and if it proves illegal, the information is sent to the Police and Border Guard Board. It is prohibited by Estonian law to create, possess and distribute a material (image, video etc) depicting a person under the age of 18 in a pornographic situation or a child under the age of 14 in a pornographic or erotic situation. If the host of the webpage is located outside of Estonia, the information will be sent to the according country's hotline (if there is one) and/or law enforcement agency.

Since the hotline was established up to May 2012, 1,353 reports have been received at the hotline, of which 190 contained a reference to content consistent with the sexual exploitation of children. The majority of websites with illegal content reported has been of foreign origin, but some cases have pertained to websites uploaded in Estonia. As the Internet transcends national boundaries, content uploaded elsewhere is also available in Estonia. Thus international cooperation between hotlines in different countries is important to stop the spread of such content. Starting in November 2011, Estonia is a member of the INHOPE network of hotlines, which has members in 40 countries.

Children's helpline 116111

The nationwide, free 24h children's helpline 116111 went into operation on 1 January 2009. The goal is to give the public a way to report children in need, ensure that information reaches the right specialists, and to offer people related to and working with children primary social counselling and, if needed, crisis counselling. The legal basis for provision of this service is the first clause of Section 59 of the Child Protection Act, which obliged every citizen to immediately report to the authorities about children who need assistance and are in distress.

Starting in March 2011, counselling and aid are offered in Internet safety matters as well, such as: how to recognize computer addiction, how to limit children's use of computers, identity theft and Internet social network accounts, recommendations on what to do in the case of cyberbullying etc. There are the following opportunities for get-

ting advice: call the free helpline 116111, online calls made through Skype (Skype username: lasteabi_116111; users will not be added to contacts, no need to be on the list of contacts to call), online chat on the website www.lasteabi.ee, online conversation on MSN Messenger (username info@lasteabi.ee), personal message via www.lasteabi.ee; e-mail directly to info@lasteabi.ee.

In the case of communications related to Internet use, people above all ask for advice on what to do when their child has been exposed to websites with harmful content (violence, pornography, suicide); what to do in the event of cyberbullying or if a stranger tries to interact with the child online. Privacy-related problems are also salient (identity theft, disclosure of personal information, misuse of personal information).

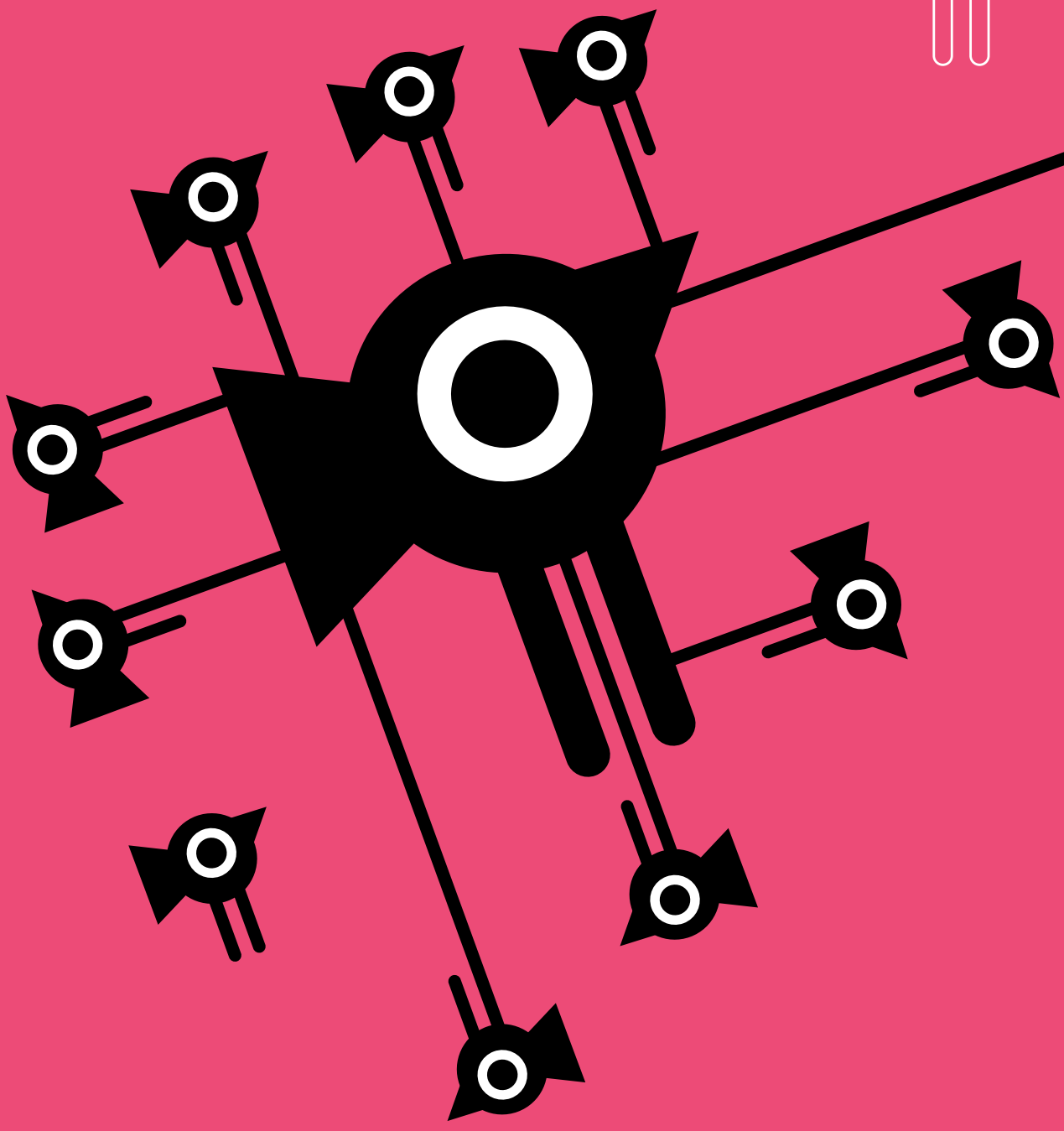
Domestic and international cooperation

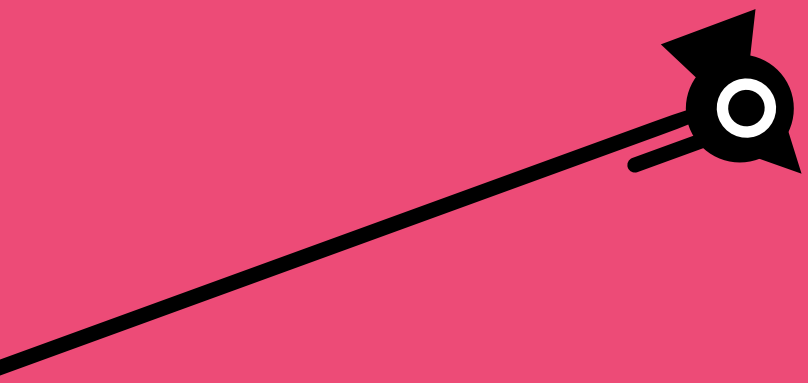
The project includes a youth panel, the members of which provide advice to the project team above all in planning and carrying out activities for the young. The youth panel members include 15 people ages 14-18, representing Tallinn's Pelgulinn Gymnasium, Tallinn's Lilleküla Gymnasium, Tallinn's Ühisgümnaasium, Ehte Gymnasium for the Humanities, Kohtla-Järve Gymnasium, Valga Gymnasium, Pärnu Sütevaka Gymnasium for the Humanities, Kuressaare Gymnasium and Põlva Ühisgümnaasium. Youth panellists inform event organisers and content developers about opinions of children and adolescents what sort of information they need for more successful, safer use of the Internet and in what way the information could best reach them. Through trainings held in the framework of the project, the youth panellists have received knowledge and skills in how to convey safer Internet use to youths – they have also been successful in applying them, organizing events on safer Internet use for the younger grades at their school. The youth panellists have represented Estonia successfully at a number of international events.

The advisory board of the project Smartly on the Web also contributes to the implementation of project activities. The members of the advisory board are the representatives from the Ministry of Education and Research, the Ministry of Justice, the University of Tartu, Microsoft Estonia, the Estonian Information System´s Authority, EMT, Rate.ee, the Estonian Parents Association, Tallinn Association of Information Science Teachers, the Association of School Psychologists, the Estonian Association of Information Technology and Telecommunications, the projects' youth panel and the project's partner organizations. In addition to the domestic cooperation, there is also participation in international networks such as INSAFE, which unites European safer Internet centres (www.saferinternet.org), and INHOPE, which is an international association of Internet hotlines (www.inhope.org).

The implementation of the project is supported to a 75% share by the European Commission programme "Safer Internet", which now has been joined by 27 European member states and Norway, Iceland and Russia.

The next phase of "Smartly on the Web " began in June 2012 and runs until October 2014. It is planned to continue extensive training, create new and interesting educational materials, publish an e-textbook for safer use of the Internet, organize a number of thematic competitive games and interactive events: conferences for pupils, campaigns and much more. It is planned to engage in more cooperation with social workers, youth centres, the Tartu Child Support Centre, the Data Protection Inspectorate and other organizations that promote safer Internet use among children. The hotline and helpline will continue to operate. For more information on the project, visit www.targaltinternetis.ee.





CHAPTER 4
HIGH-SPEED INTERNET

The Internet has become one of the most important preconditions for the functioning of today's society: Internet access is crucial for ensuring economic growth and developing a society that increases people's well-being. According to data from the McKinsey consulting firm, a 10 per cent growth in use of broadband connections in households will increase gross domestic product (GDP) by 0.1–1.3 per cent. Thus, the development of broadband is a top priority both for Europe and the rest of the world. For example, Europe's information society strategy "Digital Agenda for Europe" sets a goal for all Europeans to have an Internet connection of at least 30 Mbit/s by 2020 and for half of households to have access to an at least 100 Mbit/s connection. This chapter discusses what is being done to improve Internet coverage and access to high-speed Internet in Estonia.

Estonia's experience in developing broadband connections

OLAV HARJO
olav.harjo@elasa.ee
Estonian Broadband Development Foundation

The flagship project of the Europe 2020 project, "Digital Agenda for Europe", sets the goal of covering all of Europe with high-speed Internet. All homes, companies and institutions in the EU must have the possibility of connecting to at least a 30Mbit/s Internet connection and at least half must have access to 100Mbit/s and faster connections.

Estonia, too, has set the goal of ensuring that everyone has the chance to connect to the new-generation broadband network. This goal and action plan were developed by the Ministry of Economic Affairs and Communications (MEAC) and the Estonian Association of Information Technology and Telecommunications in 2009 and it is enshrined in the document titled "Development vision for Estonia's new generation broadband network".

From 2009, the establishing of broadband connections in Estonia has gone well. In larger cities, high-speed Internet connections are already widely available. Communications undertakings have built new fibre optic networks and adopted new technologies and equipment. The 100Mbit/s and faster connections can be used by one-half of households and companies both through FTTH and DOCIS 3 technologies. Mobile Internet is also making strides, data volumes quadrupled last year, 2011 – and an even greater jump is expected with the spread of 4G technologies.

Thus in places with enough potential customers, the market functions and communications undertakings ensure broadband connections for all comers.

Broadband connections for rural areas

Estonia's average population density is 30 per square kilometre. In rural areas, population density can be under 10. Thus it cannot be assumed that the market high-speed Internet will penetrate rural areas in Estonia. Yet the state is interested in keeping life going outside the largest cities and towns so that people could live, work and get an education everywhere in Estonia. To make people want to live outside the major population centres, they must have a high-quality living environment, jobs and education opportunities. Today no company or institution can function without an Internet connection. Nor can anyone imagine an education or research institution without high-speed Internet. Be it a basic school or university – without it there is no possibility of getting an education or engaging in research. Without a high-speed Internet connection, people's living environment loses in quality: no access to many services, no possibility of using modern communication media and even participation in information society is limited. Rapid high-speed broadband connections form a basic building block for development of rural areas.

Development of EstWin

To get high-speed broadband to penetrate rural areas in Estonia as well, the Ministry of Economic Affairs and Communications and the Estonian Association of Information Technology and Telecommunications (ITL) launched the EstWin project in spring 2009.

The project model is unique. The state and communications undertakings that would otherwise be mutual competitors act in concerted fashion. The state supports the construction of a fibre-optic cable based trunking network in all settlements. Communications undertakings ensure the supply of service to end consumers as well as sustainable management of the trunking network.

To implement the EstWin project, eight members of the ITL founded the Estonian Broadband Development Foundation (ELA). In ELA, the interests of all parties – ministries, local governments, communications undertakings – meet and they are all included in the planning of the trunking network.

The task of the ELA is to plan the trunk network based on the wishes of all parties, and to organize the financing of the construction of the trunking network and to build the network. The ELA is also the owner and operator of the completed trunking network. The function of the ELA is to ensure the availability of the network and its sustainable management.

In the beginning of EstWin, all of the fibre optic networks in rural regions were mapped and the plans of communications undertakings for establishing new networks were determined. As a result, the areas with market disruptions were found and an initial plan was put together as to where the network had to be established under the EstWin project. Altogether 6,000 km of network must be constructed.

The detailed network planning process is much more complicated and time-consuming, however. It involves many parties and different information is used. An address register is used to determine the location of inhabitants and buildings. Information on all schools, libraries, community centres, youth centres and the like is consolidated; the wishes of all local government with regard to connection sites are pooled as well. All of the information on existing networks, communications junctions, mobile towers and objects considered important for the state are specified in a card application developed specially for planning the broadband network. In addition, information both on road work planned by the Road Administration (as a majority of the cables are installed on roads) and other infrastructure development plans are used. On the basis of all this, about 30-50 km work segment projects are prepared and coordinated with all parties. The final decisions on each project are made by the EU support fund implementing authority – in the case of EstWin projects the Estonian Information System´s Authority, Estonian Agricultural Registers and Information Board and Enterprise Estonia. Financing applications for a total of 58 projects have been submitted for implementation.

> Without a high-speed Internet connection, people's living environment loses in quality. Rapid high-speed broad-band connections form a basic building block for development of rural areas.

Completed networks

The EstWin network has already extended to the territory of 77 local governments. Around one-fifth of the planned network – about 1,200 km – has been completed. A total of 420 network connection points have been built. A total of 1,300 km of network is still in the design stage, and this will be completed this autumn. The entirety of the completed network is described in detail in the network register; the necessary means have also been devised for getting information for network administrators, communications undertakings and other related parties. The entirety of the completed network and network under construction can be seen on the page http://ela12.elasa.ee/elakaart/.

For the next stage, a plan for 1,500 km of network has already been prepared, and it is hoped to start building it in 2013. If the rest of the »»

» development of the network goes according to plan, the entire EstWin network will be completed by the end of 2015.

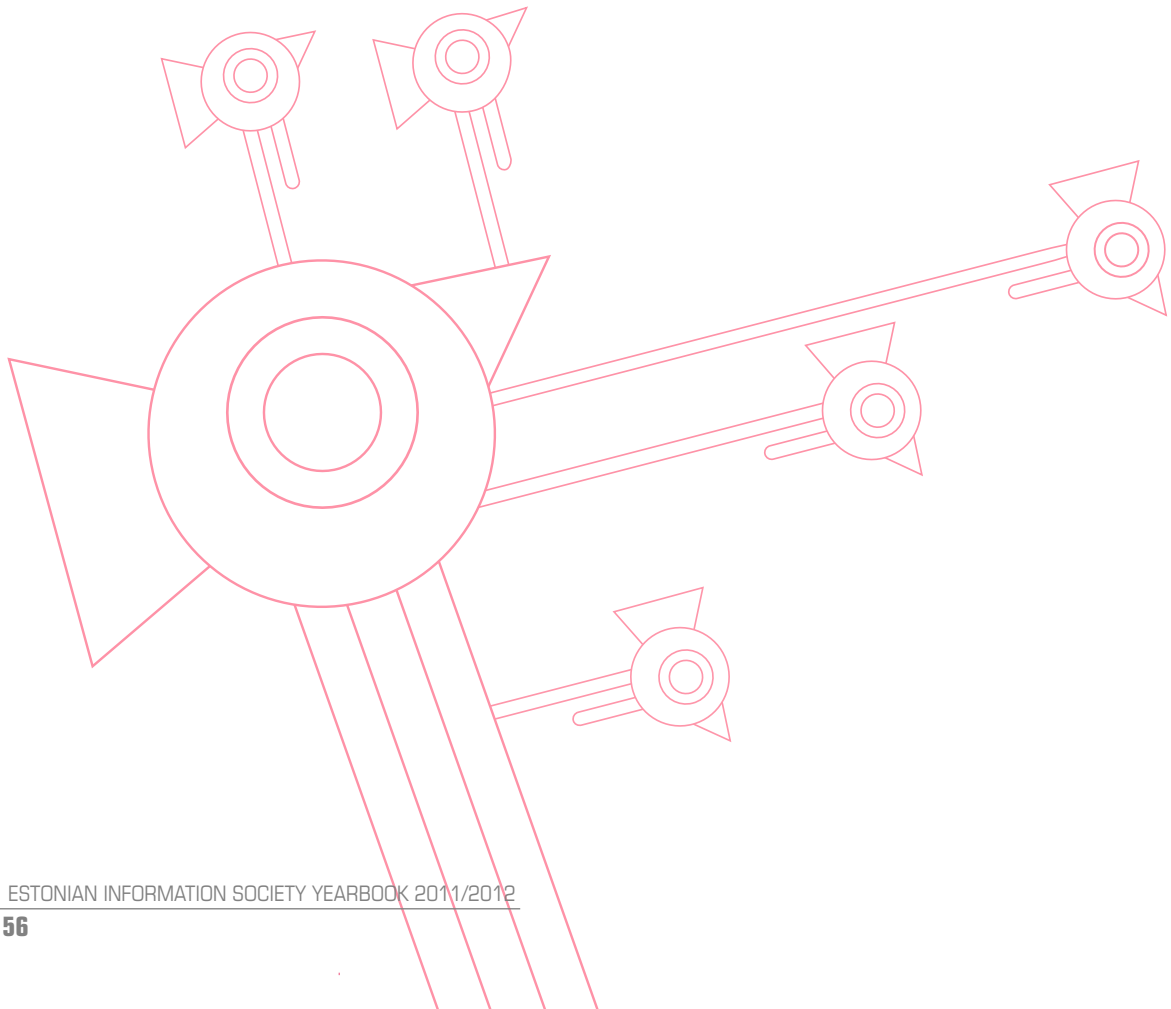
The finished network has 24/7 monitoring, and rapid fault elimination is ensured. Pursuant to the agreements with maintainers, all faults in the network must be eliminated within six hours. As this is a technologically up to date network and all of it is documented in detail, the likelihood of faults is low. During 2011 there was only one fault in the network, resulting in a temporary interruption of service and this was due to human error.

The network can be used by all communications undertakings and government departments on an equal basis. That means that the network is in common use for all who desire to use it. As the ELA is a non-profit organization, the users of the network must jointly pay only the network maintenance costs and financial expenses related to self-financing. Thanks to this the network usage fees are low and communications undertakings are able to offer high-speed Internet even in regions sparsely populated with potential customers. There are now close to 200 product agreements signed for the use of parts of the network.

International interest

The EstWin project has proven that it is possible to rapidly develop a nationwide broadband network if there is a clear goal, if all parties' interests are taken into consideration and if there is a strong organization that carries out the project. Our success has not gone unnoticed in other EU member states. A number of states have expressed interest in our operating model, and also want to develop broadband connections: for instance Latvia and Finland, as well as more distant countries such as Poland, Spain and Italy.

Although the problems and opportunities of the countries vary, we certainly have something to pass on to others. Our experience from the EstWin project could end up being an export article to EU countries that want to develop high-speed broadband.



4G: Estonia's mobile Internet – opportunities and success story

ANDO MEENTALO
ando.meentalo@emt.ee
AS EMT

When the Estonian government handed out the frequency licences as a result of the first 4G bidding on 17 December 2010, an unofficial world record was set in Estonia – the EMT 4G-network was launched and placed in the use of users just six minutes after the licence was issued! Fittingly for Estonia, the first client was IT visionary Linnar Viik.

The EMT network was the world's 11th 4G network. What was important was that the state chose to charge a moderate licence fee and in exchange operators had to guarantee that the network would be built rapidly. The result: already by 2014, all of Estonia will be covered by a new-generation mobile broadband network. These are speeds which many regions could thus far only dream of.

High speeds were the key to success

The mobile Internet age in Estonia began in October 2005 with EMT's 3G network. In 2003 the first 3G tests were conducted, the primary visible difference appeared to be the possibility for video calls. When the service was actually launched in 2005, the most popular applications were the viewing of traffic cameras in order to circumnavigate traffic congestion and Mobile-TV, viewable on a cell phone's small screen. Today, the actual success factor in 3G mobile communications is mobile Internet: high-speed broadband everywhere in Estonia and usable with the same device and wide array of services as in other countries.

At the time of the launch, Internet usage on traditional computer was still lagging behind interest from users. A more rapid phase of growth started in 2007, when coverage as seen on a map of Estonia had become so widespread that it caught the eye and the price of equipment became affordable. No less important was the fact that the ease of use of the mobile Internet no longer required an IT education as the use of earlier equipment was like a battle between the computer's hardware and software. But now anyone could make do with a USB modem.

What happened next was a time of increasing speeds. The speeds were sufficient for net surfing, but the multimedia era with YouTube and video clips on news sites signalled that the existing 3G networks would soon be too limiting for users.

In late 2009, TeliaSonera launched the first commercial 4G networks in the Nordic countries and by February 2010 EMT – owned by that group – opened the first LTE-technology-based test network. The new network offered everyone a speed of up to 100 Mbit/s. Only a few months were left before launch. »»

» We will certainly be expecting that the EstWin project being developed as a public-private initiative will be of much help in expanding this network. It should allow rapid trunking connections to connect stations outside towns and villages. After all, in coming years, the 4G technology will also develop in terms of speed, up to 1Gbit. Only a fibre optic trunking network will allow such speeds to be transmitted up to the base stations. It is not beyond the realm of possibility that by the end of 2014 most of Estonia's territory will be covered by 4G.

What did 4G bring Estonia?

The fact that Kohila got the first 4G station certainly caused some interest, as Kohila is outside urban areas and is not even a county seat. "Does someone have a good friend who lives there?" was a question frequently asked. But the truth was that the new developments were home to people who need high-speed Internet and had not previously enjoyed it. People like this are the reason the network is being established!

Realistically, 4G is the only technology that can be expected to bring speeds of up to tens of megabits to Estonian homes, especially in sparsely settled areas. It is unrealistic for fibre-optic or copper pair services with a comparable speed to reach every home.

As mentioned, the biggest drawback of the 3G network was the fact that it was not possible to use future high-res mobile multimedia services. 4G will allow large-screen digiTV services to reach users at the same level of quality as that offered by cable companies. Today's 3G allows such services to be offered at a high quality on small smartphone screens, but 4G will bring a "Triple Play" to us all: telephone, Internet and TV all in one. The first good selection of mobile TV services is expected to reach market this year or next.

Video, TV, online games

The developments in hardware that have brought tablet computers with 4G support are bound to accelerate consumption of video content. They are handy for surfing the Internet, but also make a good additional screen at home or for showing movies to the kids in the back of the car.

Video and image content providers are just as interested in 4G, as they can bring news directly to viewers without satellite transmission stations and cable subscriptions. And the 4G network is the thing that will make security cameras installed at remote forest cabins truly effective.

For businesses, 4G is of interest for manufacturing units that need high-speed Internet before cable connection reaches their area. In practice, remaining wireless is a feasible choice in the case of 4G. This seemed unrealistic just a few years ago.

We will soon see smart TVs that use a SIM card slot for a connection to TV and Internet services. The only cord a 4G TV will need is the 220 V power cable. A futuristic vision? It wasn't so long ago that WiFi on a TV set seemed strange. Then WiFi was available as an add-on, but now it is a natural feature on new TVs.

One circle that has viewed mobile Internet with pragmatic scepticism is the online gamer community. Game consoles and computer games require good reaction time to beat one's opponent 3G didn't seem quick enough on the uptake. 4G solves this problem, offering capability just as good as any competing technologies.

Recently there was news of a driverless car that would pull information off the Internet. Certainly such a car would require high-speed feedback to improve the quality of the driving. Given Estonian roads, imagine how much information could be transmitted to the car about potholes? And certainly one should not forget that drivers need quality Internet and additional features – why not send friends picture of all those scenic views from the car window – in real time?

Where do we go from here? 4G/LTE technology will develop not just in terms of increased coverage but also speeds. Certainly speeds in the hundreds of megabits in the near future are not a utopia. The selection of hardware will also broaden.

4G will not be restricted only to Estonia. The world is bound to become much smaller and 4G/LTE is a technology that will spread much the same way in Europe as it does in America and Asia. It is important for Estonian service providers and software developers – and naturally customers – not to lose their head start and that they remain in the vanguard when it comes to tapping the potential of 4G.

4G mobile ultra-broadband Internet to rural areas

ANDRUS KAARELSON
andrus.kaarelson@elisa.ee
Elisa Eesti AS

Today all of the wireless operators have launched 4G base stations in the 2600 MHz frequency band. Elisa has launched 4G test networks in five Estonian cities: Tallinn, Pärnu, Viljandi, Haapsalu and Tartu city centre.

As this band has a very limited range, these 4G base stations will have more of a supporting function for increasing data transmission rates. All the operators are looking ahead eagerly to the competition for operating licences in the 800 MHz band, which should take place 2013. This technology can be used by operators to bring the 4G network to every corner of Estonia.

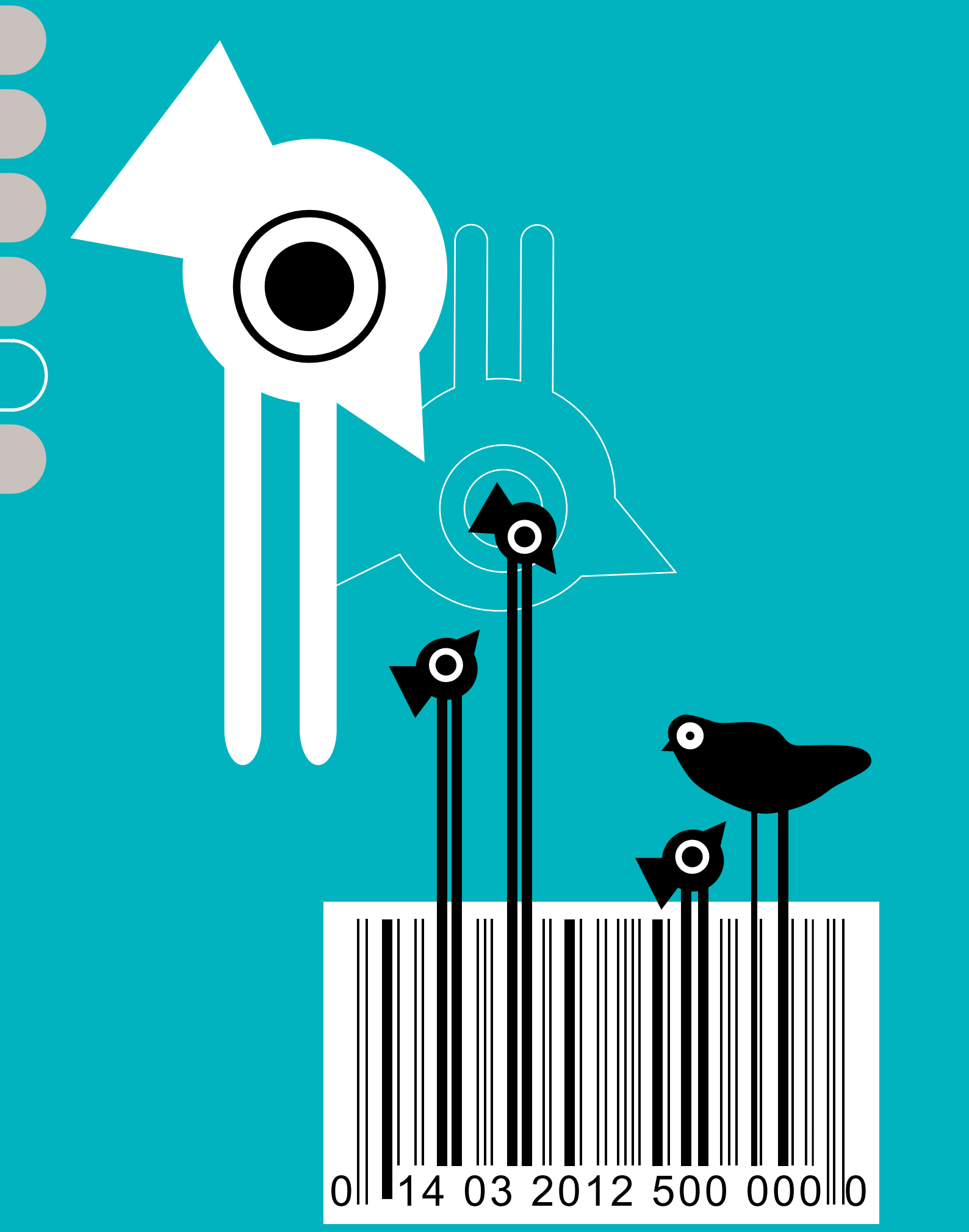
Elisa has already launched testing of the 800 MHz band. In March, the first test areas were opened in the small town of Kobela in Võru County and the western city of Haapsalu. All of Elisa future 4G development plans were developed for the 4G 800 MHz frequency band. This frequency will enable the building of a 4G network that offers blanket high-speed mobile Internet coverage countrywide. In this frequency band, Elisa will also be working together with the EstWin project launched by the state. EstWin and mobile Internet are closely related. The last 1.5 kilometres of Internet connection to a customer's home can be built very effectively based on mobile Internet, and this is much more cost-effective for customers.

Pursuant to Estonia's new generation broadband network development vision prepared by the Association of Information Technology and Telecommunications in April 2009, all households, companies and institutions must by 2015 have access to a 100 Mbit/s broadband connection. Achieving this goal depends directly on the EstWin project. By 2015, a fibre-optic cable network will be ready and this will cover all settlements in Estonia. As a result, 98% of households, companies and institutions must be closer than 1.5 km to the network.

LTE 800 MHz is a technology that allows the last 1.5 km to be covered between customers and the Estonian Broadband Development Foundation developed fibre optic cable network, and thus bring 4G Internet to every customer's home or office. EstWin will allow Internet to reach rural homes of residential customers. Moreover, businesses and public sector organizations such as schools, libraries and local governments also need a high-speed Internet connection.

Compared to the LTE 2600 MHz frequency handed out the year before last, the 800 MHz connection will allow Estonia to be covered with high-speed Internet faster as about five times fewer base stations will be needed than in the case of 2600 MHz. The lower frequency will also ensure better indoor reception thanks to which customers will enjoy higher-quality service and much faster Internet connection speeds.

The 4G LTE standard based network will allow mobile ultra-broadband Internet to be provided to customers. The 4G network based on this novel technology will increase mobile data download speeds to as high as 100 Mbit/s and upload speeds to as much as 50 Mbit/s.


0 14 03 2012 500 000 0

CHAPTER 5
ELECTRONIC IDENTITY

January 2012 marked the 10th anniversary of the issue of the first ID card in Estonia. Today, it is clear that the decision made at the end of the 1990s – to adopt universal certificates that can be used in any application – has paid off. The ID card has long ceased to be seen as just an additional identity document, it is a secure tool used frequently by the public and private sector in their services and IT solutions. Public Key Infrastructure, which covers the services necessary for giving and verifying digital signatures, and the ID card are the two cornerstones of the state information system, on which Estonia's international reputation as an e-state is largely founded. This chapter gives an overview of the Estonian eID ecosystem and its most important components, such as digital timestamping, mobile-ID and digital ID. The last article in the chapter looks at challenges related to digital signatures in the context of the European single market. Before reading the chapter, it might also be interesting to take a look at an article published 10 years ago in the yearbook, which discusses the ID card (http://www.riso.ee/en/pub/2002it/).

Ten years of the eID ecosystem

TARVI MARTENS
tarvi.martens@sk.ee
Certification Centre Ltd

MARK ERLICH
mark.erlich@ria.ee
Estonian Information System´s Authority

TAAVI VALDLO
taavi.valdlo@riso.ee
Ministry of Economic Affairs and Communications

UUNO VALLNER
uuno.vallner@riso.ee
Ministry of Economic Affairs and Communications

Over ten years, electronic identity (eID) has become a self-organizing ecosystem in Estonia. By the end of the 20th century, strong traditions in security expertise developed in universities, and the public and private sector. Banks and telecommunications companies were among the most active parties. The parties shared a common interest in wanting to develop a practically functional public key infrastructure (PKI) and thereby create new opportunities for commerce. The ideas from back then were transformed into decisions made at the political level,

and they created a basis for public-private cooperation. Today 1.2 million people hold a valid ID card, of whom 85 percent are Estonian citizens and 15 percent of whom are foreign nationals. In ten years time, 72.6 million digital signatures have been given and close to one-half of ID card holders have used the document electronically.

Institutions have begun to understand the advantages of digital signing. For instance, a study conducted by the Certification Centre and MoZg Agency[1] found that digital signing allows Eltel Networks to save 1,380 euros every month while the University of Tartu saves 11,500 euros, comprising half a million euros in four years. The greatest savings come on workforce expenses, and printing and postal costs.

In building public key infrastructure, ecosystem components should be dispersed as much as possible in the interests of security. Decentralization ensures transparency of processes and avoids single point of failure risks, which are characteristic of monopolistic, centralized systems.

eID is one of the priorities for the public sector. In administrative proceedings, electronic channels are considered the equivalent of written ones. Digital identification and digital signing are in widespread use in administrative proceedings. Estonia wants to continue to be a leader in this area in Europe, taking part in many international projects such as STORK and e-CODEX.

In STORK (Secure idenTity acrOss boRders linKed) a cross-compatible eID platform for all of the European Union is being created. The participation of our experts in the next phase, STORK 2.0, will ensure that Estonian entrepreneurs have secure access to Europe's Internet-based systems and allow European entrepreneurs to electronically use information systems and websites both in the e-state and private sector. Among the goals of the European Union's cross-border IT project e-CODEX is to establish possibilities for widespread use of electronic ID cards and digital signing in digital cross-border judicial proceedings.

Who's who in the eID ecosystem?

Persons are the most important participants in the ecosystem. The manner in which a population adopts new solutions affects the development of the entire ecosystem. Every person has an identity – a self-knowledge. The person passes on a part of that knowledge to other parties with whom he or she agrees on the name/identifier for the person, such as site account, bank account, personal identification code in dealings with the state. It is especially important for persons to open part of their identity to independent third parties, such as the state or certification authority. The person gives the state data about him or herself (name, images etc) that allow the person to be identified unequivocally. The state assigns a unique ID (personal identification code) to the person and issues his or her so-called papers (passport, ID card etc). A third party can use such an identity, linked to a so-called qualified certificate, to digitally authenticate identity.

In the digital world, a person uses passwords, PIN codes and certificates, etc to prove that he or she is linked to the identifier. Under Estonian law, a person uses a qualified certificate to authenticate his or her association with the identifier. In Estonia, a person's basic certificate consists of the certificates on the ID card for digital identification and digital signing.

To obtain an additional certificate, a person chooses a certification service provider, receives a certificate and uses the basic certificate to activate the service provider's certificate.

Institutions. A second major component of the ecosystem is institutions. The motivation of institutions to accept digital signatures and to create systems that support certificate-based authentication and signing has been one key to Estonia's success. One leader in this area has been the public sector, as institutions are required under the Digital Signatures Act[2] **to accept digitally signed documents.**

The Police and Border Guard Board (PPA) is one of the most important players in the eID ecosystem. The PPA is responsible for assigning and administering identity for residents. The PPA's roles in regard to PKI are the following:

- issues ID cards and digital IDs and ensures they have the qualified certificates issued by the certification service providers;
- ensures that citizens have a means, through an activation service, to link/activate their eID with the qualified certification service provider's certificates.

In Estonian conditions, the PPA covers the life-cycle costs for residents' basic certificates, ensuring »»

» free-of-charge administration of the certificates and is responsible for the security and conformity to the requirements of the means of secure signing (card, chip, chip operation system, encryption algorithm etc).

Certification Centre (SK)

Digital trust service providers issue qualified certificates and offer digital trust services. In the digital world, trust service providers are at the heart of PKI. In the case of qualified certificates, the provider of certification service must ensure that consumers have the possibility, by way of activation, of linking an issued certificate with the eID administered by PPA. In Estonia, the primary service provider is AS Sertifitseerimiskeskus (SK) – Certification Centre Ltd.

The Certification Centre, founded in 2001, is a state-accredited company that specializes in certification and timestamping service and developing and operating the related software. The founders and owners of SK are, in equal parts, Swedbank, SEB Bank, AS EMT and AS Elion Ettevõtted. Primary activities of SK:

- providing certification and timestamping service;
- developing digital signing technology and applications;
- offering validation services;
- consultation services.

SK, being the partner of the Estonian state, issues certificates for state identity documents (ID card, residence permit, digital ID and mobile-ID). In addition, SK provides certification service for electronic tachograph project in Estonia, Latvia, and Lithuania. SK is also the partner of the Lithuanian mobile operator Omnitel in providing certification services. On a commission from the state, SK developed the middleware needed to use the ID card, including the DigiDoc program, which allows digital signing, verification of the validity of digital signatures and encryption of data.

SK is one of Europe's leading firms in the field of eID. The Ministry of Economic Affairs and Communications has authorized SK to represent Estonia in a number of European initiatives. The most important of them are expertise in developing the trusted service lists and the digital signature format and the aspects related to electronic exchange of data at points of single contact as required by the services directive.

The Department of State Information Systems (RISO) at the Ministry of Economic Affairs and Communications is responsible for general ICT coordination at the state level. With regard to eID ecosystem, RISO's specific roles are as follows:

- organizing the activities of the interagency working group on electronic identity;
- legal regulation of PKI;
- supervision over digital trust service providers;
- chief processor of the digital trust services register;
- organization responsible for interoperability of eID infrastructure.

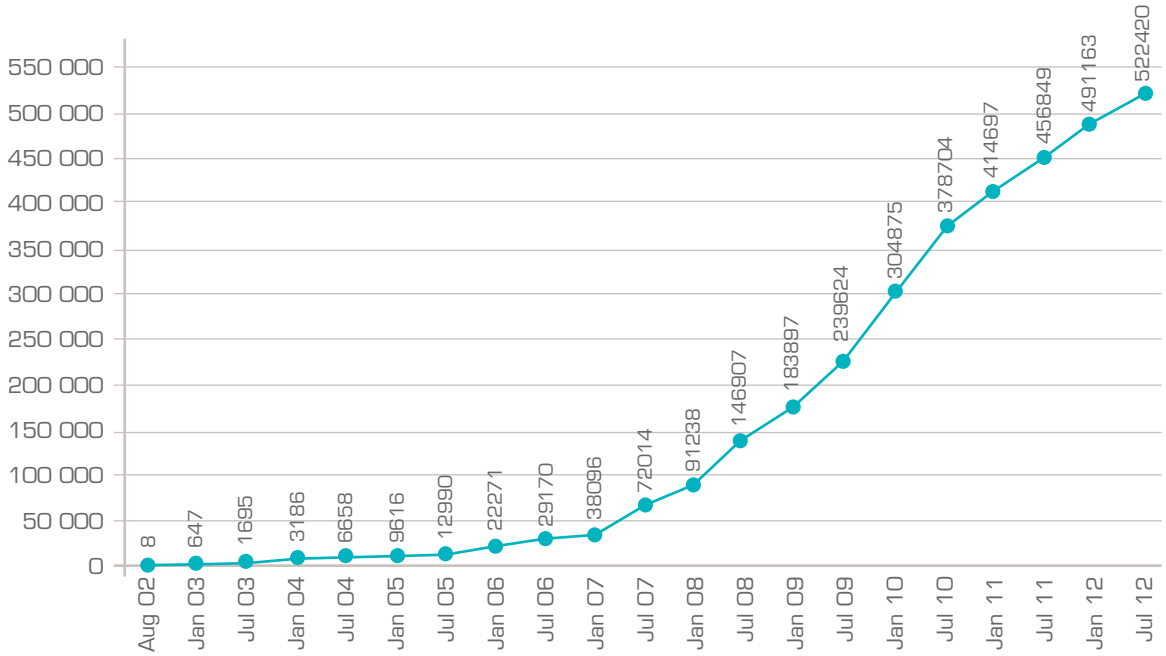
Estonian Technical Surveillance Authority (TJA) is the authorized processor of the digital trust services register. The trust services register records all of Estonia's certification services and other trust services as well as the service providers. The TJA administers the Estonian list of trust services, EE-TSL, and associates it with the master list of European TSLs. The TJA evaluates other European certificates and keeps it in the VTSL, the list of external trust services.

The roles of the Estonian Information System´s Authority (RIA):

- developing and administration of the digital signature infrastructure;
- organizing PKI development projects through structural funds;
- organizing ID card middleware development projects;
- incubating PKI solutions.

The Centre of Registers and Information Systems (RIK) under the Ministry of Justice is one of the pioneers in developing cross-border services in Europe. Using the E-Business Register, a company can be registered using an ID card in just a few hours and without leaving home. In addition to founding a company, the register data of a company may be changed using the Company Registration Portal and annual reports can be filed electronically. The website accepts ID cards from Finland, Portugal, Belgium and Lithuania.

The Ministry of the Interior's IT and Development Centre (SMIT). The Ministry of the Interior´s and PPA's IT projects are implemented through SMIT - for instance, systems for verifying personal data, entering data on wanted persons and forwarding them to the European Schengen information system.



Number of and growth in the number of electronic users of the ID card August 2002 – July 2012

AS Cybernetica. Cybernetica is one of Europe's leading providers of security solutions. Cybernetica came up with the first solution for certification register. It developed the certification centre for the X-road, the data exchange layer for state information systems. For years, Cybernetica has also been a provider of trust services. Cybernetica has designed PKI solutions for other countries.

TRÜB AG. TRÜB prints Estonian ID cards and provides PKI services at chip level.

AS GuardTime. GuardTime is one of Estonia's accredited timestamping service providers. It offers user keyless service. The National Archives of Estonia plans to use it in the public sector.

AS Smartlink. Smartlink is a professional system integration and software development company that prefers open platforms. Smartlink has been engaged in developing the middleware for ID cards and developing the cross-border validity certification service.

Ideelabor. Ideelabor specializes in resolving electronic identity and related platform specific problems related to eID. In cooperation with the Certification Centre, basic ID card software for various platforms has been developed. Ideelabor specializes in services based on the OpenID standard and the widespread use of ID card and mobile-ID infrastructure in online applications.

To sum up: Estonia's eID ecosystem has been created and it is functional in cooperation between public sector and private sector. Estonia has a unified public key infrastructure and eID solutions are universally usable, satisfying the requirements of even the highest-security fields.

1 http://www.sk.ee/en/useful/digitalsigning

2 https://www.riigiteataja.ee/akt/13314840 (in Estonian)

Mobile-ID – one of a kind

HELAR LAASIK
helar.laasik@politsei.ee
Police and Border Guard Board

"Estonia has stood out at the world level in the past by boldly adopting innovative e-solutions and I am glad that the next step is the use of mobile-ID to vote in elections. Western democratic traditions and modern technology make a good match."

Minister of Economic Affairs and Communications Juhan Parts

EMT first introduced mobile-ID in May 2007. It was initially available only to the company's own customers. Later on, other operators started offering the service – Elisa and Tele2. The service proved extremely popular among the users, and the number of service providers that enabled mobile-ID logins grew quickly. The rapid spread was attributed mainly to ease of use and the lack of a need for an ID card and ID card reader.

Now Estonia had an identification medium that met technical security requirements, but which could be used only outside the public sector. As its popularity grew, there was a push to recognize mobile-ID as an official document. And when the February 2011 parliamentary elections drew near, the aim was set – to make it possible to voters to authenticate themselves via mobile-ID among other means.

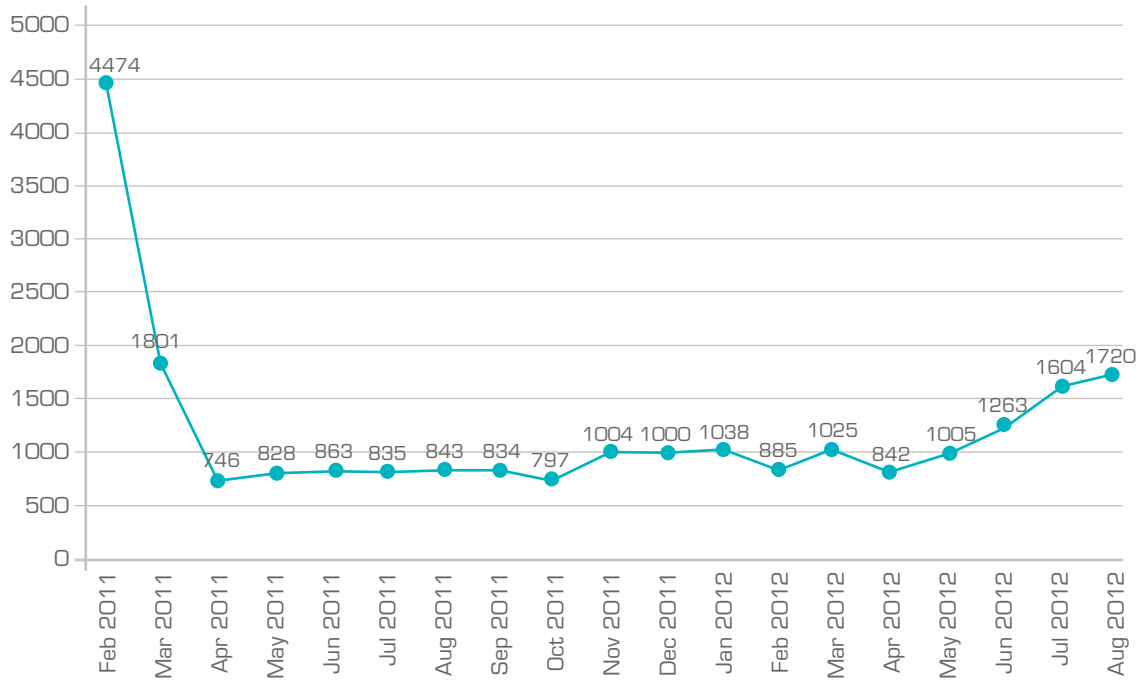
There were two main obstacles to official recognition.

First, there was no mention of the medium in the Identity Documents Act – this hindrance was eliminated with a rewording of the act that entered into force on 1 January 2011.

Secondly, the mobile-ID was issued outside the state's jurisdiction. The question arose: how could the state be sure that it can be liable for the new document falling into the wrong hands, and what risks lay in wait here? To this point, a Police and Border Guard official had established the identity of users, but mobile phone companies were the ones who issued mobile-ID compliant SIM cards to users. It was considered inconceivable for people to make multiple trips to mobile phone company customer service and Police and Border Guard office. Thus it was up to mobile telephone operators who were charged with ensuring proper identification procedure.

After considering several alternatives, the solution was found: certificates could be activated by users through the Police and Border Guard web environment, which is entered by ID card. This solution was possible due to the obligation that ID card users keep their document and PIN code from falling into unauthorized hands. It was presumed that a person activating the mobile-ID certificates would log into the application environment under his or her own name and such an authentication would be sufficient in the eesti.ee state portal and for banks.

After entering the application site, the applicant must digitally sign a pre-generated application (the field contents may not be changed) and after confirming that the data are correct and the



Number of mobile-ID applications per month

certificates in order, the system issues a positive decision to activate the certificates. Mobile-ID is the only identity document where a decision can be made without human involvement. If an error becomes evident, the process is halted and the application is reviewed by the customer service representative.

In the first few weeks the system had to be fine-tuned to work in the real environment, the activation on a large scale of the mobile-ID cards already issued helped to disclose the bugs quickly. By April 2011, the number of applications stabilized at 1000 a month and has remained at the same level ever since.

Unlike ID card users, the deadline for filing annual reports did not catch mobile-ID users unawares – there was no increase in applications in June 2011.

Today, mobile-ID is yet one more unique means at the disposal of e-Estonia for authentication and digitally signing documents, a step that other countries are only now beginning to develop.

Digi-ID is a big help

HELAR LAASIK
helar.laasik@politsei.ee
Police and Border Guard Board

When the idea of Digi-ID started germinating, Estonian information society had reached a level in its development where some active people's lives could conceivably come to a standstill in the absence of a digital environment and ID card. Such people faced the prospect of once again having to go to a bank in person, or of transacting business face to face with city government officials. Doors equipped with ID card readers would no longer open for them, and so on.

From the user's standpoint, the ID card can be compared to a washing machine, car or even a particle collider – sometimes even it can break down. After all, it is nothing if not a miniature computer concealed in a plastic shell.

There had to be some way of minimizing the amount of time that people were cut off from the e-world they were used to. Estonian law mandates that people must be issued a new ID card within 30 days. In some situations, though, the month's wait is equivalent to the earth standing still.

The ID card is a secure document and its production, personalisation and logistics must meet many stringent requirements, unfortunately it is not possible to reduce the time from application to issue beyond a certain point. Some other solution was needed.

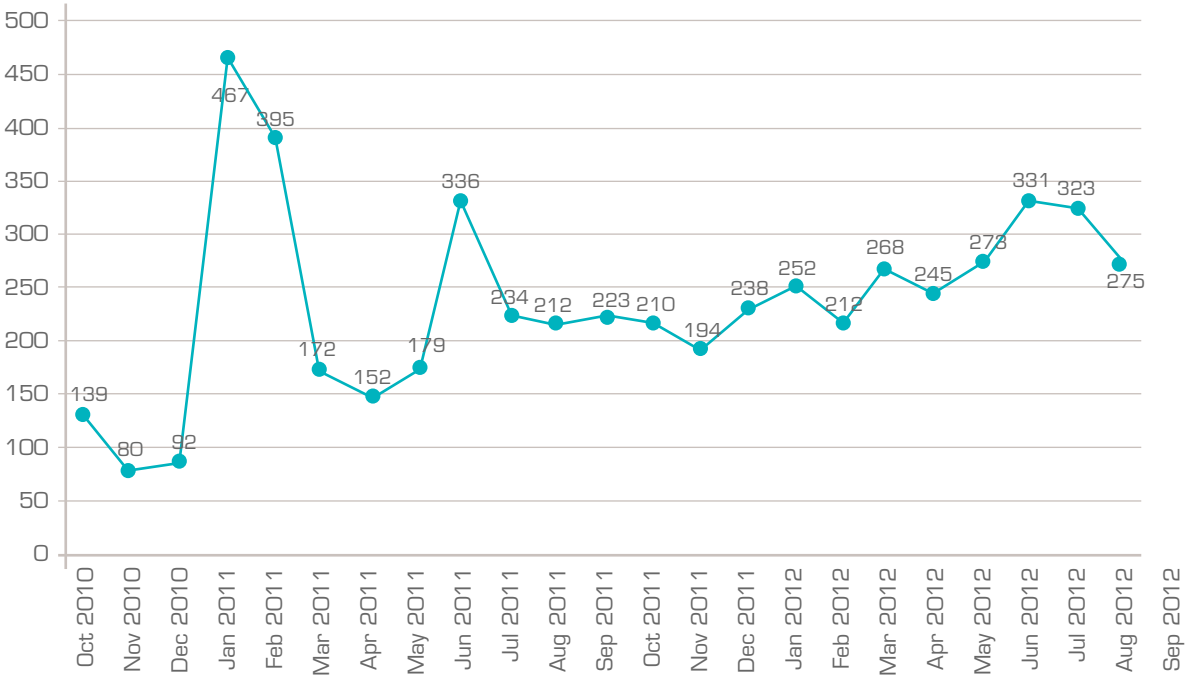
The Citizenship and Migration Board – at that time an independent authority – started developing a solution for expedited issue of an identity document. But issuing an personalised ID card on the spot was not an option, as the necessary technology was extremely expensive and personalisation must by definition take place in an extremely restricted-access environment, which no customer service area can ever be. For this reason, it was decided to establish a new type of document that has no known counterpart anywhere in the world – an identity document that works only in a digital environment. As a digital environment allows a secure area to be set up for individualizing a card, even a customer service office can also individualize an electronic document.

Digi-ID is a MultOS card. It lacks a personal data file, and the information needed for authentication and digital signing is read from the certificates on the card. The facial image and signature image of the user are not encoded on the card and thus heat-transfer printing can be used for visual information. This is not as high-security a means as laser engraving but neither does it require expensive personalisation devices. The card bears a notation that it cannot be used as a visual identity document.

The quick ID, as it was called at first, was first mentioned in 2007, but work began in earnest in autumn 2009 and October 2010 saw the issue of the first 139 Digi-IDs.

The adoption of the new document required changes in a number of fields. For instance, a new wording of the Identity Documents Act had to be drafted and passed by Parliament. The Certification Centre took care of the possibility that more than one certificate pair could be issued to one person, and developed changes to certification policy. Trüb AG produced the blanks and got them ready for personalisation at the customer service bureaus of the Citizenship and Migration Department, which was then already

Digi-ID design



Number of Digi-ID applications by each month

part of the Police and Border Guard Board. The printers for personalising the blanks were installed in the Police and Border Guard Board offices. The printers can be used to apply visual data on to the cards as well as enter write electronic data on to the chips. The Ministry of the Interior's IT and Development Centre carried out the first changes in the Citizenship and Migration Department's information system stemming from the adoption of the new document type and the personalisation equipment. The developers of the user applications updated their own systems to start using parallel certificates. There was plenty of work for many parties.

The number of applications for Digi-ID has kept on growing. Excepting the Digi-IDs issued together with the new ID card in early 2011, the number of Digi-IDs issued rose in June 2011, when the deadline for filing annual reports on companies drew near. As this was the first time it had to be done in a fully digital manner, a number of company officials discovered to their inconvenience that their ID card did not work and they could not digitally sign their annual reports. Applying for a Digi-ID proved to be a quick fix, allowing the necessary procedure to be performed.

Digi-ID has now claimed its rightful spot in Estonia's suite of identity documents. People whose ID card has become non-functional or who need an additional combination of the electronic and physical functionality not offered by mobile-ID can resort to Digi-ID.

How to put the eID ecosystem to good use for your service?

URMO KESKEL
urmo.keskel@sk.ee
Certification Centre Ltd

The ID card and mobile-ID are the basic pillar of e-Estonia and have allowed the country to develop a set of online services that would not otherwise be possible. Often a complaint is heard upon adding eID support to services: that it is technically complicated and results in additional work for developers.

In this article, I will describe how e-service providers could make their lives easier, spend less time dealing with the technical details of eID and focus on developing the business functionality of their service. This simplicity is made possible by DigiDocService – a SOAP-based Web service that offers digital signatures, signature verification capability and eID authentication functionality.

The first version of DigiDocService was released to the public in 2004 and made it possible to sign documents digitally using an ID card and process DigiDoc files. DigiDocService was launched with the goal of providing an easier way of adding digital signature support to small and mid-sized information systems. Today, the functionality offered by DigiDocService has become much broader than it was in 2004: DigiDocService has become one of the key components in mobile-ID service and there is now also the possibility of using the service for authentication with an ID card.

The number of e-services that use DigiDocService has grown to several hundred, much more than was anticipated in 2004. Thus it can be said that the DigiDocService concept has paid off.

The primary advantages of using DigiDocService web service compared to DigiDoc are the following:

- The DigiDocService protocol is much simpler compared to DigiDoc libraries.
- There is no need for web service users to expend effort on various dependencies that use of libraries tends to cause, installation of additional system and third-party libraries is not necessary, as all of today's development frameworks have SOAP support.
- The corrections made to DigiDoc libraries, and changes related to certificates are centrally administered – e-service providers and developer have much less work to do in implementing version updates.

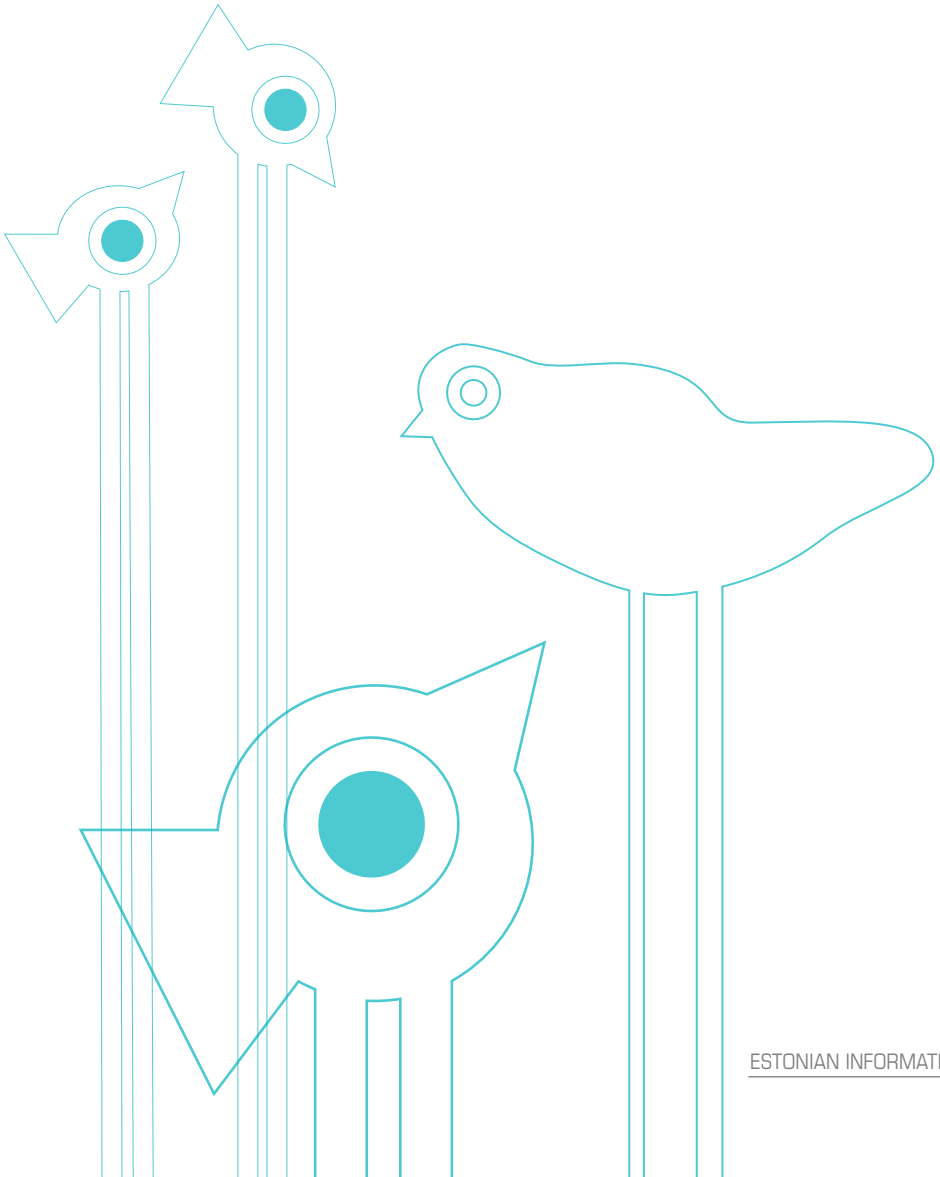
Still, there are situations where use of libraries is necessary or preferred. DigiDocService does

not offer encryption/decryption functions. And in the case of very large batches of digital signatures as well, it is sometimes more reasonable to handle the signing through libraries. Likewise, when using DigiDocService, e-service providers must take into account that more data is sent to the service regarding the document being signed than in case of digital signing using DigiDoc libraries.

DigiDocService was also developed with thought given to how ID-card-based authentication could be implemented in as simple a manner as possible for e-service providers. One problem related to authentication has been the conversion of data in the certificate into the right code and how to perform checks of the certificate using OCSP service. It is possible to forward to the DigiDocService the certificate of the person entering the e-service, which was received during authentication. The personal data in the certificate and information on the validity of the certificate are contained in the response. DigiDocService itself makes sure that the validity of the certificate is verified from the right source and ensures that the data in the certificate are always returned in the same form and format.

From the field of e-services in Estonia and Lithuania, there is good news. To this point, the mobile-ID function could be used with all Estonian wireless operators and Lithuania's largest operator Omnitel, as of spring 2012, support for Lithuanian wireless operators Bite and Tele2 is also newly available. In addition, the Lithuanian ID card is supported. Thus the DigiDocService platform is interoperable with all users of Mobile ID and ID cards in Estonia and Lithuania.

DigiDocService offers a great opportunity to keep up with eID developments and to put the possibilities offered by eID infrastructure to work for your business in e-services and information systems.



Digital stamp

ANNIKA LJAŠ
annika@sk.ee
Certification Centre Ltd

We have grown accustomed to a good authentic document being laid out on the letterhead of the institution or company and furnished with a relevant stamp. But in some sense it is paradoxical as ink impressions have no legal force. Nor is it known how the company or department coordinates the security of the use of the stamp. In the digital world, however, an entirely new quality can be conferred on stamps – a digital stamp that can only be used by a specific department or company. The head of the company or department is responsible for the use of the stamp and he or she can delegate this responsibility at his or her discretion.

Digital stamp significantly increases the reliability of a document issued by an institution or a company as it gives the recipient certainty that the document originates from namely that entity. Digital stamp cannot be forged and it provides a way to determine whether the person that stamped the document has the requisite authority to do so. If the digital stamp is used in conjunction with digital signature, there is ironclad certainty that the signer is connected to the institution/company.

The Certification Centre (SK) has been issuing digital stamp certificates since 2004. In 2009, digital stamp was also introduced into the Digital Signatures Act. Digital stamp is issued only to institutions and companies and SK first performs verification as to whether the relevant company/institution has the right to receive the digital stamp. It also checks whether the person requesting the stamp has legal grounds to represent the company/institution. With its internal procedures, SK ensures that the digital stamp gets in the hands of the correct person. An institution or a company can have different digital stamps - for instance for issuing invoices and data and for submitting offers. In general, the digital stamp is used on a crypto-stick containing the certificate's private key and the corresponding certificate and it works in the same way as giving a digital signature. The software is also common to each – DigiDoc. A program called TempelPlus was developed for batch stamping which can be integrated with most information systems and in addition, automated. For instance, if a company's information system sends partners automatically generated letters and notices.Thus the employee does not need to spend time on separate digital stamping of documents.

Who is already using the digital stamp? Banks issue digitally stamped confirmations of payment orders that substantiate that the payment has been executed. Real estate appraisals and digital powers of attorney and contracts sent to leasing firms and banks are also validated by digital stamp. Digital stamping is also actively used by the Government Office when it sends cabinet decisions for publication in the State Gazette.

A good example of the savings in time and ease of use achieved with digital stamping is the graduation certificates issued by the National Examinations and Qualifications Centre each June. Previously 40,000 graduation certificates had to be printed out on paper, filled in and posted, which took over two weeks and was very labour-intensive. In addition, an electronically stamped graduation certificate is much more secure, as it cannot be counterfeited and has timeless legal force.

Estonia is one of the few countries in Europe that has made digital stamp part of its law. There is great interest from the rest of the world in Estonia's experience in this field. It is exceedingly likely that digital stamps will become legitimatized throughout Europe in the regulation on electronic identification and trust services that is currently under consideration.

Digital signatures in Estonia and the rest of Europe – a look back and ahead

TARVI MARTENS
tarvi.martens@sk.ee
Certification Centre Ltd

Estonia's clear leader position in Europe and worldwide[1] in the field of electronic identity (eID) is no surprise – it's the result of 10 years of work. While a number of other countries have also issued Estonian-style ID cards to the population, Estonia is unique in that the cards are actually used electronically. Nearly half of Estonia's adult population has used their ID card at least once over a computer; while the average ID card or mobile-ID user tallies about 20 authentications or digital signatures per month.

Seeing the digital signature the same way

Estonia appears to be the only country where the validity of digital signature is considered beyond reproach and where there are no fundamental technical problems in using them. The reason for the success is choice of strategy – already back in 2002, a number of freeware programs were released to end users and system integrators. All of the components of the software processed the same document format – the DigiDoc format, .ddoc-extension files familiar to us. Everyone assumes that the digital signatures they generate are legitimate, have long-term validity and are legally accepted in Estonia. They're right!

In contrast, the view of digital signatures in Europe differs greatly and often it is e-service-central: a website prompts the user for the PIN2 at some point and then thanks them – the system does not return the digitally signed output. The reason for this is largely the fact that every e-service generates digital signatures in a proprietary format and for internal use only.

On one hand, the problem for Europe is that the scope of application of the electronic signature directive that entered into force in 1999 is too lax. Estonian legislation requires certification that the signer's certificate is valid at the time of the signature (incidentally, that is why we must be connected to the Internet at the moment of the signature – so that this confirmation can be obtained). The directive does not require this, though. Worse, the directive mandates that digital signature generated by means less secure than the Estonian ID card or mobile-ID are also to be accepted. This has all led to a state of neglect, meaning that digital signatures are viewed in practice more as a »»

» security measure that has little to do with an actual signature.

A second problem for Europe is the large number of digital signature standards and the laxity of these standards, occasioned by the nature of the directive itself. The most popular standard, the one Estonia uses, too, XAdES[2], is long and wide, allowing different security levels as well as internal technologies and formats. DigiDoc is nothing but a specific XAdES profile that ensures the highest level of security and which keeps internal options to a minimum. Many of the producers of software compatible with XAdES support all of the options allowed by the standard, posing a difficult problem for the user – how could a signer know what kind of signature the verifier "likes"?

Latvia (their XAdES profile is called edoc) and Lithuania (adoc) have gone the same route as Estonia. But unfortunately adoc, edoc and ddoc are not interoperable. In 2007, a compromise was struck as part of the work of the Baltic WPKI Forum – we would develop a new profile, called BDOC. Estonia has since adapted it into a national standard, but Latvia and Lithuania have not followed suit.

There is hope, however. In early 2012, the institution that maintains the XAdES standard, ETSI (European Telecommunication Standards Institute) unveiled a XAdeS profile at the behest of the European Commission[3] („Baseline Profile"), which limits options significantly. It is quite similar to the specifications of the BDOC. The container that joins files and digital signatures, ASiC[4], and its profile[5] have been standardized, and these are 99% compatible with our BDOC standard. These developments give reason to hope that we will make headway from national standards toward European ones and that digital interoperability will be achieved.

There is still a long way to go, though. And that goes for Estonia, too.

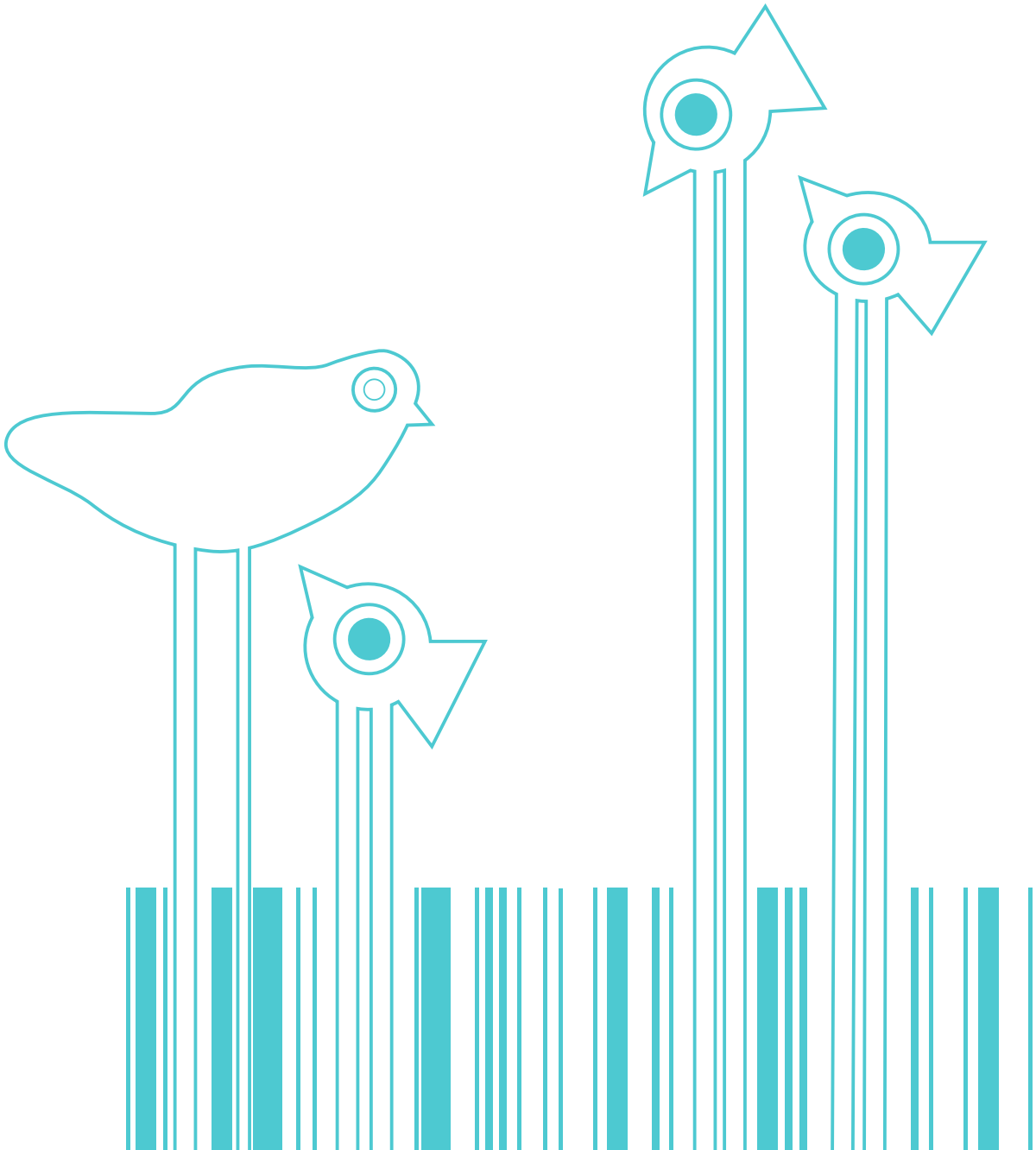
1 http://www.itif.org/publications/explaining-international-it-application-leadership-electronic-identification-systems

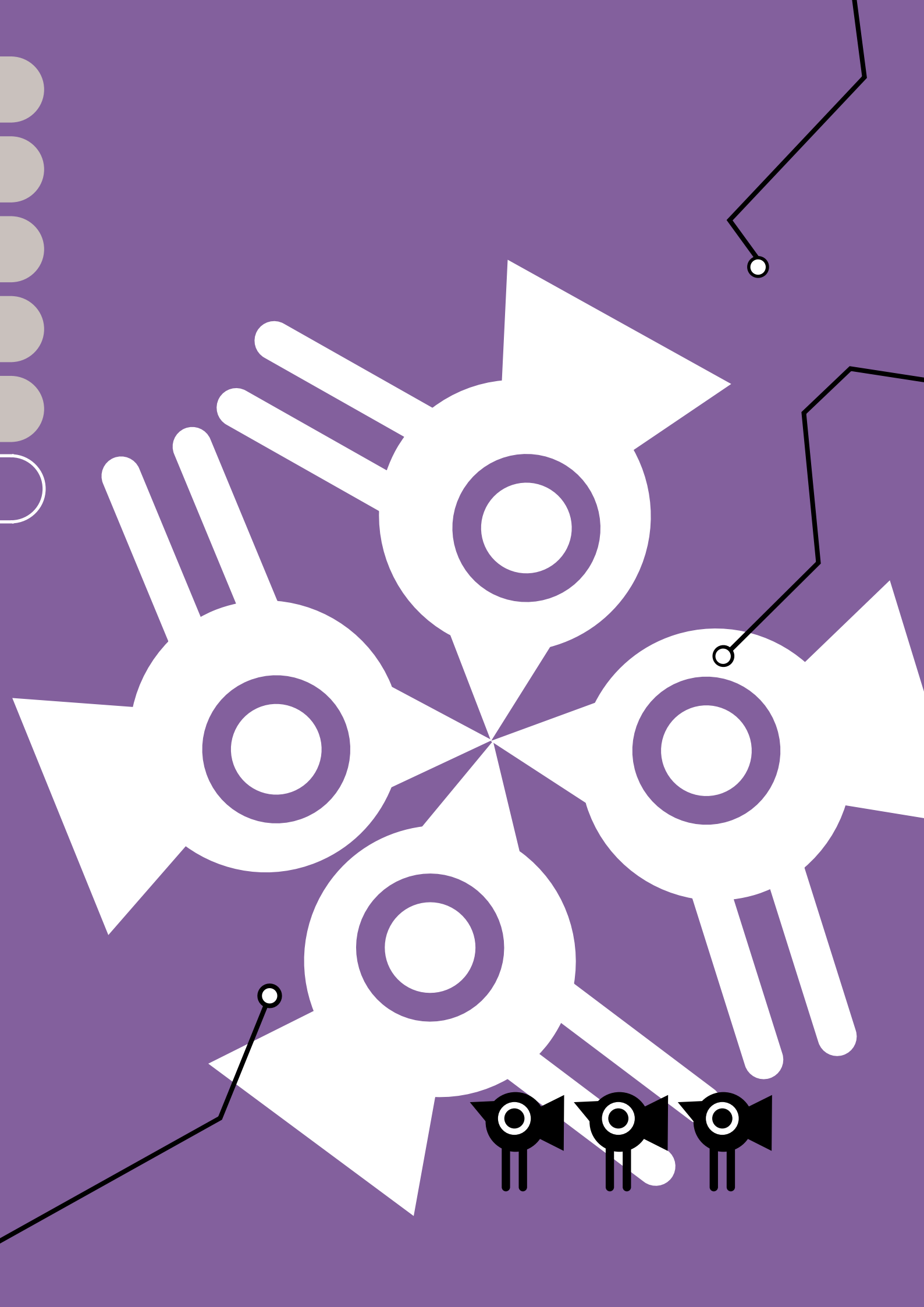
2 ETSI TS 101 903 - XML Advanced Electronic Signatures

3 ETSI TS 103 171 – XAdES Baseline Profile

4 ETSI TS 102 918 – Associated Signature Containers

5 ETSI TS 103 174 – AsiC Baseline Profile





CHAPTER 6
X-ROAD

2011 was an anniversary year for one of the cornerstones of the Estonian e-state and secure data exchange – the X-road. The X-road has reached its fifth version and over 100 databases have joined it. It is now used nearly a million times a day. The consistent development of the X-road has been covered many times in previous yearbooks and the opening article of this chapter takes a look at the entirety of the journey to this point. There is discussion of the experience with implementing the X-road in other countries, showing tellingly how important it is for state institutions to work together, use uniform standards and govern the principles of creating the state information system. You will also find articles that discuss the importance of ontologies and possibilities of using them both in the field of the e-state in general and in administering X-road services, as well as the innovative encoding services in version 5 of the X-road.

The first ten years of X-road

AHTO KALJA
ahto.kalja@ria.ee
Estonian Information System's Authority
Tallinn University of Technology

X-road version history

On 17 December 2011, X-road turned 10. Specifically, the first version of X-road was adopted on 17 December 2001 and was thereafter immediately ready for the first to join the X-road – both data providers and users. It didn't actually go that way immediately, as there were a few obstacles. The ID card had not yet been issued and the question of how to authenticate and authorize users was still open. By that time, commercial banks had working Internet bank solutions and the director of the Department of State Information Systems in Ministry of Economic Affairs and Communications at that time, Arvo Ott, held fruitful negotiations with the vice-presidents of major commercial banks. It was agreed that the banks would enable use of their customers' online banking code cards for authenticating the e-Government's services. The other concern was a bigger one. Namely, legislation on databases at that time contained a rule that if any task required data from more than one database at a time, a special licence from the Data Protection Inspectorate would have to be obtained to solve the task. This challenge was resolved as well, albeit only in October of that year. An amendment was introduced into the legislation: the X-road would be exempt from the special licence requirement.

Development of the *second version* of the X-road began the next year and it was completely finished by early 2003. The reason for the new development was the fact that in 2002, W3C made a new recommendation to adopt use of the SOAP protocol and thus it was reasonable for the X-road to immediately make the transition to that protocol and replace XML-RPC. Later practice showed that the old protocol, XML-RPC, would in fact remain in use for many years to come. It was abandoned only with the advent of X-road version 5. SOAP allowed parallel use of the WSDL description language and the service repository standard UDDI. These protocols are currently in worldwide use and thus timely transition saved a great deal on development funds, as it took place back when there were few services and the effort on redoing them was much less.

The *third version* of X-road was developed in 2003–2004. A string of new additions was made to the third version, which was occasioned by the needs of many new users. For instance, in connection with the fact that departments of the Tallinn city government (a total of 26 of them) joined X-road, it was a good idea to make use of their existing user administration system, built on the basis of MS Active Directory. The X-road standard portal Mini-Information-System-Portal (MISP) was furnished with a gateway, which allowed the MS Active Directory user administration solution to be utilized. A second major functional change in this version was the implementation of asynchronous queries – i.e. data transfers. By 2003, some Ministry of Justice courts' data transfers had become so high-volume that it was reasonable to handle these streams of hundreds of megabytes asynchronously. This version also included a number of

minor new features and expanded functions; for instance databases could be written to as well as read, etc.

The *fourth version* of X-road was developed in the period from 2005 to early 2006. The development was preceded by research into ways of increasing the security of data on the X-road and related applications. By 2005, pursuant to government regulation, all state institutions that used data exchange between information systems were required to join X-road and use its technology. It turned out that the security of the X-road in use at this time did not conform to the solution needed by institutions that handled state secrets and thus additional technologies had to be adopted for encrypting data. When the version was completed, ordinary citizens could organize their data processing (use of services) so that the service use logs were encrypted if necessary and the citizen could read his or her log using the key on the personal ID card. This version remained for many years the main version on the basis of which data exchange in large information systems (e-Health, Schengen information system, e-File etc) was structured.

The *fifth version* of X-road was developed in December 2009 - October 2010. This was for several reasons. The fourth version had been in use for more than four years and the daily number of services via X-road had risen by nearly an order of magnitude: from 13 million services in 2005 to 100 million services in 2009. The problem was not so much uptime and availability as the fact that many changes take place in IT development in the course of five years and they must be taken into consideration. For instance, the WSDL style RPC/Encoded was adopted for describing services in previous X-road versions, as most information systems used it. By 2009 the situation had changed and the primary style was now Document/Literal wrapped. For this reason, the style of the web service description language was switched. Another important component that had become obsolete was encryption algorithms. There was the risk that Chinese specialists could break a number of well-known encryption algorithms – the situation had to be pre-empted. That is why the encryption algorithms used on the X-road were changed. The technology was replaced by a new technology in the user interface as well. The current X-road Mini-Information-System-Portal version MISP2 uses the same technology to shape the user interface as the state portal eesti.ee – the Xforms technology. Yet another important functionality was added to version 5 of X-road: A number of ministries have, namely, started transitioning to use of data warehouses in data processing. This has led to a need to process personal data so that the fields from which the identity of the person can be unequivocally determined are redacted from the records (name fields, personal identification code, address, etc). It is simpler to redact these fields when transferring data from database to the data warehouse, replacing them with some code with no relation to the content. The encoding service built into version 5 of X-road supports such an operation. Naturally, five years is a long time in information technology and during this time very many inconveniences and minor problems emerge in a system that sees high use. Rectifying these problems was one of the tasks in developing version 5 of X-road.

Naturally, five years is a long time in information technology and during this time very many inconveniences and minor problems emerge in a system that sees high use. Rectifying these problems was one of the tasks in developing version 5 of X-road.

Primary characteristics of X-road

What are the primary properties and functionalities on which X-road is founded, which have resulted in its use reaching such stunning volumes – nearly a million use-instances per day?
First of all, *dispersed architecture.* When the X-road was designed, it was specified right at the outset that the solution had to be completely decentralized. Thus many of the same principles that govern the Internet had to be adopted: the system had to be as spread as out as possible in light of security requirements. Potential bottlenecks had to be avoided. For instance, many states have concentrated their databases at one »»

» point in terms of IT architecture, i.e. large computing centres. If something happens to that hub, all of the state's critical services will likely come to a halt. The X-road tried to nip such bottlenecks in the bud.

The X-road's service-based nature should also be highlighted. The entire functionality is service-based: the X-road offers a service-based solution for development of the state information system and use of data. X-road itself uses many metaservices that were structured as services. Ordinary users, too, are offered data processing solutions that are, again, services. Elementary and complex services are distinguished. Universally known service standards are used, e.g. SOAP, WSDL, SAWSDL, UDDI etc.

One of the main noteworthy X-road properties is high *availability*. Right from the beginning, developers and users have expressed concern regarding whether the data processing operations conducted throughout X-road are too slow and whether security servers form a bottleneck that take up much time. This is certainly not the case. On the contrary, one of the ideologies of X-road since the beginning has been *scalability.* In the case of secure servers, that means that if they have too little capacity in their information system's server, they can be replaced with a more productive server. If this does not help, many secure servers must be operated in parallel and the load can be distributed among them. Use of two parallel servers also constitutes an advantage in a situation where one device goes off line due to a chance error.

A number of other X-road properties can be noted, such as *saving logs* and *ensuring the verification value of the logs*, as well as *multilevel user authentication.*

X-road statistics, new directions, interest from other countries

In talking and writing about X-road, the statistics on the use of services has always been highlighted. Use statistics have risen as high as a million services a day and around 240 million services per year. The addition of new information systems among providers of X-road services and their users raises the number even higher.

What's next on the X-road? We are trying to develop more and more tools that would make it easier to develop new services, test service and monitor their use. One helpful resource for X-road is the Administration System for the State Information System (RIHA), which is used to join X-road and which has amassed a large number of descriptions of databases and e-services. Quality indicators of services will start to be saved here (time indicators, frequency of errors etc). Descriptions (such as ontologies of data objects) are useful in the sense that they are human-readable as well as the fact that they are machine-readable. Machine-readability guarantees that if we start putting together more complicated complex services from elementary services, then the mutual compatibility of service inputs and outputs can be automatically checked. This is a matter that sees much work in other countries and often the activity is called composition and orchestration of services. We definitely want to be in the vanguard when it comes to automatic composition of services and we launched collaborative work with researches from Institute of Cybernetics at Tallinn University of Technology in this field.

In closing, it must be said that X-road continues to generate interest among government information technology specialists and those responsible for developing information systems in other countries. Our development partners, the private companies Cybernetica AS and Aktors OÜ have developed an environment similar to X-road for Azerbaijan. Lately, Russian counterparts have familiarized themselves actively with X-road. Neighbours from Finland and Latvia have also visited us. There are frequent inquiries from European Union development projects, and they consult with us in regard to future development scenarios.

Ontologies and semantic annotation of X-road services

HELE-MAI HAAV
helemai@cs.ioc.ee
Institute of Cybernetics at Tallinn University of Technology

Nowadays, exchange of knowledge is no longer limited to people; software agents are also involved in the process. In this regard, ontologies (systems of concepts in a given domain) have become a common means of semantically formalizing knowledge. In this context, the e-government is no longer considered as a central web-portal where the government publishes information for citizens. Instead, it is viewed as an active environment for sharing knowledge and e-services, one of the parties to which may be a software agent.

In order to uniquely understand the data collected to databases of the state information system (IS), a common shared system of concepts – ontology – is needed. It is sufficient for a person if an IS data object has, besides a label, a textual description in a natural language they can understand, but a software agent requires some formal description to understand the label. For instance, ontologies can be formally described in OWL[1] (Ontology Web Language). For both humans and software agents to understand the meaning of data objects in the same way, descriptions of data objects must be enriched with so-called semantic descriptions – that is, references to the concepts used in a given ontology. The X-road data services use data objects of IS as input-output parameters of services. Enriching descriptions of X-road data services with semantic references to the components of the ontology of the relevant IS domain makes it possible to use software agents for maintaining X-road data services.

Possibilities of using ontologies in the Estonian e-government domain

Ontologies have many fields of use both in the domain of the e-government in general and in managing X-road services in particular. Some possible areas of use are as follows:

- Semantic search of information and services. Ontologies allow a common understanding to be gained regarding a field and make it possible to present it formally. It is also possible to use domain ontologies to link different informational structures (such as data objects from different ISs). Informational objects semantically enriched using ontologies (such as texts, images, descriptions of services, ISs' data etc) can be searched semantically. For example, there are semantic search engines Google, Bing etc that offer, for this purpose, the ontology on the schema.org site for annotating websites (e.g. using MicroFormats). The eesti.ee portal as well can be expanded »»

» with semantic searches, provided domain ontologies exist. Semantic search of semantically enriched X-road services and data objects has now been partially implemented at RIHA.

- Process design and implementation. Many X-road service providers may have a relatively similar portfolio of services. In the interests of the faster and higher-quality development of X-road services, it is good to re-use and share knowledge, and domain ontologies and descriptions of X-road services enriched by ontologies are a suitable means for this.
- Interoperability and composition of services. To faster develop new X-road services from existing ones, software that enables automatic or semiautomatic composition of complex services can be used. The prerequisite is semantically enriched description of X-road services. Ontologies can be applied to link open data, ensuring that linked open data is consistent.

The Semantic Interoperability Framework of State Information Systems[2] calls for development and adoption of semantic technologies in the near future. Under the semantic interoperability framework, every ministry is obliged to create and administer ontologies connected to their area of administration, domain vocabulary and semantic descriptions of web services related to them. The interoperability framework sets forth the use of OWL for describing ontologies and the use of SAWSDL[3] for semantically enriching X-road services' WSDL descriptions. Semantic interoperability based on state database services is a precondition (or the first stage) for the broader semantic interoperability treated in the framework.

Creating an ontology allows the domain's concepts to be dealt with systematically, creating a system of concepts, the related business process, and the relevant IS data structure.

The RIHA regulation[4] requires that, as part of the data processed in a database to be entered into its subregister of databases, a semantic description of the data object be presented in the form of a reference to the domain terminology (the relevant concept, relationship or attribute of the domain ontology). In addition to this, the semantic description of the service's inputs and outputs must also be presented as part of the services' data to be entered into the RIHA services subregister.

Status of domain ontologies in Estonia

As mentioned above, the semantic descriptions of X-road services require the existing of ISs' domain ontologies. Their availability makes possible the semantic description of X-road services and their use in any kind of application.

To create domain ontologies, a methodology for creating ontologies has been developed[5] along with requirements for ontologies to be published in RIHA[6].

Besides this, trainings of various durations on creation of ontologies and semantic descriptions of X-road services have been held in the last five years. In 2010–2011, trainings were held for six groups (each had up to 12 participants) from the domain of ISs at different ministries. These trainings differed from earlier ones as the purpose was to create a relevant domain ontology in practice and to use it to semantically enrich the relevant data structure and descriptions of X-road data service.

As a result of the training, 19 ontologies were created in 2010 and 13 in 2011. The main domains were related to the Centre of Registers and Information Systems, Population Register, Land Board, Ministry of Social Affairs, e-health and Estonian Agricultural Registers and Information Board. Ontologies that are strategically important from the point of view of annotating already-specified X-road data services include ontologies for Population Register, address data, spatial data and Business Register, the components of which cover about 80% of the current X-road data service input-output parameters.

Thirteen ontologies have now been published in RIHA. This shows that some ontologies created at trainings have not been completely finished and published. There are a number of reasons for this, but the principal one is that trainings

alone are not enough for completing the labour-intensive development of ontologies. As the priority of this activity is not high at workplaces, the development of ontologies tends to bog down after the training. This is a shame, of course, as it hinders their use in applications and sharing of knowledge. From the point of view of semantic description of X-road services, it is important that, besides the natural person ontology, the other three strategically important ontologies be ready in practice and published on RIHA. The natural person ontology is under construction.

In spite of the knowledge- and labour-intensive nature of ontology development, some beneficial angles can nevertheless be found from the point of view of the IS holder, developer and administrator:

- Creating an ontology allows the domain's concepts to be dealt with systematically, creating a system of concepts, the related business process, and the relevant IS data structure.
- A domain ontology allows the knowledge in the domain to be shared with experts, non-experts and software agents of other ISs.
- Ontological development is especially beneficial in planning ISs or updating old ones (in the analysis stage).

Nor should resources necessary for ontological development be underestimated in the context of ISs. In the long term, they will be undoubtedly worth it.

Semantic descriptions of X-road data services

A manual for semantic descriptions[7] has been developed, and this was also used in the above-mentioned trainings. All of the mentioned ontologies were used in the course of training for semantic description of either databases or X-road data services. Unfortunately, none of the semantically described X-road data service or data structure has been published on RIHA.

In the near future, however, the descriptions of the relevant X-road data services semantically described using the address data ontology should nevertheless become publicly available.

Conclusion

The e-government domain in Estonia is technically ready to apply semantic technologies, especially in the context of maintaining X-road data services. Currently complex data services are being developed on the X-road manually; however, if semantically described X-road services existed, it would be possible to partially automate the process. The automatic or semi-automatic development of X-road data services could be one possible application for e-government semantic assets in the public sector.

1 OWL, www.w3.org/TR/owl-guide

2 Riigi infosüsteemide semantilise koosvõime raamistik. (Semantic interoperability framework of state information systems) http://www.riso.ee/et/files/RISsemantikaV07-loplik.pdf. Versioon 0.7 (01.08.2007) (in Estonian)

3 SAWSDL, http://www.w3.org/TR/sawsdl/

4 Riigi infosüsteemi haldussüsteem. (Administration system for state information systems) https://www.riigiteataja.ee/akt/12933746?leiaKehtiv. Redaktsiooni jõustumise kuup.: 16.02.2009 (in Estonian)

5 H-M. Haav. Ontoloogiate loomise metoodika. (Methods of creating ontologies) Tallinn, 2010. http://ftp.ria.ee/pub/riha/metoodika.pdf (in Estonian)

6 H-M. Haav. Nõuded RIHA ontoloogiatele. (Requirements for RIHA ontologies) Tallinn, 2010. http://ftp.ria.ee/pub/riha/nouded.pdf (in Estonian)

7 P. Küngas. Semantilise kirjeldamise juhis. (Manual for semantic descriptions) Tallinn, 2010. http://ftp.ria.ee/pub/riha/Semantilise_kirjeldamise_juhis_v04.pdf (in Estonian)

Secure aggregation of databases

JAN WILLEMSON
janwil@cyber.ee
Cybernetica AS

Data are not collected for the sake of collecting them – usually there is a purpose and view to use them for providing some specific service. Often there is a need for data from more than one database and the X-road, which has been in use for around ten years in Estonia, is used as a convenient solution to this problem.

Once data have already been gathered, the benefits they generate can increase in the case of applications that were not even foreseen when the database was first established. The most typical example is research – a researcher can develop interest in data on the social field or health to study how various factors influence the state of the nation. Such databases can also generate benefits for state policy planning and other applications.

Two new problems come up here. For one thing, many databases were not amassed with research in mind, and that would be a case of use other than for the designated purpose. Secondly, many social and health databases contain delicate personal data that researchers have no right to access.

Fortunately the identity of specific individuals is not necessary for researchers, as they are mainly interested only in the statistical end result. But they do need to link the various databases according to individual. A standard means of doing this is a personal identification code. Unfortunately the identification code is in some sense too powerful, as besides the databases needed for a given study it allows data to be linked to other sources and this can lead to an extensive breach of privacy.

This necessitates a solution that would ensure a possibility of linking databases without opening universal identifiers (names, personal identification codes). One method for realizing such a solution is the use of pseudonyms, i.e. replacing personal identification codes with identifiers for onetime use used only to form a specific aggregate database.

Version 5 of X-road, which was implemented in early 2011, includes convenient pseudonymization means as a new tool. The so-called encoding service generates the necessary pseudonyms by encrypting personal identification codes and to do this the security service infrastructure already extant on the X-road is used. An encryption key is installed into each data source server used to form the aggregate database and the necessary fields that require pseudonyms are marked in the X-road query responses. The name of the person is deleted, the entries are integrated into a database on the basis of the encrypted personal identification codes, and the necessary statistical or political studies are performed on this basis.

Such a solution does not protect us against all the potential attacks. As other fields besides names and personal identification codes remain open, a malicious researcher could likely find out the identity of the individuals in some aggregate databases. This means that besides encoding service, other security measures must be used – for instance, researchers could be asked to justify their goals before the research is conducted and to describe the methods to the ethics committee. If the research is justified and there is no reason to fear misuse, X-road encoding service offers a convenient and effective way of forming secure databases.

Feasibility of the X-road in other countries

MONIKA OIT
monika.oit@cyber.ee
Cybernetica AS

ARNE ANSPER
arne.ansper@cyber.ee
Cybernetica AS

We are proud of Estonia's X-road environment and we would like to pitch it to other countries as a secure and economically reasonable solution for organizing communication between information systems. The following outlines our experiences, both negative and positive.

Prerequisites

X-road is a secure environment for exchanging messages and in principle nothing at all keeps it from being utilized in any country or community for information exchange between organizations. But to make full use of the strength and security properties of X-road, certain prerequisites do apply.

The existence of an organisation for coordinating **state information system** is a key prerequisite. X-road is the e-state's backbone and its administration requires a separate organizational structure that must keep a highly secure system operational and incite government institutions to engage in cooperation and use common standards. Yet often countries lack an inter- or transministerial trusted centre with a suitable capability. It would be reasonable for such an institution to be in place before implementation of X-road starts, because the local X-road centre should steer the project on the spot and direct activities already before the procurement process. Implementation of X-road requires solid public relations outreach on many levels; the success of the project depends largely on how deep into state institutions the vision of the usefulness of implementation of X-road has penetrated.

A second important precondition is the **existence of a capable local partner.** This is a well-known fact that local support is the key issue when implementing any system in another country. Talking about the X-road as the principal support system, the project partners must, besides having knowledge of the sector, be politically correct and capable of communicating at the level of very senior decision-makers. Proficiency »»

» in the local language is also very important. It is not always possible to find one partner with all these qualities, so there must be several.

Desires and opportunities

A number of countries have decided to implement an X-road – Palestine, Moldova and Serbia for example. They try to find the best solutions for common use of information systems. Such a desire occurs generally when specialists understand the unique functionality of X-road (a highly available integration environment that ensures unified verification value) and politicians find ways to implement X-road in their interests, and in order to make this wish materialize we need investors to also have a desire to provide funding for X-road. Politicians are attracted by citizen-oriented services that can be realized easily and specialists are enticed by the technological value of the X-road, yet no key has been found for persuading potential investors.

We are proud of Estonia's X-road environment and we would like to pitch it to other countries as a secure and economically reasonable solution for organizing communication between information systems.

Once decision-makers have reached the conclusion that it would be reasonable to follow an X-road type solution when developing e-state in their country, then a public procurement must generally be carried out to procure such a system. Good practice in the area of public procurements generally prevents a government from procuring the X-road per se, but rather it must purchase a secure information exchange environment, with the specifications of the object of the procurement written so that they are very similar to the X-road. But if an "information exchange environment" is procured, actually a number of major corporations offer solutions under such a designation – these being companies armed with corporate sales subsidies for entering the market, or support from their own country's government in the form of export support, development assistance or other such label. And governments will mostly favour the economically most cost-effective offer, regardless of how suitable it is for the requirements. Major companies see such systems as strategic investments and are prepared to do all they can to win such tenders.

In state system procurements it is also typical that there is a desire to make the procurement as large and all-encompassing as possible: certainly it has to include much hardware and other useful-seeming aspects because if a commitment has already been made to finance a development of a system, then an attempt will be made to procure everything that will add scope to the system – after all, there is no certainty as to when it might be possible to do so again. Expanding the scope in this manner engenders unhealthy interest in insignificant details while the topics that are actually important (such as building an organisation for system administration in the case of X-road) are given short shrift. And thus the hardware side tends to dictate things – if a supplier turns up who plans to recoup its initial investment by offering the contracting authority service plans and future upgrades, they can bundle a software component with their hardware. And again, this is generally seen by governments as an irresistible opportunity.

Fortunately there are positive examples in addition to many unsuccessful procurements. Our experience from Azerbaijan's e-state development project, for example, is such an example: here a secure information exchange environment based on X-road technology was set up and implemented as one component of the project.

Particularities of the X-road implementation process

Much PR and explanatory work needed

After the contract for implementation of X-road is awarded, actually the next sales iteration begins. And as in every other case where implementation of a new information system significantly changes processes and habits, it initially meets with great opposition. The principles of X-road are very hard to accept, as effective implementation requires multiple organizations to make coordinated changes to their business processes. As state information systems are

mainly structured from the point of view of ministries, thus amendment proposals must be very skilfully justified and come from a very high level if they are to be considered at all.

It should be mentioned that the decentralized nature of X-road, the fact that data are dispersed and that control over access remains in the hands of the same owners add up to an important argument for persuading reluctant ministries. This simple solution is so innovative and surprising that communicating it takes much time and effort. Once the idea gets across, the rest comes easier.

In truth, in Estonia X-road was pushed through by force – i.e. by government regulation that required all data in state databases to be used through X-road. There is no point in assuming that it could go differently in some other country. For that reason, implementation of X-road must be supported by some suitable legal act that makes the use of the system obligatory for state institutions. Considering the slow speed at which legal acts are deliberated, the creation of such a regulation, directive or other legal act must be launched to coincide with the beginning of the implementation project. It took about a year for the relevant ukase in Azerbaijan to go from draft to law and it required very solid lobbying work.

If it turns out that no general principles have been set forth for creating state information systems, it would be wise to immediately propose such draft legal acts.

Actual situation as regards support systems

Another topic that has to be launched immediately is determining the actual state of local support systems. Naturally it would be good if there were a clear picture before the X-road implementation tender were made; otherwise there might be an inadequate estimate of the amount of additional efforts needed to integrate existing systems or finding alternatives to them. Unfortunately such information is not necessarily accessible before contractual relations. In the case of Azerbaijan, we knew that everyone in the country had a personal identification code. But it turned out that the status of the national personal identification code and implementation mechanisms were not agreed upon, and that there were more than one encoding system for identifying persons, and that these were not interlinked. It was also known that companies had "commercial register" codes but it unfortunately turned out that they were the Ministry of Taxation taxpayer codes and not related to companies' right of signature but rather with the accountants who remitted tax payments. This experience suggests a bold conjecture: that the Estonian scenario with one personal identification code and one Business Register code is superb and this has saved millions for the state. It is very hard to integrate systems if there are no ways to link data on persons and persons/companies.

In any case, the preconditions laid down for support systems should be checked as early as possible; information should be obtained from different sources and different levels, right down to the technical details. There will be situations where in the opinion of management a certain service is functional but the information from specialists indicates otherwise. A situation must be achieved where all parties have an identical understanding of functionalities.

Local administrative team

As implementation of X-road requires an administrative structure to be created as well and fairly large-scale knowledge transfer, the topic of personnel is also important. The lesson we learned is that building the local team and establishing a solid level of know-how for the team is the most important criterion for successful system launch. Don't assume that suitably qualified people have been trained or are waiting on reserve for the project. Assume you will have to build the admin team yourself. Training should be started from a basic level and certainly people and organizations cannot be expected to have the level of knowledge and capability that is considered standard in Estonian conditions.

Provision of service

To be able to provide X-road services in other countries similarly to Estonia, general principles for creating databases should be in place. What data are gathered, in what way, and who is responsible for their integrity and authenticity, how can information be obtained on existing data to keep from doubling databases etc. In Estonia, the Databases Act originally governed the field; now these topics have been integrated into the Public Information Act. There are no such laws in Azerbaijan; the state's basic registers have not been defined, nor have supporting systems. There is no official system of classifiers and the basic principles of the land »»

» cadastre are likewise not agreed upon. Nor is there an address data system.

Use of services

The basic idea behind X-road is that automatic queries can be made between the state's information systems. Yet it is clear that these services will not immediately take shape as they require several parties to be prepared. First of all, some kinds of data viewing services can be offered instead. In Estonia, the primary service in X-road portal was, after all, data viewing; the more powerful services came later. The first serious users of X-road and its possibilities were the Police and Border Guard systems.

In Azerbaijan, people are very interested in the kind of information the state gathers on them. Social Insurance Fund information is considered of particular interest, as a person's pension depends on the sums that the employer has transferred to their pension account – and the only way to find out is to go to an office in person and ask. The Social Insurance Fund's information system is a completely modern electronic register and the registrar is prepared to provide the service electronically once the personal identification code issue is resolved. As the first services that is functional in practice, people can query names and addresses of individuals by phone number and the vice versa (the telephone network is national and administered by the Ministry of Communications and IT). The service is said to have users as well.

But it is possible!

To sum up, X-road technology can be implemented in other countries, but it is a relatively difficult task. Not so much technically – although key security improvements were made in Azerbaijan due to their stricter digital signatures act – as, in particular, organizationally and politically difficult: it requires cooperation between many organizations and can mean changes to business processes at state institutions. As all of it has to be completed in the framework of the implementation project, it should be considered a sizeable challenge for the project staff.

Statistical overview 2011–2012

Statistics on use of information and communication technology by Estonian individuals and enterprises is gathered every year in European Union countries on the basis of a unified methodology. In addition to gathering basic data, various themes are also in the focus.

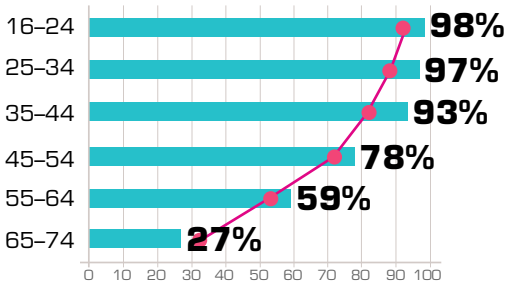
2011:
- the e-skills of individuals aged 16-74
- ICT possibilities that can be used in enterprises for environmental conservation

2012:
- use of mobile Internet among individuals
- enterprises' use of online retail opportunities

The use of IT by individuals aged 16-74 and households has been studied by Statistics Estonia as an annex to the Labour Force Survey starting in 2005, and the use of information technology among enterprises has been studied since 2001[1]. The sample includes 3,100 enterprises and over 4,000 Estonian individuals.

Share of individuals aged 16–74 who use the Internet

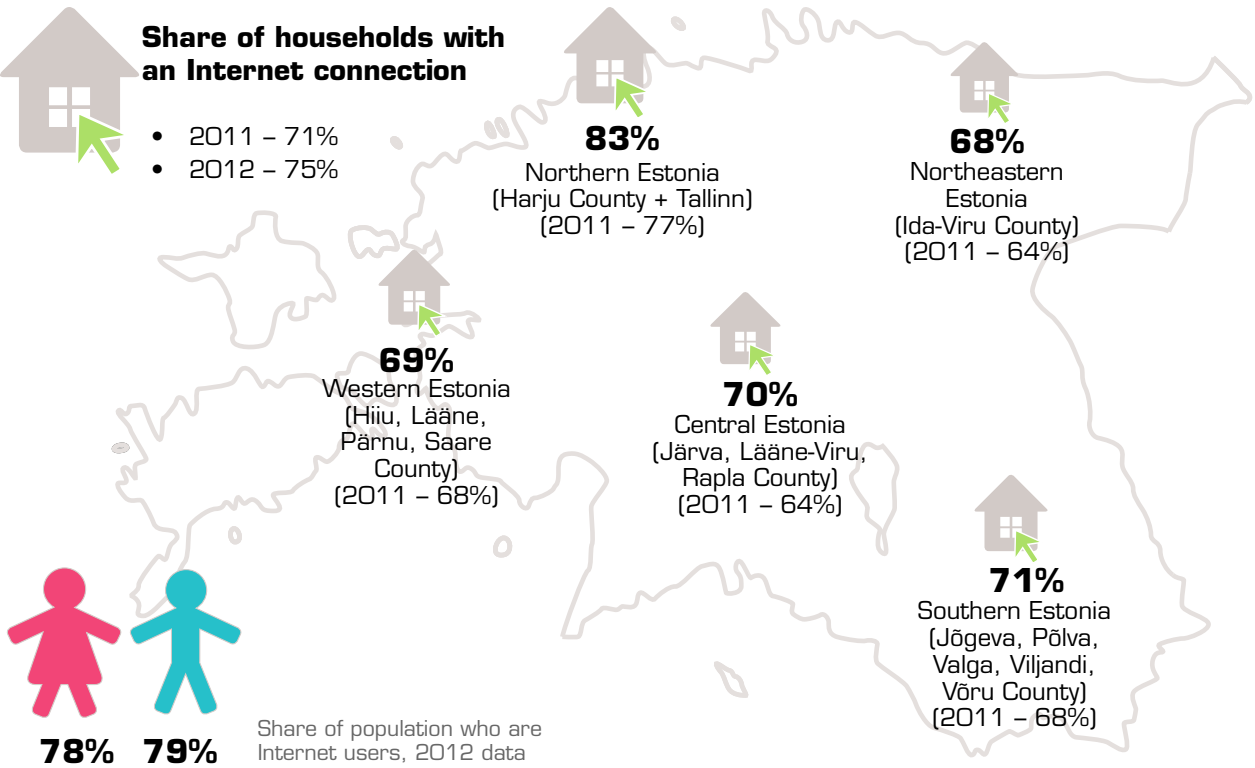
- 2011 – 77%
- 2012 – 78%



Share of Internet users by age group in Estonia, according to 2012 data, compared to EU average

Share of households with an Internet connection

- 2011 – 71%
- 2012 – 75%



Share of population who are Internet users, 2012 data

ICT usage in households and by individuals

Objectives of using the Internet

Estonian Internet users use online environments for many activities but the most important ones are communication, information searches, entertainment, and online banking. The most popular activities online in 2012 were undoubtedly reading newspapers and magazines (91% of Internet users; growth of 3 percentage points compared to 2011), sending and receiving e-mail (90%).

Finding information about goods and services have also seen significant growth. In 2011, 71% of Internet users used this option, but in 2012, the figure was 89%. But not all information searches lead to online shopping. Only 30% of Internet users used the Internet for purchasing goods or services, females did so somewhat more frequently than men. Purchases of concert, cinema, theatre tickets and the like make up the most significant category of online purchases (48% of all online shopping). Over 40% of all purchases of travel arrangements and holiday accommodation services and clothing and sports goods are made online. The Internet is used less for buying books, magazines and e-learning materials (24% of all online purchases). The supply of goods and services from individuals is also growing: in 2012, the Internet was used by 17% of Internet users for selling goods and services and online auctions. The year before it was 14%.

The use of Internet banking stands out in particular. Compared to 2011, the number of users here has remained stable: about 639,000 users, which is about 90% of all Internet users. In Europe, the countries that lead Estonia in use of Internet banking are primarily in Scandinavia – Norway, Iceland, Finland, Sweden, Denmark, where close to 80% of the population aged 16-74 are Internet bank users.

The Internet plays a very major role in satisfying people's **communication needs**. As mentioned, most Internet users (90%) send or receive e-mails. People have started using the Internet more actively for telephoning over the Internet and for video calls over the Internet. In 2011, 50% of Internet users used this option, and the figure had grown by 8 percentage points in 2012. People are also interested in participating in social networks (49% of Internet users in 2011) and posting messages to chat sites, blogs, newsgroups or online discussion forums (56% of Internet users in 2012).

Estonian Internet users are also fond of the entertainment opportunities offered online. Over half of them (56%) have played online games or downloaded images, films or music. Close to one-half (49% in 2012) of Internet users have listened to online radio or watched online TV. They have also been relatively active in uploading self-created content (text, photos, music, videos, software etc) to any website to be shared (40% of Internet users in 2012). Fewer have created their own website or blog (12% in 2012).

The Internet is used to a somewhat lesser extent for learning and work. Over one-half of Internet users have consulted Wiki pages (54% 2011), while only 7.8% (2011) said they had taken part in online courses. Over one-third of Internet users have used the net for looking for a job or sending a job application (33% 2011) and compared to ordinary social networks, the rate of participation in professional networks is still low, only 17% (2011) of Internet users.

The use of the opportunities offered by **e-democracy** was also studied separately in 2011. A total of 23% of Internet users said they had read websites on civic or political issues and posted such

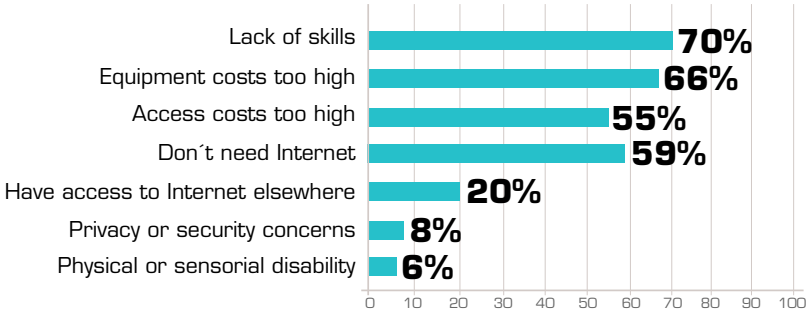


Figure1. Reasons for not having Access to the Internet at home (based on 2012 data) – share of households without Internet »»

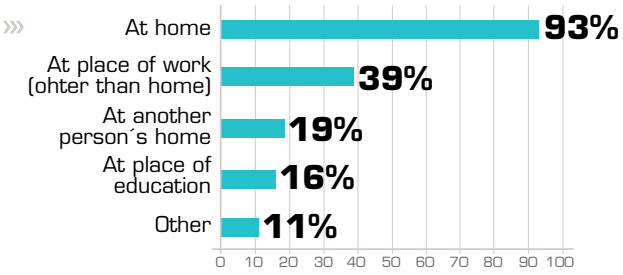


Figure 2.
Place where Internet is used, share among Internet users based on 2011 data

entries themselves. Eleven per cent have been more active, having taken part in online consultations or voting to define civic or political issues. Finns are the most active users of e-democracy opportunities in Europe – 43% of them say they read and posted on civic or political topics on the Web.

Starting in 2011, at the behest of the Ministry of Economic Affairs and Communications, Statistics Estonia also asks the Estonian population about **awareness of, use of and satisfaction with online public services**. Only slightly over 1% (2011, 2012) of Internet users say they do not know any online services offered by public sector institutions.

Internet users most frequently profess awareness and use of e-services that are needed regularly. The income tax return is filed through the e-Tax Board by 71% (2012) of Internet users and this percentage has grown compared to the previous year. They also know of digital prescriptions – compared to 2011, its use has grown by 13 percentage points (49% of Internet users in 2011 and 62% in 2012). Over half of Internet users use the option of paying for online services or state fees by using an Internet bank. Awareness and use of the state portal eesti.ee is gradually growing. In 2012, 47% of Internet users have used the possibilities afforded by this portal.

There are also many online services that are known about but not used. For instance, in the context of the 2011 parliamentary elections, 66% of Internet users said they know of the possibilities of voting online. And a two-year comparison shows that the people are aware of the online service for applying for ID documents (2012: 64%), the Unemployment Insurance Fund`s self-service portal (2012: 62%), the option of registration for state examinations (2012: 61%) and the options for submission of admissions documents (SAIS) (2012: 57%), but they had not had to use them.

Satisfaction with public sector institutions' online services is high. In 2011, 78% of people who are aware of electronic services were somewhat or very satisfied with public sector e-services. In 2012 the number of satisfied users had risen to 81% but the number of very satisfied users decreased somewhat.

Computer and Internet user skills among those aged 16-74

In 2011, more detailed data was gathered regarding individuals' computer and Internet literacy as in addition to Internet access it is increasingly important to know what people do online. It was studied how the computer and Internet use skills were obtained, what people can do with computers and Internet and how good they judge their skills.

Today there are many possibilities for **obtaining** computer and Internet **skills**. While the younger age group (16-34-year-olds) frequently learned their computer and Internet skills at formal education institution, very often they have mastered the skill in the course of actually performing the activity. Eighty-nine per cent of Estonia's 16-24-year-olds say they acquired their computer and Internet skills at school. In addition, of all Estonian individuals aged 16-74, 72% say they learned in the course of doing – this is most common in the youngest age group. Learning by doing is also popular in the Nordics: this is the case in Norway for 89%, in Sweden for 88%, and in Finland for 83% of all those age 16-74. People often use informal assistance from their colleagues, relatives and friends to acquire new e-skills and again, this is the case in the youngest age group for 90%.

People attend computer and Internet training course on their own or on the demand of the employer to a much lesser degree. Only 13% of all 16-74-year-olds have attended training courses at their own initiative. That is less than 45-55-year-olds (22%) and 35-44-year-olds (18%). Yet it should be mentioned that attending training at one's own initiative is not very popular anywhere in Europe. The most active individuals are in Germany (32%), Austria (21%), but the number in

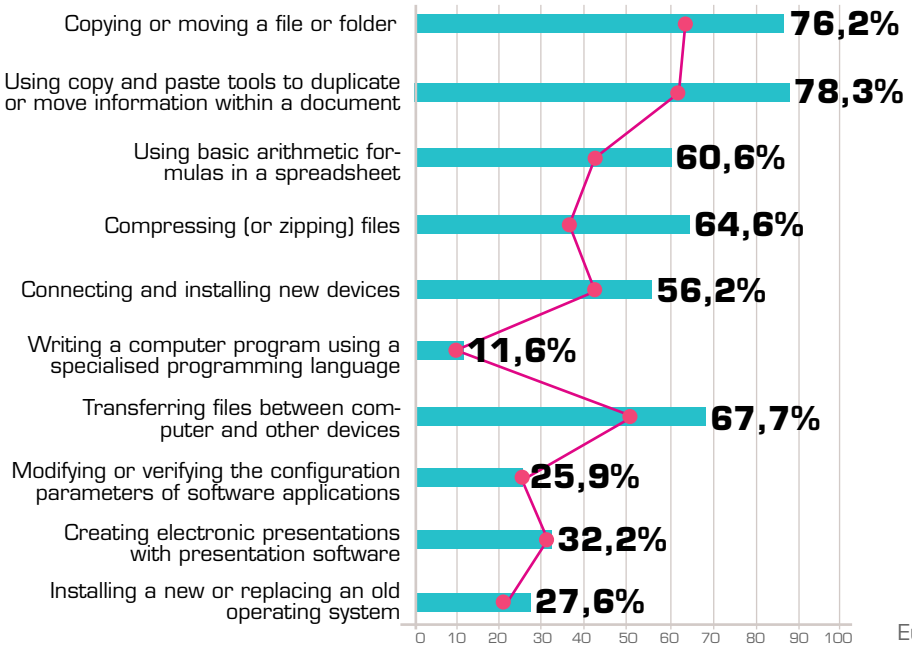


Figure 3. Estonian idividuals' computer-related activities compared to the average for the European Union (EU 27)

Finland and Sweden is only 18% of all 16-74-year-old individuals. But the difference with the Nordics is clearly visible in terms of attending IT courses on the demand of the employer in Estonia. Whereas just 12% of individuals aged 16-74 acquired their computer and online literacy skills attending vocational training courses at their employer's initiative, the respective figures are 44% in Sweden, 34% in Norway and 33% in Finland. Of Sweden's individuals aged 45-64, 60% say they acquired their computer and Internet use skills in precisely such a manner. In Estonia, 16% of individuals in this age group acquired their computer and Internet skills in this way.

The main reason for **not attending computer user courses** is sufficient skills – 35% of those 16-74 years of age in Estonia cite this as the reason. Over half of those 24-34 years of age judge their skills as sufficient but those younger or up to 44 years of age are not much less confident in their abilities. It can be noted here that 54% of Estonia's 16-74-year-olds judge their computer skills sufficient to find a new job within a year, if they needed to do so. And 41% of those 16-74 years of age judge their skills sufficient to protect their personal computer against private computer from virus or other computer infection and 48% judge their skills sufficient to protect their personal data. It is those 16-34 who are more self-confident.

People judge their computer and Internet skills best in regard to communicating with relatives, friends and colleagues over the Internet. Only 5% of all those 16-74 years of age consider their skills insufficient in this regard. Those 16-24 years old are the most confident (98%) followed by those 25-34 years of age (95%). Even 20% of those 65-74 years of age consider this one of their skills sufficient, although it is under the ratings among the same age group in Sweden – 60%. It must of course be considered that 25% of this age group uses the Internet in Estonia, compared to 65% in Sweden.

One reason that people do not attend IT courses in Estonia that is noteworthy at the European level is the fact that people attribute the reason to rarely use of computers and, therefore, absence of a need. Eighteen per cent of Estonian individuals 16-74 years of age cite infrequent computer use as the reason for not attending IT courses. Only Slovenia has a higher figure and the reason is also seen in different age groups.

The reason for not participating in courses can also be a desire to learn independently from others. In the age group 35-44, Estonian individuals are Europe's keenest self-learners (65% of all individuals in this age group) followed by Norway (65%) and Latvia (62%). In older age groups, Estonian individuals have a lower desire to be self-taught – the figure was 47% for those between the age of 45 and 54 and only 20% among those 65-74 years of age.

Mobile use of Internet

Use of the mobile Internet is slowly making inroads in everyday life. In 2012, more thorough »»

» study was devoted to the mobile Internet use habits and problems of the population between the ages of 16-74. Mobile Internet refers to use of the mobile phone network or wireless network (e.g. Wi-Fi) over a laptop or tablet computer, or cell phone, including smartphone models. Mobile Internet is used most actively (40% of mobile Internet users) and above all by non-working (university) students, and equally by women and men. The preferred means is Wi-Fi (27%) with mobile phone operators' networks being 9 percentage points less. There are more men and people aged 16-24 among the daily or almost daily users of mobile Internet.

People make nearly equal use of mobile communications and Wi-Fi over mobile phone/smartphones (17% and 15% respectively). While in the case of use of mobile Internet over a laptop, less frequent use (less than once a week) is predominant, daily or almost daily use is predominant in the case of use of Internet over mobile and smartphones. The primary users are men and the use is equal among the 16-24 and 35-44 age groups. Women and those 25-33 years of age use the Internet over mobile or smartphone less than once a week.

The share of mobile Internet users via tablet computers was 7% of all mobile Internet users in 2012. Men and women are nearly equally distributed: males 8%, women 6%.

Non-users of mobile Internet cite as the primary reason the lack of a need. Ninety per cent of women who do not use mobile Internet say they have no need to use the Internet outside home and work. The 35-54 age group also cited this reason most often. To a much lesser extent, other problems are cited, such as the cost of equipment and/or connection (36% of non-users) – people who say they are non-users for this reason are, namely, price conscious: the unemployed, pensioners, and non-working students. Older age groups cite more frequently such problems as the discomfort of using a small screen on a handheld device, ability to use or too complicated use and concerns about security and privacy.

The biggest problem for users of mobile Internet is constant difficulties with mobile phone network signal (22% of all mobile Internet users). A little over 10% of users cite problems with a small screen on a handheld device, difficulties in setting or changing parameters for internet access and unexpectedly large invoices. It is above all the 16-24 age group that is concerned about the last issue.

The mobile Internet is used above all for sending and receiving e-mail (76% of mobile Internet users), for reading newspapers and magazines etc (63%) and participating in social networks (59%). The activities of younger age groups also include playing games, and downloading images, films and music etc (a total of 48% mobile Internet users) and receiving audio and video files via podcasts (24%). Primarily the 16-24 age group and non-working students read and download online or e-books. Very often people access the Internet using a handheld device for performing job duties. Eighty-two per cent of employed Internet users used Internet via handheld device for performing job duties.

ICT usage in enterprises

Statistics Estonia studies use of information technology as of 2001. They study both general computer and Internet use trends, use of the Internet to interact with the public authorities and making internal corporate processes more efficient using IT means. The Statistics Estonia sample includes enterprises with 10 or more employees.

Estonia's most wired and computerized enterprises are those with more than 250 employees, where all have computers and Internet connection. But the share of computers and Internet connection among the smallest enterprises included in the sample, those with 10-19 employees, is also over 90%.

One-third of Estonian enterprises have not yet discovered the importance of having a company **website**. Most of the large enterprises (over 250 employees) have a website, but of smaller enterprises 66% have a website. Websites are most often used for displaying product catalogues and price lists (70% of enterprises with

websites), but under 20% of enterprises with websites offer online shopping, ordering or booking possibilities. In even fewer cases (10% of enterprises with websites) the client can track the order online. Close to one-quarter of enterprises use their website to provide advertisements of open job positions or online job application.

Close to 20% of enterprises had an account in a **social network** as of January 2012. Use of social networks is common among larger enterprises, but there are also examples of enterprises in the fields of education, art, entertainment, recreation and leisure, information and communications as well as lodging and food services. Over one-half of such enterprises had a social network account.

In addition to a website, Customer Relations Management software (CRM) and Enterprise Resource Planning software (ERP) are more common among larger enterprises. Over the years, the popularity of such software programs has grown a couple percentage points each year. Over one-half of large enterprises use ERP software (53%) and 40% use CRM software.

To make companies' activities more effective, one possibility is to use automatic data exchange within the company as well as in communicating with external partners.

To make enterprises' activities more effective, one possibility is to use **electronic data interchange (EDI)** within the enterprises as well as in communicating with external partners. In such a system, notices (such as orders, invoices, payment transactions or descriptions of goods) are exchanged over the Internet or other computer networks in a format that enables automatic processing, without the individual message being typed manually. An average of 37% of enterprises used electronic data interchange options in both 2011 and 2012. The most frequent EDI partners are the public authorities. One-third of enterprises have received from or sent to the public authorities data (tax refunds, statistical data, import or export declarations etc). Less than one-quarter of enterprises have used EDI for sending or receiving product information (catalogues, price lists). Sending and receiving waybills and sending payment instructions to financial institutions are less common.

Automatic share of information within the enterprise means sharing information electronically and automatically between different functions of the enterprise who using one single software application, common database or data warehouse or data linking between the software applications. Both the 2011 and 2012 enterprise questionnaire gauged access of the inventories management unit, accounting department, production or customer service and distribution unit to electronic and automatic information on orders and purchase orders. Accounting departments most frequently have access to such information via automatic share of information (36% of computer-using enterprises). An average of one-quarter of computer-using enterprises have created access to information via automatic share of information for other enterprise units as well.

In 2011, the **use of open source software** in Estonian enterprises was studied more closely. Open source Internet browser software are used most frequently (71% of computer-using enterprises), but half of enterprises prefer to use open source office software. Major enterprises make the least use of open source office software and enterprises with 20-49 employees make the most use of open source software. To somewhat lesser extent, enterprises use open source operating systems (23% of computer-using enterprises), open source web servers (17%) and open source ERP or CRM applications for business process automation.

Use of **ID cards** in enterprises shows a constant increase. Whereas in 2010, 67% of enterprises had used an ID card, the figure in 2012 had already grown to 91%. Just as predominant was the use of ID cards for digital signatures – in 2012, 89% of enterprises did so and over one-half of enterprises (67%) used ID cards for establishing users in information systems.

The use of **public sector information** for commercial purposes is seen as in increasingly major source of economic growth. Still, about 10% of enterprises make significant use of public sector information for commercial purposes. At the »»

» same time, about one-third of enterprises do not see a possibility of using such data for commercial purposes. Above all, small enterprises with 10-19 employees are sceptical. Awareness of the possibilities of commercial use of public sector information has grown slightly over the year: whereas in 2011 close to 14% of enterprises said they do not know of such a possibility, in 2012, 12% of enterprises with an Internet connection said they did not know of it.

Another important trend is the use of information and communication technology for environmental conservation. In 2011, the **environmental conservation activities** of computer using enterprises were studied**.** The greatest number of enterprises (68% of computer using enterprises) have tried to reduce use of paper for printing and copying. But to a similar degree, personal attendance and travel have been supplanted with use of telephone, web or video conferencing. Over one-half of enterprises (59%) has considered reducing energy consumption of information and technological equipment by using, for instance, turning off computers and screens, use of automated power down devices for the ICT equipment or multi-function peripheral imaging devices (printers, scanners, photocopiers) etc. Employees are also offered remote access to company e-mail, documents and applications. Adherence to environmental conservation principles is most common among larger enterprises where the effect is also probably greater.

Estonian enterprises' **satisfaction with public sector e-services** has remained high over the years and continued to be high in 2011 and 2012. Only 4% of enterprises that used public sector e-services were not satisfied with the services. The share of enterprises that were very satisfied with public sector online services rose in 2012 to 22%. Nearly all enterprises with Internet connections and 10 or more employees use public sector e-services.

Besides individuals, possibilities for mobile Internet use also have an impact on enterprises. Nearly half (48%) of Estonian enterprises (including 80% of enterprises with 250 employees) have offered their employees **equipment that enable mobile use of Internet** (mobile telephone, smartphone, laptop etc). For fulfilling work duties, employees are mainly offered laptop or tablet computers. These devices are mainly used for accessing e-mail systems (87%) or public information on the Internet (86%), and to a lesser degree for accessing and modifying company documents (57%).

The greatest reason for non-use of mobile Internet is lack of need to do so (16% of enterprises with an Internet connection), where enterprises with 50-99 employees felt the least need for mobile Internet. Problems with the mobile phone network Internet connection itself (12%) were an obstacle, as were technical difficulties or high costs of integrating mobile Internet connection with business software (9%). Obstacles also cited include potential security risks (8%) or lack of knowledge and skills, contractual barriers or employees difficulty becoming accustomed to new work methods (7%). High costs for the subscription or use of the Internet are a problem for 7% of enterprises with an Internet connection.

Use of e-Commerce is still fairly uncommon among Estonian enterprises. An **e-Commerce transaction** is the sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. Sales from the company's online store or website (web sales) may be used as well as via electronic data interchange (EDI[2]; EDI-type sales). E-Commerce transactions exclude orders made by manually typed e-mail messages. In 2010 and 2011, only 12% of computer using enterprises sold their goods or services online or using EDI. Use of these channels for buying was even less common – 8%. Estonia was the primary market for purchase and sale (9% of enterprises). Under 3% of Estonian enterprises sell to other European Union member states and elsewhere in the world.

1 http://www.stat.ee/57584 (in Estonian)

2 EDI – *electronic data interchange*. It is used here as a general term for sending business information in a form that enables automatic processing.