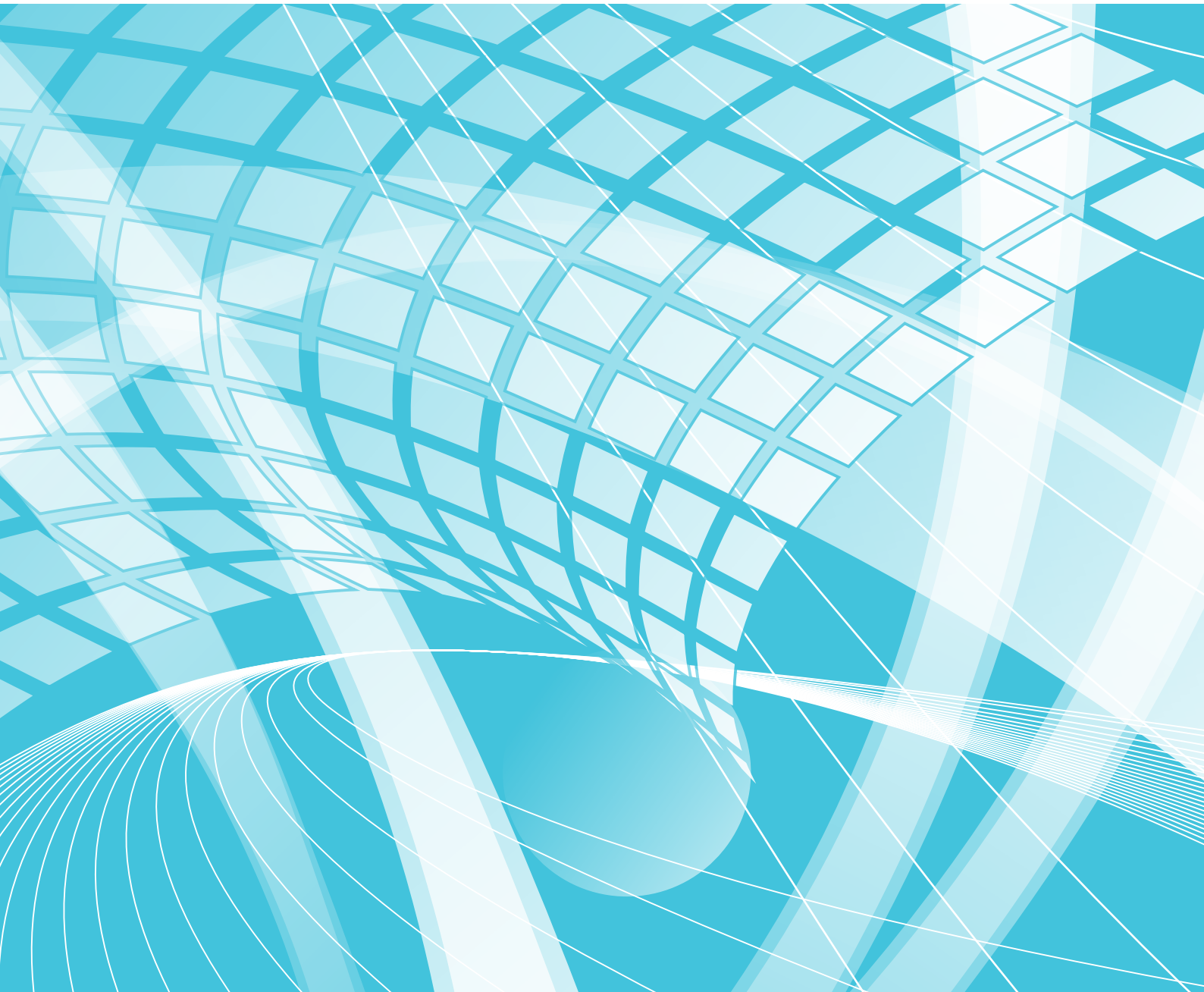
INFORMATION TECHNOLOGY IN PUBLIC ADMINISTRATION OF ESTONIA

YEARBOOK 2007



MINISTRY OF
ECONOMIC AFFAIRS AND
COMMUNICATIONS

Department of State Information Systems

Information Technology
in Public Administration of Estonia

Yearbook 2007

TALLINN 2008

Compiled and edited by Ivar Odrats

Translated by Karin Rits and Kadri Põdra

Design by Katrin Põdra
Illustrations by Katrin Põdra
Printed by Vali Press OÜ

ISSN 1406-5010

Co-authors of the yearbook:

Hannes Astok – *Member of the Riigikogu;*

Katrin Edasi, Mait Heidelberg, Ivar Odrats, Monika Saarmann and Uuno Vallner – *Ministry of Economic Affairs and Communications;*

Hille Hinsberg and Kädi Riismaa – *State Chancellery;*

Epp Maaten – *Member of the Estonian National Electoral Committee;*

Lauri Leht and Tõnis Türna – *National Archives of Estonia;*

Reet Oorn, Rica Semjonova and Toomas Viira – *Estonian Informatics Centre;*

Gerli Hämmal and Ingmar Vali – *Centre of Registers and Information Systems;*

prof. Ahto Kalja and prof. Jaak Tepandi – *Tallinn Technical University.*

Acknowledgements:

The compiler would like to thank the following co-authors of the Estonian edition of the yearbook 2007 for the opportunity to use their articles and data in preparing this yearbook:

Katrin Hänni (Ch.6), Egert Ivask (Ch.4.1), Riina Kivi (Ch.2.7), Vaho Klaamann (Ch.6), Tarvi Martens (Ch.2.8), Väino Olev (Ch. 4.7), Mai-Liis Palginõmm (Ch.6), Mart Parve (Ch.3.2), Geroli Peedu (Ch.4.1), Risto Pomerants (Ch. 4.7), Mari Roots (Ch. 4.7), Monika Saarmann (Ch.6) and Rauno Temmer (Ch.4.1).

The compiler is also thankful to Ms Karin Rits for her comments and suggestions on the yearbook.

Contents

1. Policy formulation in the field of information society in Estonia

1.1. Climbing the e-mountain

Estonia has no real mountains. Our highest top is, in reality, a small, though cute hill. Maybe it is the lack of higher grounds in nature that makes our people look for higher levels and achievements in other areas.

There are some simple things that need to be kept in mind both when climbing a mountain and wishing to move forward in the development of the information society. Namely, we have to ensure that everybody involved is with us, safety rules are followed and we make use of all the best equipment and techniques available to us. And, of course, we'd better have some kind of a plan on how to complete the task.

Year 2007 was, in some sense, a milestone in terms of creating possibilities for all to participate in the information society. Today we can say that high bandwidth Internet services are available all over the country. Public money was used to stimulate service provision in remote and sparsely populated areas. Service providers used the opportunity to make infrastructure investments in regions, where it normally is not economically wise. New market areas were created and today we can see competition even in places, where broadband Internet was not available at all just a couple of years ago.

In 2001-2002 there were heated discussions about the planned ID card for citizens. Should it be electronic or not, would everybody need the electronic functions of the ID card or should there be different options? It was decided that there would be one type of an electronic ID card for everybody. Now, five years later, most people have the ID card. Although not everybody uses the electronic functions of the card now, they still have the possibility to do this once they so decide. A number of different services requiring electronic identity have already been developed and there are many more yet to be created. The wide spread of electronic ID has enabled us to introduce services like voting over the Internet, etc. When the new Parliament was elected at the beginning of 2007, more than 5% of voters preferred to cast their vote electronically. The percentage as such might not be impressive, but it has to be kept in mind that this was the very first time that iVoting was possible at the parliamentary elections in Estonia (and, in fact, in the world).

Basic infrastructure of the information society is available everywhere and for everybody. This does not mean that all the work is done, issues concerning the digital divide have been solved and full inclusion is achieved. Nowadays, we must focus on different stratums of society rather than concentrate solely on the digital divide. Important issues to be tackled include motivation to use technology, insufficient skills, and limited awareness about possibilities of the information society. Recent studies show surprisingly that there are user-groups even among the so-called heavy users of the Internet, who are not aware of the existing *e*Government services. Traditionally, there is no budget line for marketing expenses in the expenditure list of the state budget, but some new programmes give hope in this field.

In order to use the Internet for managing one's affairs, people must trust the new ways of interaction.

Fortunately, trust towards e-services is rather high in Estonia. Positive experiences with e-banking, lack of big drawbacks and relatively high awareness of avoidable risks and threats have made the Internet a commonly accepted medium for all kind of activities in Estonia. Of course, one cannot be too relaxed in this field. Thus, we have elaborated our information security framework, created CERT-Estonia and introduced regulative guidelines for the use of information security measures in the public sector. In 2007, all these documents and activities proved to be much needed. In April and May 2007, Estonian Internet resources fell under heavy attacks. Inspired by the tense political situation caused by the relocation of a World War II monument, waves of heavy denial of service attacks were targeted at Estonian websites. Significant damage was avoided, but there were disruptions in the accessibility of websites and temporary cutoffs from international traffic. These attacks, also called the "cyber war", caused problems to government websites, but – even more importantly – significantly disturbed the conduct of everyday business of the private sector. As with most of the things in the world – these cyber attacks also had a positive effect. The importance of security and network resilience are now better acknowledged and adjustments have been done where needed.

The "cyber war" is not the only threat in the connected world. All kinds of "bad guys" use their creativity in order to get hold of other people's identities and money. The Estonian private sector has co-operated with the government to powerfully promote Internet security. The joint initiative called *Computer Protection 2009* aims at increasing the skills and ability of ordinary Internet users to protect themselves. Of course, for important transactions we have a powerful tool – the electronic ID-card. In 2007, a new innovative solution was introduced for electronic identity – Mobiil-ID.

Mobiil-ID offers security and proof of evidence that is comparable with the ID card – you just do not need the card reader, as necessary certificates and keys are handled through your mobile phone.

*e*Government has been one of the most advanced areas of the information society in Estonia. As a small country, Estonia cannot be the source of many new technological inventions (except maybe Skype), but we try to utilise ICT possibilities for streamlining the citizens' interaction with the government. In this context, one e-service developed in 2007 in particular deserves special mentioning – the service enabling the establishment of a company in two hours (in practice even less). As all documents necessary for starting a company can be generated, digitally signed, appropriate payments handled and confirmation acquired within very short time, the service should be encouraging for people with business ideas.

As expected, there are plans for the development of the information society also on the governmental level. The Estonian long-term strategy document in the field – *Estonian Information Society Strategy 2013* – was approved by the Government in 2006. Short-term policy is set out in annual implementation plans and the first one of them – *Implementation Plan of the Estonian Information Society Strategy for 2007-2008* was approved in 2007.

The implementation plan focuses on the involvement of citizens, electronic business environment, paperless document management in the public sector, further development of public services, and security issues. Coherent policy planning is also done for utilising a part of available EU Structural Funds for the information society development, especially in horizontal areas, where traditional institutional planning is not effective.

When climbing a mountain, one must always have a plan on how

to get back down. In case of the information society, the situation is different – nobody seriously wants to turn back. Advancements are expected to be constant and continuous, despite the fact that the essence of those improvements as well as of challenges to be faced is not always clear. What counts the most is the satisfaction and well-being of customers – our citizens.

1.2. Information Society Strategy for Local Governments – Municipality Online 2013

Pursuant to the Estonian legislation, all 227 local governments in Estonia – both the city of Tallinn with its 400,000 residents and the parish of Piirissaare with 150 inhabitants – have similar tasks to perform. As the administrative organisation in Estonia is two-dimensional, local governments are responsible for a whole range of areas, beginning from education and territorial planning to public transport and development of public water supply and sewage.

Local governments have a vital role in the development of the information society. Local government is the closest representative of the public power to citizens. Thus, for citizens the "state" often takes the face of the local power, giving the latter an excellent opportunity to act as the introducer and implementer of possibilities enabled by the information society.

However, the development of the information society at local level has been extremely uneven: alongside well developed e-towns, such as Tartu and Tallinn, there are a number of small municipalities for whom the development of *e*State by themselves is clearly beyond their power.

Thus, a document entitled *Information Society Strategy for Local Governments: Municipality Online 2013. State Policy for 2007-2013. White Book* was completed in spring 2007. The policy document, commissioned by the Ministry of Internal Affairs, was elaborated by the *e*Governance Academy in co-operation with representatives from AS Andmevara, most of local governments, the Association of Estonian Cities, the Association of Municipalities of Estonia, the Department of State Information Systems of the Ministry of Economic Affairs and Communications, and the Estonian Informatics Centre.

The document was compiled as a white paper that the Ministry of Internal Affairs could use both as an input for the elaboration of other development plans and strategies and for making fundamental decisions.

Summary of Information Society Strategy for Local Governments: Municipality Online 2013. White Paper

So far, no information society strategy for local governments has existed. Also lacking have been an agreement on a co-operation framework, division of work and responsibility between central and local governments and enterprises. Therefore, local governments have not been able to modernise the provision of public services with ICT to the same extent as the state.

The White Book describes the current situation, sets out demanding objectives, and determines roles and responsible authorities.

In spring 2007, the situation in local governments could be described as following:

All local governments have Internet connection and local government officials have a computer. The problem lies in the low quality of service and in the age and incompatibility of the existing software and hardware.

Citizens' access to fast Internet has improved constantly. Thanks to the joint efforts of telecommunications companies and the state, broadband Internet is available in most parts of Estonia. Real competition in the field is still lacking.

Digital divide between rural and city areas. Cost of broadband Internet.

Two thirds of local governments use digital document management. Archiving of digital documents has not yet been launched.

Competence in the protection, backup and secure preservation of data of local governments is limited. In addition, problems occur with the reliability of outsourced services and weak legal competence in the conclusion of contracts.

225 local governments of 227 maintain an official website. The quality of information on websites is uneven.

More active local governments have begun to **implement *e*Participation tools, making use of web forums, publishing responses given by officials to citizens' enquiries and creating possibilities for submitting comments**. Some larger local governments also offer webcasts of municipal council sessions.

Provision of e-services is limited with blank document forms for downloading and completing being the most widespread ones. Only Tallinn and Tartu offer integrated e-services, while other local governments are limited to some odd forms to be completed in the web environment.

Co-operation between local governments in the field of the information society usually takes place within one county, being dependent on the existence of leaders in local governments, county governments and/or local government associations.

There is no centre of excellence that would advise local governments on issues related to technical, legal and organisational aspects of the information society.

State support for the development of the information society in local governments has been unsystematic and based on single strong thematic programmes (i.e. Tiger Leap, Village Road, internetisation of public libraries). Pursuant to the legislation, however, local governments have the obligation to independently develop various digital registers (register of waste holders, register of misdemeanour). So far, there has not been any co-operation in developing local e-services that would yield synergy and savings.

The *Information Society Strategy for Local Governments* **sets out the following demanding objectives** in order to ensure the functioning of the state as a whole, increase the welfare of citizens and enterprises, and to quickly modernise the public sector and its services:

Fast Internet for everybody. The objective is to ensure high-quality Internet of appropriate speed for a reasonable price for citizens and enterprises in every inhabited place of Estonia by 2009.

Transition to digital management of business. The objective is to introduce digital document management in all Estonian local governments, agencies administered

thereby, as well as related enterprises by 2009.

Native language Internet and development of content of local government websites. The objective is to develop, in co-operation with residents, the native language content of websites and make available local historical heritage and information on cultural events.

Easy searchability and systematic provision of information. The objective is to make, by 2009, all local government websites information rich and easy to use also for people with special needs.

Extensive take-up of *e*Democracy tools. The objective is to provide citizens with the opportunity to participate, as from 2009, in interactive forums and debates on issues concerning the development and organisation of life of local governments.

Widespread take-up of 24/7 e-services. The objective is to ensure, by 2010, the provision of all kinds of local services also in the electronic form.

Development and take-up of geoinformation systems. The objective is the transition to digital administration of spatial data in all Estonian local governments, agencies administered thereby and related enterprises, enabling them to provide respective services gradually beginning from 2008.

Development of ICT infrastructure in local governments. The objective is to equip all local governments with up-to-date software, hardware and Internet connections by 2010.

User training and awareness-raising. The objective is to ensure that by 2010, 90% of Estonian population aged 12-74 can use the computer and Internet-based services.

Implementation of the possibilities of new technology in enterprises. The objective is to ensure that by 2009, 95% of small businesses operating in traditional branches of economy would make use of ICT in their work.

Responsibility for the development of the information society will primarily be divided between local governments and the Ministry of Internal Affairs.

The Ministry of Internal Affairs will co-ordinate the general development and co-operation with other state institutions.

Local governments will be responsible for all local matters, while the Ministry of Internal Affairs will assume responsibility for the development, implementation and administration of common solutions as well as the financing of joint activities. Some services may be provided for local governments for a fee.

As the organisation of matters related to the information society is of horizontal nature, other ministries and the State Chancellery will be responsible for the co-operation and development of services with local governments within their field of responsibility.

County governments and local government associations will be responsible for the organisation of county-level co-operation, development of joint initiatives and leading of joint projects in order to ensure the involvement of all local governments in the development of the information society.

The development and quality of e-services in local governments has continuously been examined also by the National Audit Office. A survey conducted b the National Audit Office on the development of the information society was treated in the previous yearbook (see Information Technology in Public Administration of Estonia, Yearbook 2006, Chapter 6.5 *http://www.riso.ee/en/pub/2006it/index.php?mn=44&prnt=39)*.

2. Integration of state information systems into a single interoperable whole

2.1. Estonian Semantic Interoperability Framework

The Estonian Interoperability Framework as well as developments related to international interoperability were dealt with in the previous yearbook (see Chapter 1.2 *http://www.riso.ee/en/pub/2006it/index.php)*.

While IT interoperability means the ability of information systems and of business processes they support to exchange data and share information and knowledge, semantic interoperability denotes the ability of information systems as well as of their developers to similarly understand, what type of data is exchanged and what kind of information is used. In other words, semantic interoperability refers to the ability of organisations to understand the exchanged data in a similar way.

Semantic interoperability is complicated by the fact that the use of software systems, their objectives, as well as contexts differ, leading thus differences in ways of presentation, coding and shades of meaning. In order to achieve semantic interoperability, it has to be clearly defined, which components of an information system should be semantically described in the first place. Since the development and administration of the semantics of information systems is a rather costly process, the framework focuses on most widely-used components, i.e. information systems that have been joined with the middleware X-Road. Semantic interoperability is regarded as a task to facilitate the work of software engineers and developers, who have to build interfaces with other software systems.

Reaching semantic interoperability is, to a great extent, a matter of organisational, social and educational nature. First, support is planned to be provided for system specialists of various areas in order to better understand each other's fields of activities, to compile sound documentation of data structures and protocols, and to facilitate the search of such documentation. Information systems use different tools for publishing knowledge stored in them, beginning from languages, dictionaries, classifications, and rules to complicated ontologies.

Semantic assets

Similarly to software and hardware of an information system, we can also speak of its semantic assets. The semantic interoperability assets are divided into syntactic assets and semantic assets. In order to ensure semantic interoperability between two information systems, a semantic gateway has to be established between them. The semantic gateway has to ensure semantic alterations leading to adequate use of each other's data between information systems. The semantic gateway of the state information system is a set of multilateral agreements and rules that facilitates the mutual linking of systems on the semantic level.

Syntactic interoperability assets include XML schemas, metadata schemas, and models. In this area, the objective for the coming years is to establish principles on the publication of data-schemas and definitions of metadata. The syntactic level of interoperability is the first stage in achieving semantic interoperability and it can be

achieved by creating repositories for XML schemas.

Semantic assets of semantic interoperability denote information resources that have been created in order to ensure interoperability of information systems. Semantic assets of semantic interoperability are divided as following (the division is based on the IDABC working paper *IDABC Content Interoperability Strategy*):

- dictionaries,
- thesauri,
- nomenclatures,
- taxonomies,
- mapping tables,
- ontologies,
- service registers.

The benefits of implementing semantic assets are the following:

- the quality of data will improve, data from different sources can be integrated, there will be less errors and inaccuracies upon using the data and making decisions;
- less investments in the production (acquisition) of data will be needed, as it will be easier to reuse the existing data;
- parties will have to spend less time on integrating the information systems of different organisations;
- sustainability of the information systems will increase and it will be easier to make further developments. The knowledge base related to information systems will be preserved also after key persons have left the organisation.

The Semantic Interoperability Framework's chapter on requirements sets out specific tasks and timetables for public sector institutions. The tasks are furnished with explanations.

For an in-depth overview of problems related to semantic interoperability, see *Methodology for the Semantic Interoperability of Databases and Operations Performed by Databases* and *Instructions for the Semantic Interoperability of Databases and Operations Performed by Databases* at: *http://www.riso.ee/en/information-policy/interoperability* (in English).

2.2. Web Interoperability Framework

Every public sector institution maintains a website. As websites are considered parts of agencies' information systems, they could be regarded as Internet-based human-readable views of them. The development of the website of a public body is procured by its management. The website can be designed, developed and administered internally by the agency or it can be (entirely or partly) outsourced. Every state agency is responsible for the content and form of its website.

The Web Interoperability Framework deals with interoperability of central and local government agencies' websites. The main emphasis of the document is placed on semantic and organisational interoperability. The *semantic* interoperability of websites means access to data (names, addresses, dates, texts, etc.) in a form enabling their further automatic processing, not just for displaying them. The *organisational* interoperability of websites in turn describes the administration and implementation processes

of web content. The framework together with the related documents is available at: *http://www.riso.ee/et/koosvoime/internet* (only in Estonian).

The Web Interoperability Framework does not provide requirements or recommendations for state agencies' intranets. Neither contains the document detailed requirements for the websites' content and form. Recommendations and requirements for the content of websites have been set out in the Public Information Act, while rules for the form of websites have been established in WAI standards (see *http://www.w3.org/WAI/*). The framework deals, first and foremost, with problems related to the semantic and organisational interoperability of websites. No direct state-level requirements have been established for the hardware and software of websites – every institution is free to choose the most suitable platform.

Nationwide portals, such as the *e*State portal at *http://www.riik.ee* and the Citizen portal at *http://www.eesti.ee* serve as single point of entries that operate in collaboration of information systems/websites. Users of these portals are not interested in information systems/websites that have generated the information, but rather in the data maintained in them. Thus, websites maintained by public, private and third sector organisations must cooperate and function as a whole for users.

The framework sets out general architectural principles for the websites and portals of central and local government agencies as well as requirements for the organisational and semantic interoperability. The requirements are obligatory in the development of state portals *http://www.riik.ee* and *http://www.eesti.ee* and recommended for all public sector information systems.

Key principles of web interoperability

The framework establishes the following principles to be pursued in the development of websites:

- the content of websites is XML-based and re-usable by any agency or person in any information system;
- for data exchange, HTML or XML format is used over http or https protocol;
- the used XML format is easily comprehensible, documented in an understandable manner for the developers, and does not contain noise – unnecessary tags and details;
- the presentation layer is realised as a separate application that communicates with the main application via XML documents;
- public sector websites are displayed in the user's browser in HTML or XHTML format;
- public sector websites use clear addresses with semantic content (use of dynamic addresses is not recommended);
- files to be downloaded from public sector websites are in open format, i.e. .odf, .pdf, .png, .svg, .rtf or compressed versions thereof in zipped format. Use of company-specific formats (such as, e.g., .doc, .xls, .ppt, etc.) should be avoided. Files published on the website must be readable (and editable if necessary) with open source software;
- the content of public sector websites must be easy to index by search engines and SEO (Search Engine Optimisation) principles are to be followed;
- in the development of public sector websites uniform copyright principles are followed;
- the tables of contents and summaries of websites are presented, in addition to their visual design, also as RSS or RDF feeds;

- standard-based interoperability is ensured between institutional/thematic portals and the Citizen information portal *http://www.eesti.ee* and the *e*State portal *http://www.riik.ee/*;
- in the development of websites, recommendations of the Web Content Accessibility Guidelines Working Group (WCAG WG) have to be followed *http://www.w3.org/WAI/*;
- a state agency's website is laconic, aesthetic, adequate, topical and ergonomic. The structure of text material on state agencies' websites has to be well-considered. The information and data management of a website must ensure that users could find solutions to their problems in a fast and transparent manner. Use of pictorial material on state agencies' websites should be brought to a minimum;
- the websites of public sector institutions make use of modern technologies and solutions in order to promote democratic processes and increase the interactivity of websites through wikis, forums, polls, etc.;
- each ministry has the obligation to organise, for its websites, the development and administration of semantic assets proceeding from its administrative area;
- the content of websites must correspond to the standard EVS 8:2000 "Requirements on Information Technology in Estonian Language and Cultural Environment";
- the content of websites must be encoded in UTF8 format.

The framework sets out deadlines for the realisation of the key principles, e.g. public sector portals have to be brought into accordance with the principles of the framework by July 1, 2008 and central portals by January 1, 2008. The framework also establishes deadlines for the development and implementation of specific tools (e.g. lemmatizer, etc.) and functionalities (RSS, wikis, forums, polls, blogs, etc.).

2.3. Co-operation in the field of information security

The Estonian economy is largely based on the development of IT. Although the recent episode of cyber attacks put Estonia to test, it strengthened Estonia's resistance and highlighted the weaknesses of our IT systems and infrastructure. Information security is of utmost importance when it comes to situations where cyber attacks that are technically not that complex might disturb the external communication of state agencies or the Internet banking operations of major banks. The Estonian Information Society Strategy 2013 also envisages increasing the security of the public sector services provided to businesses and citizens and raising people's awareness of security issues. Ensuring information security is no longer up to one authority, company, working group or the state – all stakeholders in Estonia and abroad need to join their efforts.

To this end, a number of co-operation principles have been included in the Information Security Interoperability Framework. This document aims at establishing a safe, security-conscious and development-oriented information society in Estonia. That includes the following activities: management of IT related risks; protection of fundamental human rights; raising of the competitiveness of Estonia's economy; public and private sector

co-operation on information security; acknowledgement of information security related problems, and IT security training.

The framework comprises five primary fields of IT security, covering both public and private sector agencies. The following table outlines the five IT security fields along with examples of respective activities and field co-ordinators.

Field	Examples of activities	**Co-ordinating authority**
Co-operation and co-ordination	Co-ordination of conducting the risk analysis of the Estonian IT environment; raising of the effectiveness of handling security incidents in Estonia	Ministry of Economic Affairs and Communications
Acknowledgement and training	Provision of IT security training for the top management and IT managers of public agencies; raising of the awareness of security issues in schools and universities	Ministry of Education and Research in co-operation with the State Chancellery, the Ministry of Defence and the Ministry of Economic Affairs and Communications
Elaboration of regulations	Drafting and updating of legislation on information security and electronic communications; drafting of regulations for the protection of critical information infrastructure; co-ordination of database administration pursuant to the requirements of the system of security measures; elaboration of information security standards applied in public procurement	Ministry of Economic Affairs and Communications in co-operation with the Ministry of Internal Affairs
Protection of information infrastructure	Provision of protection of information infrastructure; organisation and co-ordination of fight against cyber crime	Ministry of Internal Affairs in co-operation with the Ministry of Defence
Implementation activities for the protection of people and assets	Implementation of personal data protection measures; development and introduction of secure (ID card based) standard solutions; launch of cross-border ID card based services	Ministry of Internal Affairs in co-operation with the Ministry of Defence

The framework is aimed at better protection of vital information and communication infrastructure; it does not cover data or systems related to state secrets or military use. In terms of technology, the information security framework comprises the security of IT systems as well as electronic communications.

Other authorities closely related to the field of information security include the Department of State Information Systems and the Communications Department of the Ministry of Economic Affairs and Communications, the Estonian Informatics Centre, the Data Protection Inspectorate, the Technical Inspectorate, the information technology crime division of the Central Criminal Police, the IT lab of the Forensic Service Centre; the development and

learning centre of communication and information systems (SIVAK) of the Defence Forces, a NATO co-operative cyber defence centre of excellence to be established, the EENet, the Consumer Protection Board, and others.

The main private sector stakeholders are banks, telecommunications companies, Eesti Energia, AS Sertifitseerimiskeskus, IT service providers and security companies.

The organisation of information related activities should, above all, proceed from the Government Regulation on establishing a system of security measures for information systems and the methodology of ISKE (a three-level baseline protection system for information systems). The purpose of ISKE is to provide security for the data processed in information systems and related information assets. ISKE can be used also in other state and local government agencies, the business sector and non-profit organisations. However, it is not meant for ensuring the security of information systems that handle state secrets. ISKE is based on the information security standard IT Baseline Protection Manual (IT Grundschutzhandbuch) published by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI). The BSI's system is documented in considerable detail and it is revised regularly once a year. The BSI's website (*http://www.bsi.de/gshb/downloads/index.htm*) includes various materials on ISKE, including guidelines in German and English.

According to the information security framework, the senior managers, IT managers or IT experts who maintain state or local government databases must consider also the following principles:

- It is recommended to take into account the IT governance framework CoBIT and information security standards, such as ISO 27002, EVS-ISO/IEC TR 13335 etc.
- Information security policy-making and budgeting in an agency should, among other things, draw from the information policy documents and related implementation plans, the Estonian IT Architecture and Interoperability Framework and the concept of central infrastructure services of the state information system. It is also useful to consider recommendations on an agency's information security policy as well as the continuity and recovery plans of an agency's information system but also the proposals outlined in the "Computer Protection 2009" initiative (see also Chapter 3.2).
- The development of databases should, in addition to the ISKE methodology, proceed from the Public Information Act, the government regulation on the implementation of the data exchange layer of information systems, and the standards listed in the Information Security Interoperability Framework.
- As regards personal data, it is also necessary to adhere to the Personal Data Protection Act and the requirements established by the Data Protection Inspectorate for ensuring availability, integrity and confidentiality in personal data processing.

The ISKE methodology, information security standards, the CoBIT framework and strategy documents should be observed, when necessary, also if an agency does not maintain databases or process personal data.

In addition to the domestic co-operation projects described above, Estonia participates in various international information security initiatives: the establishment of a NATO co-operative cyber defence centre of excellence; the activities of ENISA (European Network and Information Security Agency); a high-level expert group on cyber crime under ITU (International Telecommunication Union), etc.

2.4. The X-Road: a key interoperability component within the state information system

The X-Road, the data exchange layer of the state information system,[1] has from the very start drawn from various strict principles that stress the uniqueness of that solution. The key starting point for building the X-Road architecture was to include a complex security solution: authentication, multi-level authorisation, a high-level log processing system, encrypted data traffic with time stamps, a warning system for servers against cyber attacks etc. No earlier public sector information systems had been designed by such strict principles. As a rule, the information system is first designed and launched, and only then do data security and availability risks become an issue.

Another important principle applied from the very start of the X-Road is its service-oriented architecture. For developers, this means that a majority of the application systems that use the X-Road can be, and already have been, built on the basis of services. Today, this principle is considered vital also elsewhere in the world, whereas in 2001 when the X-Road started off, it was not that topical.

For the X-Road, year 2007 – just as several previous years – was the year of extensive penetration, as the use of its services grew by over ten million times in number. The following gives a short overview of the developments and modifications of the X-Road carried out in 2007.

[1] For the principles and developments of the X-Road see the previous issues of the Yearbook. A summary of the previous period is available in the IT yearbook of 2006 at *http://www.riso.ee/en/pub/2006it/index.php?mn=10&prnt=6.*

New application areas of the X-Road

The **universal single user portal** is a further improvement of the X-Road portals, which enables to create specialised portals similar to the Entrepreneur Portal. For that purpose, the definition of the "sub-office" applied in the Entrepreneur Portal was specified. Instead of a "sub-office", "unit" is defined. "Unit" is an object within a universal portal, representing the owner of legal rights. For instance, legal person is the unit in the Entrepreneur Portal; in the Family Doctors Portal it is the family doctor. The unit in the Health Service Providers Portal would be the "health care institution"; that is the legal person entered in the respective register and having a licence.

Family doctors, notaries, pharmacists and others will be using X-Road services provided by the Estonian Health Insurance Fund and other databases that have joined the X-Road. In principle, the users of the new solution will be using X-Road services via programmes; i.e. the queries will be made by the softwares of the users. In addition to the main users (e.g. family doctors), the software will be used by other parties work-wise related to the user (the support staff of family doctors, e.g. nurses). Therefore, the latter will also have to use X-Road queries that are provided for the main users.

Since it would be too complicated for single users (e.g. family doctors) to join the X-Road separately, as this would require making queries through their own security servers, a common portal was created for user

groups, such as family doctors, specialist doctors, notaries, etc.

The software of such a group of single users will be making X-Road queries via programmes through the Family Doctors Portal, the Notaries Portal, etc. Moreover, the single user will be able to make queries from the user's portal in a traditional way; that is through the portal's web interface.

For Estonia's accession to the **Schengen information system**, various X-Road services were developed both for police officers and border guard officials. At the same time, the Ministry of Internal Affairs also provides other ministries with data from databases related to the Schengen information system through the X-Road. The control commission of the Schengen information system controlled compliance with the very strict safety rules and adopted the whole service package. The entire system had to be, and was, launched at the very moment of Estonia's accession to the Schengen visa area (December 22, 2007).

The most wide-spread X-Road services at the present day include the **e-services of the social sector**. The Social Insurance Board has been providing its services (parental benefits, family allowances etc.) through the X-Road already for many years. From 2006 on, the most popular services with the largest number of users have been those provided by the Estonian Health Insurance Fund (for further information see the IT yearbook of 2006[2]). In 2007, various *e*Health project solutions that are based on the X-Road were completed.

Improvements to X-Road solutions

Information technology is a rapidly developing area. The X-Road is constantly improving, and so are other state information system components, like portals and application systems (e.g. the Work Schedule and Project Management information systems). One of the latest technological changes in the X-Road stemmed from the decision that the officially outdated data transmission protocol XML-RPC would no longer be supported as of 2007. Consequently, all the services were made SOAP-based by the end of 2007.

The existing state portals were joined with a new single platform under a common design in 2007. Consequently, it was possible to start with the project of developing the presentation layer of X-Road queries. This project will result in a uniform presentation mode of the portals. Citizens will be able to see their data in the registers in the portal *www.eesti.ee* and use the services provided by the registers in the same format as available in other parts of the portal. The temporary solution launched for several years ago, known as the "blue citizen's query portal" after its blue design, will be terminated. The same bluish design will be seen for a while in 2008 in the so-called MISP-portals of state agencies. A new design will be developed during 2008.

In 2008, the new Public Information Act entered into force, which among other things envisages the elaboration of a new version of the regulation on the implementation of the data exchange layer of information systems (also known as the X-Road regulation). In 2007, also a new set of X-Road rules, the implementation guide of the X-Road, was completed.

All developers of the X-Road services and application systems have been provided with training on an annual basis and will be provided also in the future. In 2007, training was organised for the developers from various IT development companies.

[2] *http://www.riso.ee/en/pub/2006it/index.php?mn=10&prnt=6*

The use statistics of the X-Road show that private companies have started to design and utilise more and more X-Road services. For example, the usage of data by SEB Eesti Ühispank from the databases of the Citizenship and Migration Board and other similar services were introduced.

One of the biggest development projects of the Estonian Informatics Centre in 2007 was the development of a new version of the administration system for the state information system (RIHA; see Chapter 2.7). The launch of this new solution should result in the automation of various activities of the agencies that have joined or will join the X-Road, thus also making their activities more paperless. Joining the X-Road will become RIHA-based in the near future. RIHA will be offering a complete overview of all X-Road services.

Year 2008 will see improvements to the authorisation services of the X-Road. The authorisation of the users of social services started off already in 2007 when the register of family doctors was established. In the short run, similar services for the authorisation of specialist doctors and pharmacists will be introduced. Further on, the overall functionality of authorisation will be expanded. To this end, new options will be added to portals and application systems for the authorisation of officials and enabling and it will also be possible to copy the authorisation data between different service providers and users.

Statistics of the use of X-Road services

The statistics of the use of the X-Road indicate that in 2006, over 29 million X-Road services (queries, data transmission, document exchange, etc.) were utilised, whereas in 2007 the use of X-Road services was more active and more progressive over months. In February 2007, for instance, 2.85 million services were used per month; in October, the respective figure stood at 4.37 million (see Figure 2.4.1).

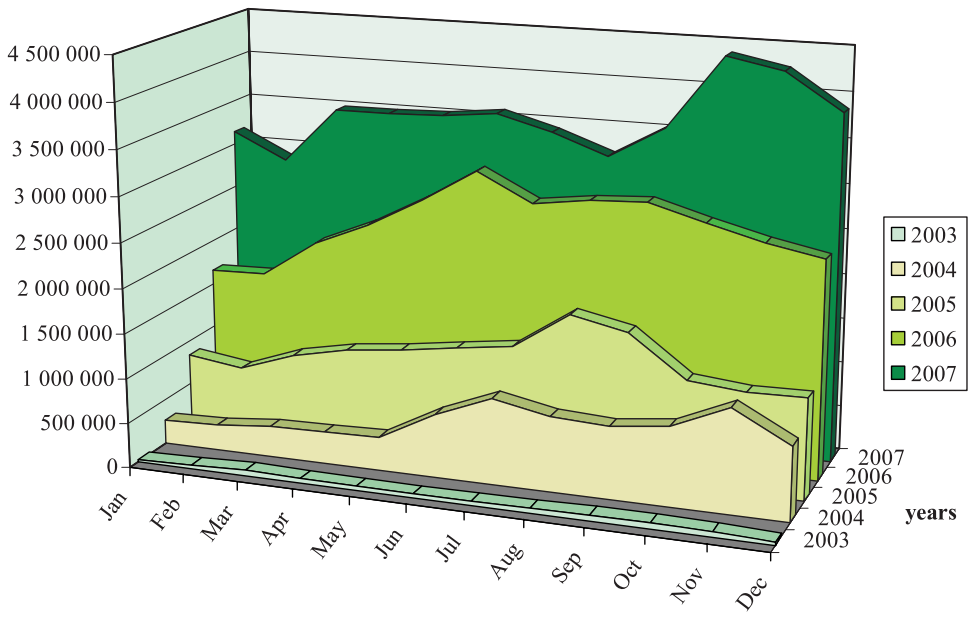


Figure 2.4.1. Statistics of the X-Road services during 2003-2007

The X-Road is scalable (it is possible to add security servers that are running in parallel), which enables the X-Road Centre to increase the power of the servers processing the system by adding new servers to, as the availability grows. There is no need to worry about exceeding the maximum power, as there is only about one million potential PC users in Estonia, whereas web-based solutions are applied also in countries where services (e.g. Internet banking) are being used by hundreds of millions. The scalability of the X-Road was highly acknowledged by the auditors of the Gartner Group who drafted a report commissioned by the European Union on Estonia's IT solutions.

2.5. Transition to paperless administration in government agencies

At the beginning of October 2007, the Estonian Government adopted amendments to the regulation on uniform bases for records management procedures with the objective to speed up the transition to paperless administration in state agencies. Consequently, the ministries and the State Chancellery were obliged to introduce the exchange of digital documents between records management systems by December 3, 2007, at the latest. County governments, boards and inspectorates will have to be ready by May 5, 2008, at the latest. (An exception has been made to three ministries who have a longer transition period.)

The amended regulation provides for exchange of digital documents via the inter-agency Document Exchange Centre of the X-Road, using the internationally recognised standard for data exchange – the Extensible Markup Language (XML). The transition to document exchange between systems will be implemented in stages (by agencies and types of documents). In the case of local governments and other groups of agencies the level of administration and availability of resources is more uneven, which is why it takes more time to prepare for the transition to electronic document exchange and it is not expedient to put all state agencies under the same obligation. Transition in these agencies will now be primarily facilitated by supportive measures.

To ensure the transition to paperless administration, a number of changes were introduced to the requirements for records management systems and exchange of digital documents between systems. As a result, records management is now treated as an integral process. Digital documents have to be drawn up on the basis of document forms with uniform data structure and linked to the metadata of document management. These metadata describe the context, content, structure and management history of a document and ensure the authenticity, integrity and usability of the document throughout its lifecycle; that is, until the destruction or transfer to an archive.

The **administration of metadata** is an integral part of records management and involves various functions and objectives. Metadata are structured or partly structured information that enables to draw up, register and classify documents, provides access to and ensures the storage and separation of documents in time within one domain as well as between different domains. Metadata first define the document at the time of its acquisition in a

records management system by registering the document through further activities and establishing control over it. New metadata are added to documents or document sets on a current basis when new operations are performed or changes made. Metadata can be used in a number of systems and reused for different purposes. The metadata related to a document during its lifecycle may be needed also when the document is no longer necessary for performing current tasks but is stored for future analyses or some other value (incl. archival value). Furthermore, metadata also support the transfer of documents between different environments or platforms.

The abovementioned regulation allows for simultaneous records management within one records management system for numerous agencies at a time. This way smaller agencies can economise on the resources needed to create a records management system. Records management systems should support this kind of approach and provide for the use of different and autonomous systems for the classification of documents.

The transition to exchange of digital documents between systems will substantially improve the efficiency of state agencies. The **Document Exchange Centre** (DEC) is a central information system for connecting dispersedly located records management systems via the X-Road.[3] Its primary function is to transfer documents, in particular digitally signed documents. There are three ways to do that:

1) If the agency has got a records management system, it is connected with the DEC, which enables to send documents to the records management systems of other agencies.

2) If the agency does not have a records management system, the DEC transfers documents to that agency by e-mail.

3) Citizens can e-mail documents to the DEC to be forwarded to relevant agencies. Agencies can reply to citizens by e-mail (either directly or through the DEC).

In the future, the Document Exchange Centre will also be used for sending other types of XML-based documents besides letters, such as legal and financial documents, invoices etc.

In addition to the IT support of the DEC, the interoperability of records management systems and the automatic, secure and paperless document exchange between agencies calls for the uniformity of the transferred documents and their metadata. Therefore, the exchange of digital documents between records management systems through the Document Exchange Centre makes use of document forms with uniform data structure, the Extensible Markup Language recommended by the World Wide Web Consortium (W3C) and the State Chancellery's guidelines on document elements and metadata. To guarantee uniform presentation of document content, state agencies must co-ordinate the XML-based presentation forms of the documents to be channelled through the DEC with the State Chancellery. The co-ordinated XML-based presentation forms will be used for setting up a database that would allow the reuse of uniform presentation forms.

The transition to electronic records management is a long process. In addition to inter-agency electronic document exchange, it entails the development of intra-agency electronic records management, optimisation of agencies' work processes and related records management processes, and so on. The amendments to the regulation on uniform bases for the records man-

[3] For further information on the Document Exchange Centre, see the IT yearbook of 2006 (*http://www.riso.ee/en/pub/2006it/index.php?mn=11&prnt=6*) and the web site of the Estonian Informatics Centre (*http://www.ria.ee/28567*).

agement procedures set out the tasks for ministries and the State Chancellery for the co-ordination of the transition to electronic records management. The State Chancellery is expected to plan and organise the development of and transition to electronic records management in the public sector as well as provide related guidelines. To make the transition as smooth as possible, the State Chancellery is to consult and assist other state agencies in the procurement, application and development of the necessary software; organise trainings; introduce the best practices of records management; harmonise records management procedures etc.

2.6. Developments in digital archiving

The development of the Estonian digital archiving is comparable to the respective developments in advanced European countries. The National Archives of Estonia[4] conducts close co-operation with the national archives of Sweden, Finland and Portugal as well as the long-term preservation centres in Luleå (Sweden) and Mikkeli (Finland) to implement various EU projects and prepare for project applications. Digital archiving is enhanced in Estonia simultaneously with the general development of electronic records management, databases and software applications.

To this end, the Digital Archiving Strategy 2005–2010 has been elaborated to achieve legal, intellectual and technological readiness for the evaluation, receipt, preservation and use of digital materials in the National Archives, and facilitate the proper management, description and archiving of digital documents and transfer of archives in state agencies. For a short overview of the Estonian Digital Archiving Strategy, see "Digital preservation in Estonian National Archives".[5] The strategy was fully completed in 2005 and followed by further steps necessary to achieve the abovementioned objective as laid down in the strategy.

In 2006, in co-operation with the consultation company Ernst&Young Baltic, the key preparatory components of the digital archive structure were completed: namely the vision, architecture and a project plan for the architecture. These components contribute to further developments of the digital archive in the National Archives.

One of the main prerequisites for designing the architecture of the digital archive information system is the conception of the functioning of a digital archive. This is set out in the functioning model of the digital archive, which is based on the Open Archival Information System standard, later known as the international standard ISO 14721:2003, and the current practices of the State Archives and the Estonian Historical Archives[6].

[4] The National Archives of Estonia is a government agency which was founded on the basis of the Archives Act in 1999 by reorganising the Public Archives Services. It is a system of state owned public archives and includes 13 archives in different locations of Estonia, and acts under the administration of Director General, who resides in Tartu. It is subordinated to the State Chancellery. The National Archives ensures the preservation of and access to information about the changes in the Estonian society.

[5] See *http://www.ra.ee/galahad/file_storage/2/949*.

[6] The State Archives and the Historical Archives are the two central archives under the National Archives.

The main functions and processes of the digital archive have been mapped and analysed, serving as the basis for the role model, conceptual model and functional requirements of the archive that specify the archive's functioning model and lay a foundation for the architecture of the digital archive information system.

The core concept for designing the digital archive infrastructure relies on the service-based architecture. Proceeding from the above-described archiving processes, the use of services of different components is related and co-ordinated by workflow management tools.

The design of the architecture strictly follows the principle of storing the applications of different data operations, logic of functioning, user interfaces and other interfaces logically separately. Such an approach makes the administration and further development of the system as simple as possible, similar to a service-based architecture.

The digital archive information system is divided into the following logical key components.

Workflow management – components that ensure the functioning and traceability of the main processes of the digital archive, including the receipt of records, access to and management and storage of records.

Repository – systems for storing data preserved in the digital archive, which can be divided into components of permanent storage, components securing the work of archivists and components securing customer service.

Records – the general register of the digital archive that includes content and technical metadata about the information packages stored in the archive.

Support registers – registers that store the support data of the digital archive workflows and include the main functionalities for adding, inquiring and changing data.

User interfaces – components that provide access for information system users to the functionalities of the digital archive.

Search engine – an index base that is based on the information available in the records and services client's queries.

Administrative support systems – systems that guarantee the information security (access rights, logs), configuration management and backup of the digital archive.

The National Archives is establishing the digital archive in stages. The objective is to complete the digital archive infrastructure by the end of 2009, so as to be able to start collecting digital records from archivists as of 2010.

The digital archive itself will be established in four stages during 2007–2010. Every stage consists of a number of projects for implementing different parts of the digital archive.

In the first stage, practical activities for offline receipt of digital records will start and additional analyses for the development of the integral digital archive will be made. This will entail additional research on the different components of the digital archive and the functioning of these components. In addition, world practices and already available solutions will be examined to see if they could be applied in the Estonian National Archives.

The second stage is aimed at the development of the basic functionality of the digital archive to a limited extent – primarily for internal use in the National Archives. In the third stage, the majority of the archive's functionalities (addressed to all stakeholders, including the customers, the archivists and the staff of the digital archive) will be implemented. A special emphasis will be laid on the functionality that enables the receipt and transfer of data only via electronic channels. The fourth stage will witness the final elaboration and introduction of the

digital archive, including setting up a duplicate repository for storage packages and developing systems that would provide for reporting and for analysing user statistics.

In addition, external interfaces need to be established, so that also other systems (e.g. records management systems; query systems of other countries) could be integrated with the functionality of the digital archive.

In 2007, an analysis of the acquisition of records metadata from electronic records management systems was prepared. Another analysis carried out last year examined the functionalities of the preliminary universal archiving model (UAM). The UAM will be used for bringing digital documents to the format set out in the archive's requirements and is located in the agency that stores the data. The module communicates with the National Archives' reception module via the X-Road (data exchange layer) and the DEC (Document Exchange Centre), and enables to store data both in the National Archives and the agency itself. In 2007, the implementation of the UAM and preparations for creating the library of records of the digital archive were started.

Another set of instructions related to the receipt of digital documents from agencies is the National Archives' requirements for archiving digital documents that handle the separation of digital documents and their metadata from electronic records management systems and transfer to the public archive. The requirements help to define the description elements of documents with archival value and give guidelines for the development of an agency's electronic records management systems so that the documents and/or their descriptions drawn up would be suitable for transfer to the public archive.

All the existing and future documents related to the establishment of the digital archive and the development of digital archiving will be available in the digital archiving consulting environment of the National Archives (*http://www.ra.ee/digiaken/* – in Estonian only).

2.7. Developments of the administration system of the state information system

Background and objective

The development of the state information system as a logical whole is based on information of the existing state information systems and databases and the services they provide. In other words, it is necessary to have a central overview (metadata) of all available information systems and the services they provide.

To this end, the Ministry of Economic Affairs and Communications is establishing the sixth support system for the state information system, namely the administration system for the state information system (RIHA). The objective of RIHA is to ensure transparent administration of the state information system, plan for the state information administration and support the interoperability of databases that provide public services (see also *http://www.ria.ee/27313*).

In Estonia, as of 2008 the establishment and maintenance of public sector information systems and databases is regulated by the Public Information Act. Pursuant to this Act, information system managers are obliged to register their databases and information systems in RIHA and ensure that the related metadata are up-to-date. The administration system for the state

information system gives a new perspective to the regulation of databases in Estonia, as it proceeds from the need to introduce a state information system that would be functioning according to new principles. New legal solutions are necessary so as to develop the state information system into a single interoperable service-based data environment in place of the current decentralised state information system.

RIHA is an improvement of the State Register of Databases (ARR), established in 1997 to maintain records of national databases and state registers. By today, ARR has become outdated and its functionality no longer meets the needs related to the description of services provided by various information systems. Therefore, RIHA is currently being developed to establish a system with extended functionality that would better respond to the needs of users.

RIHA's functionality will be extended so that the system would be regularly mapping the Estonian information systems to give an up-to-date overview of the state's IT resources and their use options. Only this way we could get a clear picture of the existing components of the state information system in various state institutions, the components still needed, and possibilities to make the optimal use of such components. It is important to ensure that all RIHA's stakeholders (target groups) would have a view and functionality responding to their roles/responsibilities and guarantee an integral treatment of the system's key objects.

RIHA's target groups and necessary functionality

RIHA will be a tool for the following target groups:

1) administrators and maintainers of state agencies' information systems;
2) users of the services of the information systems belonging to the state information system;
3) administrators and maintainers of classifications used in information systems;
4) legal persons in private law and citizens as receivers of information about the state information system;
5) Ministry of Economic Affairs and Communications as the authority co-ordinating the development of the state information system;
6) Estonian Informatics Centre as the central administrator and maintainer of the state information system;
7) Statistics Estonia as the co-ordinator of classification development and collector of statistical data;
8) Data Protection Inspectorate as the supervisory authority for the protection of personal data;
9) National Archives as the agency responsible for the preservation and use of information about the Estonian society;
10) service desk of the state information system as a tool for the employees of state agencies and the service desk staff of the Estonian Informatics Centre.

Every user group of the RIHA may perform several different roles in the state information system. For instance, the agency that administrates a classification may simultaneously be an information system administrator and service provider; the agency that has the role of a service user may also act as the information system administrator, service provider or classification administrator.

The functionality of RIHA must guarantee the information needed by the target groups to perform all their roles.

For example, a service provider needs RIHA as a tool that would enable to:

- find out about the existing services and those being developed, the service descriptions and the principles of service provision;
- see the data related to services, information systems and classifications;
- see the monitoring data and the statistics of the use of the X-Road;
- monitor the compliance of service level parameters to concrete needs;
- apply for the right to use a data service;
- make proposals for the development of new services;
- identify contact persons of agencies, etc.

For legal persons in private law and citizens, RIHA must give an overview of the state information system and enable to:

- obtain information about services, information systems and classifications;
- make proposals to information system administrators for the development of new services.

Key objects of RIHA and links between them

The key objects of RIHA include the following:

- organisations as information system administrators, service providers, service users or classification administrators;
- information systems;
- services;
- classifications.

Semantic descriptions of information systems and services constitute an important component of their general descriptions. The creation of semantic descriptions requires the development of ontologies; that is, dictionaries that define the terms of a specific domain and show the taxonomy between them.

The description of terms should be both in human-readable (HTML and UML schemas) and machine-readable (OWL and UML schemas in XMI) format.

In order to develop semantic descriptions of information systems and operations performed by them, the Instructions for the Semantic Description of Databases and Operations Performed by Databases[7] were elaborated for drawing descriptions and administering domain glossaries.

Developments of RIHA

The development of RIHA started off in 2005 with the creation of the concept of RIHA. In 2006, a procurement for the analysis and design of RIHA was carried out and completed in April 2007.

RIHA will be implemented in two stages. First, the so-called catalogue system (the "small RIHA") will be created by July 2008. Next, the whole RIHA along with all the necessary administration support processes (the "big RIHA") will be completed by 2010.

The main purpose of creating a central metadata catalogue is to give a complete overview of the Estonian state information system both for database administrators and state information system co-ordinators. Besides the catalogue service, RIHA also includes other components of an integral management system (incident management, service level management, management of changes, problem management, service desk and configuration management) that contribute to

[7] See Version 1.1 at *http://www.riso.ee/en/files/EstonianGov_Semantic_Description-Instructions_v1.1c.pdf.*

the management and design of the state information system.

One of the development principles of RIHA is to build an open system that would at all times take into account the needs and proposals of users and implement these needs stage by stage.

Pursuant to the new version of the Public Information Act, which entered into force on 1 January 2008, RIHA will be established as a support system for the state information system. Like all other support systems of the state information system, RIHA will be established by a government regulation.

More precisely, the regulation sets out the co-ordination process for the establishment of databases by stipulating the exact terms and conditions and the procedure related to the establishment and maintenance of databases, which is based on the technical solution of the administration system for the state information system. Thus, RIHA should be perceived as the collection of principles and basic rules for the management of the state information system and the related information system through which these principles and management functions are implemented.

2.8. Developments in the field of eID

Estonian ID card

Preparatory work for the use of electronic identify (eID) in Estonia was started in the second half of the 1990ies, evolving into a national programme aimed at the implementation of the Estonian ID card and the respective public key infrastructure (PKI). As an outcome of this Est-eID programme, issuing of ID cards began on 28 January 2002.

The ID card is a mandatory identity document for all Estonian citizens over 15 years of age and for aliens residing in Estonia on the basis of a residence permit irrespective of their age. The cards are issued by the Citizenship and Migration Board.

The ID card is not just a plastic document for the visual verification of its owner, but it also contains a chip with a personal data file and two certificates – one for the secure electronic authentication of users and the second for giving digital signature.

Pursuant to the Digital Signatures Act, digital signature is equivalent to handwritten one not only in transactions between the citizen and the state, but also on a wider scale in all activities between private companies and in proceedings taking place between citizens. Anyone with a valid ID card can give digital signature.

Mobiil-ID – what is this?

Though more than one million ID cards have been issued in Estonia, eID related developments are far from being finished. Rather on the contrary – only now that people already possess the ID card, main attention is paid to their extensive use. One of the basic objectives of *Computer Protection 2009* – a co-operation initiative between the state and private companies (see Chapter 3.2) – is to increase the take-up of the ID card and other similar "strong" identification mechanisms.

Wider implementation of electronic ID presumes the existence of alternatives beside the ID card. If only in case one would forget his or her ID

card at home or lose it. Similarly, it would be unfortunate if eSchool[8] could be accessed solely with the ID card, while replacing the lost card takes several days.

Such an alternative exists in the form of the Mobiil-ID service, launched by the joint effort of AS Sertifitseerimiskeskus (Certification Centre) and the Estonian mobile operator EMT in April, 2007. Mobiil-ID is a solution for electronic personal identification and giving digital signature, which is based on the public key infrastructure (PKI) and in case of which the private keys of the user are maintained on the SIM card of the mobile phone. In case of Mobiil-ID, the SIM card of your mobile acts like your personal identification document in the electronic environment, just like the ID card: i.e. in addition to the functionality of an ordinary SIM, Mobiil-ID SIM also holds your mobile identity, allowing Internet service providers to identify you and lets you give digital signature.

Mobiil-ID can be used with all modern mobile phones. The phone must have a GSM Phase 2+ support, which is a standard for almost all mobiles produced since 2000.

Prior to use, the Mobiil-ID SIM needs to be activated.

Personal identification and digital signing functionalities are secured by up-to-date security technology and corresponding Personal Identification Numbers (PIN). What makes the solution more convenient is the fact that you no longer need the ID card reader in your computer: instead, you can access your Internet bank from any available computer. The mobile phone acts as the ID card and the ID card reader at the same time. Nevertheless, the use of Mobiil-ID is not entirely free of charge and, in terms of reliability, the service probably remains slightly inferior to the ID card.

In order to identify yourself securely with Mobiil-ID, you have to click on a respective button in the web (usually saying *Enter with Mobiil-ID*), after which you mobile prompts you to enter your PIN. You will be identified after entering the code. The same routine is followed also when signing documents digitally.

Mobiil-ID is supported by practically all major Internet services in Estonia that require authentication. In the DigiDoc portal and with the help of DigiDoc Client, Mobiil-ID also allows giving digital signatures. The providers of e-services should ensure that if using their service requires the ID card, it should also be made possible with Mobiil-ID.

Providers of e-services willing to offer Mobiil-ID personal identification and digital signing functionality in their system need to subscribe to the DigiDocService, provided by the Certification Centre for digital signing, verification of signatures and personal identification. This service provides the functionality for creating digitally signed files (DigiDoc) and verifying digital signatures, enabling third parties to securely authenticate persons in their systems by Mobiil-ID.

Work is underway with other Estonian mobile operators (Elisa, Tele2) so that they, too, could launch their Mobiil-ID solutions. For more information see: *http://www.id.ee/10995.*

The Baltic dimension of Mobiil-ID

As the main providers of e-services – Internet banks – operate in all Baltic states, it is only natural that they are interested in using the

[8] *e*School is a database and web-based school-home communication interface to make school activities and information available to parents and students on current basis and to communicate with the teacher (see Chapter 4.6)

same authentication and signing method also in Latvia and Lithuania. However, putting this to practice requires considerable effort – all major mobile operators (8) and certification service provides (3) have to be convinced to launch respective services. Even more – the respective services and technologies need to be interoperable, if not entirely similar!

As an outcome of lengthy preparatory work, eleven key organisations established, in spring 2007, a round table called Baltic WPKI Forum (WPKI – Wireless Public Key Infrastructure). The forum has its own Steering Committee and a technical working group consisting of representatives of all participating organisations. The goal of the forum is to exchange WPKI related information and elaborate standards and recommendations (for more information see Baltic IT&T view *http://www.ebaltics.com/00304609?PHPSESSID=de6b83ef21c46f771cd5535a4c55d461*).

For the time being, agreement has been reached on principles regarding the mobile side of Mobiil-ID application and work is underway on unifying digital signature standards. The forum's workstation in the Internet is at: *http://www.wpki.eu*.

In October 2007, the Lithuanian operator Omnitel also launched Mobiil-ID. The company uses certificates issued by the Certification Centre and the DigiDocService.

Cross-border recognition of eID

Cross-border recognition of eID is becoming increasingly topical both in Estonia and elsewhere in Europe. More and more European countries implement ID cards and, thus, accepting digital signature generated by a foreigner or ensuring access in one's information system with a foreign ID card no longer constitute a solely "theoretically challenging" problem.

The Ministerial Declaration approved at the *e*Government conference in Manchester in 2005 has set both the European Commission and the member states in motion. Namely, the document claims that by 2010 all European citizens must be able to use electronic identity. In addition, exchange of digitally signed documents – also between member states – has to be ensured by that time.

Whether those dreams will come true by 2010 remains to be seen, but the declaration has kick-started the implementation of ID cards in Europe. Considering its long experience in the implementation of the ID card, Estonia could assist others in this. In addition, Estonia actively participates in various initiatives and projects in the field of cross-border recognition of eID and digital signing.

The "invasion" of foreign ID cards and digital signatures to Estonia is inevitable in the coming years and, thus, tackling this issue has become a common concern for our officials.

3. Increasing skills and participation

3.1. The use of IT solutions calls for knowledge

Computers and the Internet came along with general changes in the society, escaping any special attention. However, besides financial reasons also scarcity and lack of skills, know-how and motivation started to hinder the wider spread of computers and the Internet in the society.

In order to cope in the information society, new skills and know-how as well as active participation in the use of e-services is necessary. To ensure equal opportunities for information society stakeholders and apply available ICT solutions to the fullest extent, it is necessary to systematically share information society related knowledge.

A programme for raising information society awareness, funded from the EU structural funds, aims to increase the use of available electronic solutions, promote the elaboration of e-services and ensure sustainable development of the information society through raising awareness of security issues. The total cost of this programme is 50 million kroons (ca 3.2 billion euros) and the programme is planned to be implemented during 2007–2015.

The related activities are oriented to present and future users of e-services. These include Estonian residents, entrepreneurs, officials as well as the stakeholders engaged in the development of e-services, such as policy-makers and the public sector. Raising the awareness of information society of this target group enables to achieve high motivation for the introduction of new and available IT solutions. In addition to the above, the programme includes activities oriented to increasing the awareness of opinion leaders and media representatives so as to evoke public interest and shape a more positive attitude towards new technologies and solutions. Moreover, it is planned to introduce the e-services developed and used in Estonia and opportunities provided by the Estonian state information system to the public sectors of other countries.

The Implementation Plan 2007–2008 of the Estonian Information Society Strategy focuses on four major action lines: raising awareness of the use options of the electronic ID card, the State Portal *http://www.eesti.ee* and the state information system as well as security issues.

In order to promote the ID card, a national marketing campaign will be carried out aimed at the current and potential users of e-services. It is planned to increase the number of e-users of the ID card and promote the card. The campaign will comprise TV and Internet commercials and also outdoor media solutions and it will be conducted in Estonian and Russian. In addition, information days will be organised for residents as well as public sector and media representatives, and information booklets and training materials on the use of the ID card will be made.

The purpose of introducing the *eesti.ee* portal is to raise users' awareness of the existence and possibilities of this portal through a marketing and communication campaign. The target group of this portal includes the stakeholders engaged in the development of e-services as well as consumers, opinion leaders and media representatives. The campaign will involve different ad-

vertising channels, TV and radio programmes.

The opportunities provided by the state information system will be introduced, above all, to policy-makers, officials, entrepreneurs and opinion leaders to increase their awareness of public e-services provided by the state and the entire information system. This, in turn, will result in better service provision for people. To this end, an autumn school will be organised to strengthen co-operation between public sector decision-makers and IT specialists. Furthermore, a partnership day will be held for public sector IT managers and private sector IT developers, as well as an information day for database developers and administrators. The planned activities include creating a public photo bank to visually illustrate the e-services developed and used in Estonia.

Communication about security issues should improve Estonian residents' knowledge of the possible dangers and cyber risks as well as related protective measures. The marketing campaign will teach the public that secure computers contribute to a safer society and involve people in prevention activities.

The implementation of the programme for raising information society awareness will result in better awareness of society members of the fact that e-solutions make life easier and it is safe to use them.

In order to cope in the information society, new skills and know-how is necessary as this society is already a reality.

3.2. „Computer Protection 2009" helps us to increase security in the information society

In 2001, ten leading Estonian companies decided to co-operate and established a foundation called Look@World with an objective to guide Estonians to the Internet. In three years, the foundation fulfilled its ambitious goal to give basic computer and Internet training for 100,000 Estonians. In addition, 500 public Internet access points (PIAPs) were opened and an *e*School system (see Ch. 4.6.) that has gained both domestic and international reputation was developed.

By 2004, a critical mass of Estonians had been brought to the Internet and continuing the campaign would no longer have increased its efficiency. According to the statistics of the Estonian statistical office (Statistics Estonia), 53% of home PCs in Estonian households were connected to the Internet in 2007. 94% of enterprises used computers with 99% of them having Internet connection.

Thus, the more active part of the society already uses the Internet and the implementation of e-services is no longer hampered by limited Internet usage. However, concerns expressed about security risks had become louder. Indeed, the more services had moved to the Internet, the higher had become the risks. Risks against which the society could not yet secure itself; risks that had not yet been fully perceived.

The security of Internet banking is often associated solely with the application and efficiency of security measures taken by the bank. Internet banking, however, serves its purpose only in case there is a user at the other end of the bank line, who can access his money and other resources from his personal computer. It is also clear that usu-

ally people do not keep their computers under lock and key, guarded by gunmen or IT specialists. In fact, computers are an extremely easy prey for any mischievous person, who bothers to subordinate the computers of other users for his malicious intentions.

Thus, as long as each computer user does not secure his working environment himself, we cannot talk about secure e-services. This is exactly the message that IT specialists and opinion leaders began to spread among decision-makers.

At the same time, Estonia has good preconditions and possibilities to achieve success in the field of information security. Estonia has implemented an ID card that enables electronic identity and strong cryptography and is possessed by one million residents.

In 2006, the CEOs of two of the Estonia's leading commercial banks and two of the most important communications companies came together with an objective to launch a new framework programme for increasing security of the information society in Estonia. By May 2006, a co-operation agreement *Computer Protection 2009* was elaborated and signed, in addition to the leaders of Elion, SEB Eesti Ühispank, Hansapank and EMT, by the Secretary - General of the Ministry of Economic Affairs and Communications[1].

The agreement sets out a general direction – to jointly contribute to Internet security and to render support both in terms of financing and counselling. It was agreed that this would be done, among other things, by increasing the use of the ID card as the simplest and most secure self-protection tool and carrying out general awareness raising on Internet security.

The agreement provides an excellent basis for the launching of various projects.

For instance, a project targeted at the provision of ID card related training to the employees of organisations participating in the *Computer Protection 2009* was one of the first ones. The materials and methodology developed by the Look@World Foundation have already been used for the training of thousands of bank employees and the ultimate goal is to give basic information security skills to all civil servants and anyone working with the computer.

In addition, activities were launched to tackle the problem of risk-sensitive e-services being accessible with the code card. The code card has undoubtedly justified itself well in the past, but has, in terms of security, become slightly outdated by now. At the same time, no bank would want to alienate its customers from their habitual log-in methods by force – especially when the competitor still accepts the old-fashioned and familiar code card.

Thus, the participating banks in the *Computer Protection 2009* initiative co-operated to take their message – to use the ID card for logging in – to the Estonia Banking Association. Banks now unanimously move towards establishing the ID card as the primary personal identification tool in Internet banking.

Another important development was the launch of the ID card's younger brother – **Mobiil-ID** – by EMT in spring 2007. In case of Mobiil-ID certificates are not maintained on the ID card's chip, but on the SIM card of the mobile phone instead. Thus, in order to access a website one has to enter the PIN from the keyboard of his or her mobile. In addition, a joint procurement of ID card readers, organised at the initiative of banks, has to be mentioned here. As an outcome of the procurement, Estonian computer users can buy extremely inexpensive ID card readers, costing less than 5.75 euros.

[1] For more information about the objectives and essence of the co-operation agreement *Computer Protection 2009* see chapter 3.1 of "Information Technology in Public Administration of Estonia 2006" *http://www.riso.ee/en/pub/2006it/index.php*

In 2007, the initiative received a Deed of the Year prize awarded by the Estonian Association of Information and Telecommunications (ITL). On the picture (from left): Margus Püüa (Head of the State Information Systems Department; Ministry of Economic Affairs and Communications); Andres Käärik (Chairman of the Board of the Look@World Foundation); Tõnu Grünberg (Member of the Board, EMT) and Allan Martinson (investment banker).

The number of activities launched by the foundation has been on constant increase and by autumn 2007, the Look@World Foundation had six major project areas: widening the partner network, raising awareness, organising surveys, developing the ID card's service network, providing training, and developing ID card related technical readiness and infrastructure. The number of smaller sub-projects, however, amounts to nearly one hundred.

Several organisations have expressed willingness to join the *Computer Protection 2009* partnership and the initial budgetary limit of 60 million kroons set out in the initiative's co-operation agreement is likely to be surpassed several times. We can expect Estonia to become the most secure information society in the world by 2009, primarily due to the fast growth in security-related awareness and widespread take-up of the ID card's electronic functions.

Within the *Computer Protection 2009* initiative, a website has been developed for providing basic ID card training at *http://koolitus.id.ee* (as a conspectus currently only in Estonian with brief information in English and Russian). The website contains information on the purpose of the ID card, how to obtain it, how to find a suitable card reader, where to find relevant software and how to install it, how to authenticate oneself with the ID card, and how to give digital signature. Moreover, the portal provides information about the ID card's security and how to use it in the electronic environment. Practical examples are given about numerous operations related to the use of the ID card, such as changing its PIN codes, renewal and unblocking of certificates etc.

There are also blog-type websites at *http://www.arvutikaitse.ee* (in Estonian) and *http://www.infosecurity.ee* (in Rus-

sian), where computer users can obtain information about threats related to the Internet and find specific instructions on how to protect themselves. These blogs contain many links, articles and news, having involved thus into genuine signposts for finding one's way in the world of information security.

In October 2007, an Internet security initiative called *Veebivend* (The Web Brother) was launched in co-operation between Microsoft Estonia, Tiger Leap Foundation and the team leading the work of the information security portal at *http://www.arvutikaitse.ee*. The objective of the portal is to raise awareness among students, teachers and parents about Internet security and include it in the curriculum of general education schools.

First and foremost, awareness will be raised about threats related to the use of chat rooms and other social networks popular among young people. In addition, the aim of *Veebivend* is to teach the youth to recognise the mentioned threats and manage them. Furthermore, awareness raising activities are planned on the use of personal data and intellectual property.

Within the *Veebivend* initiative, a project competition will be launched, calling upon the youth to submit ideas on how to raise Internet security related awareness among their contemporaries. The objective of the competition is to involve the young and make them reflect on the subject.

3.3. Participatory democracy over the web

During a conference called *Democracy in the Information Society*, held in Estonia in summer 2006, inconsistency in the level of eParticipation in the public sector was brought out as one of the problems. At the leadership of the State Chancellery, an eParticipation and eDemocracy tool in the form of an engagement portal called *Teeme Koos* (Let's Do It Together) (*https://www.osale.ee*, only in Estonian) was launched.

The purpose of the engagement portal is to enable stakeholders - including enterprises and business organisations, Estonian residents, and citizen associations - to keep up with and have their say in public affairs.

Stakeholders can use the engagement portal for submitting their opinions on draft legislation elaborated by government agencies.

Having different parties expressing their opinions will enhance the transparency and openness of the decision-making process, improve the quality and social legitimacy of decisions, policies and legislation. From the standpoint of state agencies, the engagement portal will contribute to the formulation of more uniform engagement practices. Though the use of the engagement portal as a central discussion platform is still in its infancy, it is expected to consolidate draft policies and legislation from all government agencies. Thus, users of the portal will have comprehensive information as well as the opportunity to interactively communicate with government agencies. Civil servants will be obliged to publicly respond to all suggestions and give justifications for the acceptance or rejection of proposals.

Prior to its public launch, the portal was tested both by civil servants and representatives of different associations and their proposals were taken into account when improving the user-friendliness of the site. The Government, ministries as

well as several associations have the engagement portal's banner on their websites. In addition, there is a link to the portal in the *e*State Portal *http://www.riik.ee*.

In autumn 2007, a forum called *Engagement Academy* was organised for 160 participants, among them representatives of civil servants and different associations. At the end of 2007 and at the beginning of 2008, seminars were organised for non-governmental organisations and ministries to introduce the engagement portal. During the seminars training was given to those civil servants, who will be using the engagement portal in the ministries.

From August to November 2007, six consultations were held through the engagement portal with 25 opinions received. Thus, interest in participating in consultations has been noteworthy. There are approximately 1,700 visits per consultation. The portal has about 150 registered users, of whom most represent an organisation, e.g. a business or citizen association.

As the engagement portal was launched only in late summer of 2007, it is too early to evaluate its results. However, the feedback received so far allows to claim that it facilitates the dialogue between the state and the stakeholders. Public dialogue helps to impede corruption and increase public awareness about the work of government agencies on one hand and about the expectations of stakeholders on the other.

The objectives for 2008 include the take-up of the engagement portal by all ministries for public consultations on vital draft legislation and by at least 100 associations or organisations as regular users.

No such engagement environments have been developed before in Estonia and there are only a few similar examples in the world. By involving different stakeholders and containing strategic documents, the portal serves as a significant contribution to balanced policy formulation.

As the engagement portal has been launched recently, attention needs to be paid to ensuring its systematic use. Awareness about the portal has to be raised both among different organisations and citizens. In 2008, the development of the engagement portal will continue, also within the *e*Participation initiative[2] funded by the European Commission. In the framework of the project, the engagement portal will be linked to the participatory democracy portal TOM (Today I Decide)[3], which so far has functioned separately. As an outcome of the project, there will be a communication environment for government agencies and interest groups, where the latter can propose ideas, which would need the elaboration of new legislation or the amendment of the existing one. Secondly, the environment will enable to submit opinions on draft legislation initiated by the state. Thirdly, there will be a search function for finding existing legislation.

However, as the use of the engagement portal is advisable, not obligatory for the ministries, it will not replace the information system for co-ordinating draft legislation *eÕigus* (*e*Justice)[4]. *e*Justice does not enable giving feedback and contains information only about draft legislation currently being co-ordinated. As the engagement portal allows acquainting with plans still under elaboration as well as raising problems, those two tools can be combined.

In the development of the engagement portal, Estonia followed the example of the British government's *e*Petitions portal (*http://petitions.pm.gov.uk*) and the Finnish participatory democracy portals at *http://www.kansanvalta.fi* and *http://www.otakantaa.fi*.

[2] *http://ec.europa.eu/information_society/activities/egovernment_research/eparticipation/index_en.htm*

[3] TOM – see *https://www.eesti.ee/tom/ideas.py/avaleht* (only in Estonian; requires user authentication)

[4] *e*Õigus – see *http://eoigus.just.ee/* (in Estonian)

3.4. Estonia's second iVoting experience

Already for the second time in the history of voting in Estonia, the citizens with the right to vote could, in the elections of the *Riigikogu* (Parliament) in 2007, cast their vote over the Internet.

Though it is already two years since iVoting became possible for the first time, Estonia is still the only country, where voters can cast their vote at political elections over the Internet and the results of iVoting are equal to votes given on paper ballots. In terms of iVoting, Estonia can be considered a pioneer and there are several countries, which have already taken or are planning to take the same path.

There are different reasons why countries have not yet arrived at an implementation decision on iVoting: respect for deeply rooted election traditions, difficulties in making the political decision and amending the elections act, but also the lack of a secure nationwide Internet-based personal identification system.

Election principles are complied with also in iVoting

A decision to take elections to the Internet was made by the *Riigikogu* already in 2002. The objective was to give voters the opportunity to choose a suitable environment for making their election decision – either the traditional polling station or the Internet that has become a part and parcel of the modern information society. For the sake of clarity and simplicity, existing voting methods especially the advance polls taking place outside the polling station of one's residence, were taken into consideration in the elaboration of the Internet-based voting system. So, in both systems, iVoting and the traditional one it is checked that a person can have only one vote and its anonymity is guaranteed, i.e. though a vote travels between electoral committees either over the Internet or on paper, it is not possible to ascertain for whom a certain person has voted.

When proceeding amendments to the Election Act in the *Riigikogu* a couple of years ago, the provision according to which the Internet voter can change his vote caused the most opposition. At first glance this right may seem to be in contradiction with one of the key principles of elections, according to which every voter has only one vote. This principle, however, is not violated in iVoting, since it is guaranteed that only one vote – either that given over the Internet or the one submitted on the paper ballot – will be valid. The principle of re-voting was introduced because of the unique nature of iVoting – by casting his or her vote over the Internet the voter makes his choice in an environment, where his or her freedom of choice cannot be ensured. Giving the possibility to re-vote is an efficient and, in fact, the only way to avoid influencing the voter or buying votes.

ID card – the voter's key

There was another important decision made alongside the legalisation of iVoting five years ago. Namely, the voter must authenticate himself with nothing else than the ID card. In 2002, when the principles of iVoting were established, the issuing of ID cards had only begun and the number of card users was extremely limited. Nevertheless, it was decided that for the sake of security and autonomy, other widely used personal identification methods would be out of the question. As the ID card is a compulsory personal identification document for Estonian inhabitants and the number of card owners was expected to increase fast, the development of new electronic services has boosted. It can be said that iVoting is another way of implementing

the ID card, brought about by willingness to make more efficient use of the developed infrastructure.

At the same time, the requirement to use the ID card for authentication has limited the number of i-voters. The flood of questions to helplines during both the 2007 and 2005 elections showed that it was not so much the iVoting procedure, but first-time use of the ID card that caused problems to many people. This statement is supported by the conclusions of an international report, elaborated in co-operation with the Council of Europe and the Estonian National Electoral Committee in summer 2007[5], which stated that a person's computer skills and frequency of Internet use were among other important factors making people choose either iVoting or the traditional method.

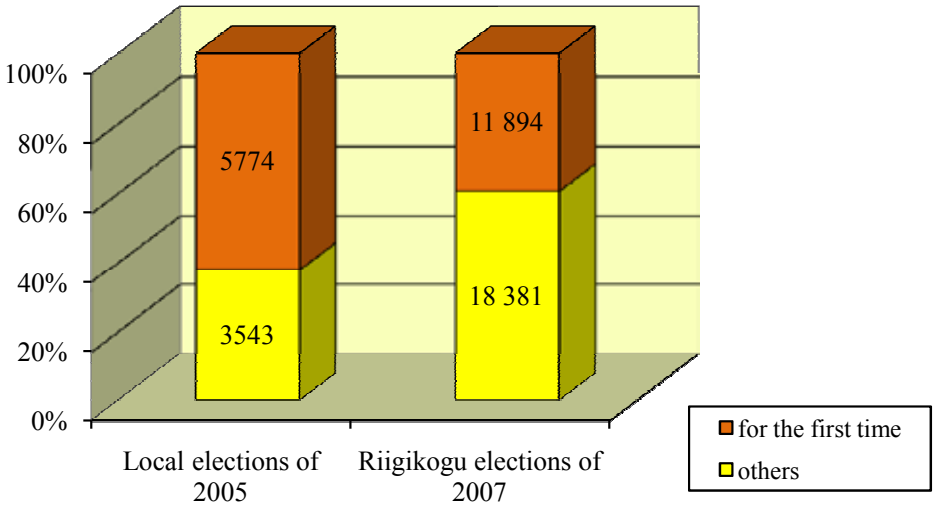


Figure 3.4.1. Share of i-voters having used the ID card for the first time

By March 2007, 80% of eligible voters had been issued the ID card and 3.4% of them used it for voting. The figure is not particularly high, but as the use of the ID card in other daily proceedings over the Internet will increase, the share of i-voters can also be expected to rise during the next elections.

Co-operation between the public and the private sector

The iVoting system serves as a good example of how different information systems, maintained both by the public and the private sector, complement each other and enable, for moderate costs, to create new values. The iVoting information system is linked with the Population Register for the compilation and renewal of the list of voters, and with the information system of the Estonian National Electoral Committee for the collection and publication of data on running for candidate and voting results. As iVoting is only possible with the ID card, the nationwide public key infrastructure and respective certification services for personal identification and digital signing play a significant role. The latter are provided by AS Sertifitseerimiskeskus (Certification Centre). In addition, the following state agencies are involved in iVoting: the Chancellery of the *Riigikogu* as the administrator of the iVoting central system, Estonian Informatics Centre (RIA) as the provider of the hosting service; Cybernetica AS as the software developer, and AS KPMG Baltics as an auditor.

[5] Report for the Council of Europe, Internet voting in the March 2007 Parliamentary Elections in Estonia, A.H. Trechsel etc, *http://www.eudo.eu/download/Report_Evoting_Estonia_for_the_CoE_2007.pdf*

The number of i-voters increased

In 2007, iVoting was used by 5.4% of all people having participated in elections, i.e. by 30,275 voters. Compared to the local government elections in 2005, the number of i-voters increased more than three times. While in 2005, iVoting was chosen for its novelty, in 2007 elections the main argument in favour of iVoting was the latter's convenience and speed. Increase in the use of the ID card's electronic functions during the recent years as well as wider availability of ID card readers also played a role.

	2005	2007
Total of i-votes	9,681	31,064
Repeated i-votes (more than one i-vote per voter)	364	789
Number of i-voters	**9,317**	**30,275**
Number of i-votes counted	9,287	30,243
I-votes cancelled by paper ballot	30	32
Percentage of i-votes among all votes given	0,9%	3,4%
Percentage of i-voters among all voters	1,9%	5,4%

Table 3.4.1. Number of i-voters in 2005 and 2007 elections

If the share of iVoting will increase also in future elections, the option of replacing some of the existing voting methods by iVoting might come into question, reducing thus election costs. As long as the organisation of paper-based elections will be maintained to the current extent, iVoting will not yield any economic benefits, but bring additional costs instead. It has to be kept in mind, however, that the transition to new voting methods must be smooth and gradual.

The organisational side of iVoting functioned efficiently at both elections. Neither have voters had any doubt in the trustworthiness of the novel voting method. Differently from the traditional paper-ballot based election system, no election complaints have been received about iVoting. Creation of trust is of utmost importance for iVoting and in order to maintain that, not only the organisers of elections, but also observers, for whom all election procedures are public, can contribute to that. As the Estonian iVoting was unique in the world, there were a number of foreign observers, including those from the OSCE, at the parliamentary elections of 2007, acquainting themselves, first and foremost, with the structure and organisation of work of the iVoting system.

Next steps

Pursuant to the Estonian electoral acts, iVoting is mandatory at all elections and referenda. There will be both local government and European Parliament elections in 2009, providing thus another opportunity to make use of iVoting.

Internet has turned out to be a suitable channel for increasing citizens' involvement in public decision-making processes. The application area of the iVoting system, too, could extend far beyond elections, as the system can be used for organising referenda of various scale, i.e. by parishes or towns. So far, iVoting has been used, outside elections, only in the framework of a poll in the city of Tallinn in 2005. Organisation of i-polls presumes, however, easy availability of the Internet and ID card readers all over Estonia and interest of voters in the take-up of the new voting method.

4. Developments related to ICT applications and user-friendly online services in the public sector

4.1. Improvements to central state portals and related application services

Year 2007 brought along a major change in the development of central state portals and related application services. Namely, the State Portal *http://www.eesti.ee* (in English only the main menu is available), which connects central state portals, was launched in October.

Actually, the State Portal is not entirely new, as it draws together the existing portals. It is developed and managed by the Estonian Informatics Centre. The portal offers practical information about the rights and obligations of permanent and temporary Estonian residents and public sector services. The interactive part of the portal provides for the use of e-services over a secure data exchange environment, the X-Road. The aim of the *eesti.ee* portal is to serve as a single access point for citizens to public sector e-services. For state and local government agencies, it offers the necessary infrastructure for providing various e-services to citizens and entrepreneurs.

The infrastructure services available (both as web-based services and online services of the X-Road) include the official e-mail address @*eesti.ee*, messaging calendar, location-based notification service and publication of online forms. In 2007, the infrastructure for mobile notification services was added.

The development of the portal has been funded form the EU structural funds under Measure 4.5: Information Society Development. The objective of this project is to increase the quality of public services through a uniform provision of such services and the effectiveness of the public sector through a central implementation of other similar functions.

Renewed content of the State Portal

The State Portal *eesti.ee* has been renewed so as to make it more user-friendly. The information content and services have been grouped into the views of the **Citizen**, the **Entrepreneur** and the **Official**, which all include personalised information and services depending on the role chosen by the user. Currently, the possibility of bringing the Official's view under the *e*Government portal *http://www.riik.ee* is under discussion. In addition, the State Portal features news about the Parliament, the President's Office and the Government as well as general public information, structured by institutions and topics.

The portal has advanced considerably both technologically and visually. The visual design supports the principles underlying the concept of the portal. In November 2007, the availability of the sub-sites of the *e*Government portal was assessed according to the methodology of the Web Content Accessibility Guidelines (WCAG). The shortcomings identified are currently being eliminated to achieve the conformance level Triple-A with respect to most of the content and services of the portal.

Development framework

The technical realisation of the State Portal is based on the technology designed for the project of *e*Government portal, meaning that the development framework of the portal involves simultaneously different developers. This framework

has been used also for the development of other information systems that are indirectly related to the State Portal's project. For years, it has been deployed as the technical platform of the Citizen's Portal. The more important latest supplements to the framework include the introduction of mobile ID based identification in May 2007, content management tools and an interface with the Document Exchange Centre. Further information about the technological solution and development framework of the State Portal is available on the web site of the Estonian Informatics Centre (*http://www.ria.ee/26993* – in Estonian only).

Apart from the Estonian Informatics Centre, the portal's development framework is used by the Road Administration (for the information systems on transport permits, job descriptions and road management), AS Andmevara (for the information system on providing childcare services) and various other institutions.

Application services within the State Portal's development framework

E-services of the Population Register

In 2007, new e-services of the Population Register were completed in co-operation with the Ministry of Internal Affairs and IT companies AS Andmevara and AS Datel: notice of residence; justified claim of the owner of the dwelling; order for the entry of vital record in the register; registration of child's birth; name query for the registration of birth; order for a duplicate certificate; query of blood relations; query of one's own personal data, and query of name statistics. These e-services function as X-Road queries to the Population Register.

The notice of residence service enables to change and enter data on residence in the Population Register. A person can submit a notice of residence concerning the residence of him or herself, his or her children or wards as well as other people living there. It is also possible to submit data on changes in the postal address. When ordering for the entry of vital record in the register, the vital record stored in the archive of a vital statistics office is entered in the Population Register. In the case of child birth it is possible to check the use statistics of the desired name from the Population Register or enquire about the suitability of the name from an official. Married parents can use the child birth registration service to register the birth and give a name to the child online. All applications must be signed digitally with an ID card or a mobile ID.

In addition, citizens can make queries about their own blood relations and personal data.

Service of transport permits

The State Portal allows to see and apply for transport permits for large-scale and/or heavy motor transport and co-ordinate the application with the Estonian Road Administration, the Road Administration of Northern Region and local road authorities.[1] Applications are processed and permits issued by authorised officials through the portal.

E-services of the police

The Police Board and AS Mebius are preparing a package of police e-services for citizens to speed up communication with the police and make it more convenient. This, however, does not rule out the possibility that, if necessary, the citizen must still go to a police station to ascertain the circumstances. The police

[1] The service of transport permits is available at *http://www.eesti.ee/portaal/velub.index* (in Estonian only).

will be providing the following services through the State Portal:

- reporting criminal offences;
- checking data on misdemeanours;
- filing objections in misdemeanour proceedings;
- submitting applications for administrative proceedings;
- submitting requests for information;
- submitting applications for permits for weapon acquisition and for changing weapons permits;
- submitting applications for entry into police service;
- submitting tips;
- managing documents submitted to the police;
- ordering for notification services.

These e-services are available as of February 2008.

Project management service[2]

The existing project management information system of the Estonian Informatics Centre was supplemented with the module of EU structural funds in 2007. The structural funds module of the project management information system is an electronic environment for the submission and proceeding of project applications for structural funds and related reporting in accordance with one of the priority action lines "Information society development" set out in the implementation plan for the development of economic environment. Applications may be submitted by constitutional institutions, government agencies and agencies under their administration, local governments, non-profit associations and foundations as well as legal persons in public law.

A tool for the application of ISKE

ISKE is a three-level baseline protection system for safeguarding the data processed in information systems (see also Chapter 2.3). The system was created primarily for the information systems of state and local governments and for securing related information assets. Moreover, also business companies can use ISKE for ensuring the security of their IT assets.

The tool for the application of ISKE is an interactive application guide for information system managers to help them choose necessary security measures for their information system depending on the nature of and non-functional requirements to the system.

Use statistics

Since September 2007, when the State Portal *eesti.ee* was renewed, the portal had around 108,000 visitors within two months. The majority of them (100,000) are from Estonia and the rest from altogether 96 countries – mainly from Finland, Sweden and the United States (see Figure 4.1.1).

[2] The service is available at *https://www.eesti.ee/projektijuhtimine* (in Estonian only).

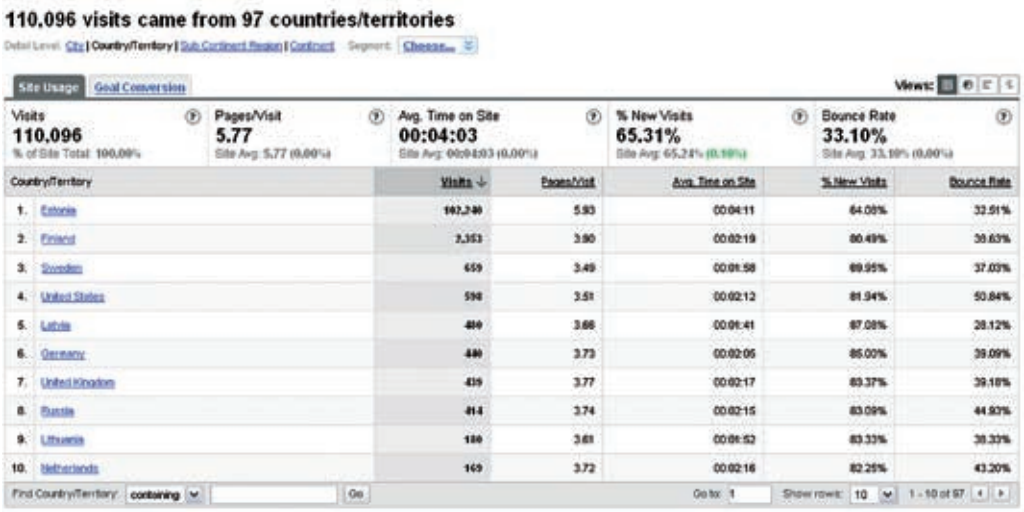


Figure 4.1.1. Top 10 countries of location of eesti.ee visitors

An average of 1,800 people visit the portal every day. The number of visitors is higher on working days from Monday to Thursday, reaching *ca* 2,000 people; at weekends there are 900 visitors on average. As the portal has been in use for a few months only, it is still too early to draw any conclusions but the use statistics shows an upward trend in terms of users. In the very first week after the launch, there were 2,095 visitors on the peak day. At the time of compiling this overview (November), there were 2,560 visits on the peak day (see Figure 4.1.2).

Figure 4.1.2. Number of visits to eesti.ee

As regards the **official e-mail system**,[3] which provides free e-mail addresses that can be also redirected, around 19,000 citizens and 17,000 enterprises had used it by mid-November.

Current and future developments

So far, the development of the State Portal project has been focused on advancing the designed functionality. The plans for 2008 include raising awareness of the services available and increasing the number of users as well as user-friendliness. The State Portal project is expected to be completed in August 2008. By that time, the services of the portal will be enhanced to the level set out in the initial project analysis and the presentation layer of the X-Road queries will be established. In the course of implementing the presentation layer of the X-Road

[3] The service is available at *https://www.eesti.ee/portaal/postisysteem.abi* (in Estonian only).

[4] The presentation layer is a component of the state information system architecture. It is the user interface for public sector e-services for entrepreneurs, officials, residents and other physical persons.

queries,[4] the X-Road's query portals for citizens, entrepreneurs and local governments will be integrated into the State Portal *eesti.ee*.

Another important line of work will be the creation of added value to other *e*Government projects with the help of the infrastructure services of the State Portal. To provide high-quality services to the citizens, state agencies are expected to offer their services in the *eesti.ee* portal and integrate the services of official e-mail, messaging calendar, location-based notification and publication of online forms and the infrastructure of mobile notification services with the existing as well as future information systems.

Moreover, also the *e*Government portal *http://www.riik.ee*, opera-ting since 1998, will be renewed in 2008. The *e*Government portal was established as a single access point for Estonian state agencies to the public information of constitutional institutions and state and local government agencies. The Russian and English versions of the portal give a comprehensive picture of Estonia's public structures also to the rest of the world.

4.2. Development of Estonian information systems to join the Schengen area

Estonia became a full member of the Schengen area on December 21, 2007. This concluded the long-standing preparatory work to extend the Schengen Convention and its advantages also to Estonia.

The Schengen Convention is primarily designed for the free movement of people within the Schengen area. In so doing, it is important to maintain security, which is ensured by the so-called compensatory measures. The abolishment of internal border controls and setting a common visa regime on the one hand, and international co-operation between the police, the border guard, the migration board and customs on the other, provide a balanced and secure environment for travelling and help to combat cross-border terrorism and organised crime.

The lack of checks at internal borders, as set out in the Schengen border rules, calls for fast and reliable exchange of data between the Schengen countries. To this end, the Schengen Information System (SIS) was set up. The structure and operations of the SIS have been specified in the Schengen Convention. The SIS consists of a technical support centre in Strasbourg, the central database (C.SIS) and national networks (N.SIS), which contain a copy of the database. Besides providing the national component of the SIS, every member country also sets up a so-called SIRENE (Supplementary Information Request at the National Entry) office. The aim of a SIRENE office is to provide missing or additional data about the country, if necessary, and co-ordinate cross-border co-operation (data exchange, cross-border monitoring and surveillance).

In Estonia, such office was set up at the Central Criminal Police. All the necessary information is transmitted to the SIS through the data processing system of the SIRENE office. The Estonian Police Board appointed the administration and development teams for E.SIS to ensure 24-hour monitoring and immediate recovery of the system in case of possible failures. The required system availability is set to 99.99%, which means that only 4 minutes of failures is allowed per a 30-day period.

Port of Tallinn, December 21, 2007 at 0:00.

In order to help new EU Member States to prepare for joining the Schengen area, the **Schengen Facility Programme** was launched for 2004–2006 and later extended to 2007[5].

The funds of this programme were allocated to the EU external border regions to help them comply with the Schengen requirements.

Estonia received 77 million euros from the European Commission and used it for financing altogether 78 projects. The majority of these projects comprised ICT infrastructure and information system developments necessary to strengthen the EU external border and border crossing procedures in accordance with the Schengen rules.

The preparations for joining the Schengen area involved various government agencies, such as the Ministry of Internal Affairs, the Border Guard Administration, the Police Board, the Central Criminal Police, the Citizenship and Migration Board, the Ministry of Internal Affairs, the Data Protection Inspectorate, the Tax and Customs Board, the Ministry of Justice, etc.

As regards ICT developments, the **Ministry of Internal Affairs** established a new operational radio communications network (ORC). The ORC network provides for operational co-operation between the police, the Border Guard, the Security Police, the Rescue Board and the Tax and Customs Board. Other authorities related to crisis management can be connected to that network too. The network complies with the requirements of the Schengen area. It covers the entire country and operates independently of other communication networks. Operational radio communications provides secure access to information servers and facilitates cross-border co-operation with the respective authorities in neighbour countries.

The **Central Criminal Police** conducted several ICT projects in 2007, including the development and introduction of the national central system for the Schengen information system and the establishment of an application that consists of high-availability software and hardware components and enables authorised Estonian institutions to

[5] The article draws from the information available on the web site of the Ministry of Internal Affairs concerning the results of the implementation of the Schengen Facility programme in Estonia.

make queries to the Schengen Information System.

The Estonian SIS (E.SIS) contains various information systems, each of which performs its own specific task in the process of compiling Estonian SIS-messages and sending queries to the SIS. One of the important criteria in the use of the SIS is data protection. At the national level, the exchange of data between authorised institutions and the E.SIS is carried out through the X-Road – the secure data exchange layer.

The initial action plans were aimed at joining the second-generation Schengen Information System (SIS II) and will be completed in 2009. However, in 2006 Portugal suggested that the new EU members could join the first-generation SIS and use a Portuguese software solution called SISone4All for that purpose. This allowed to extend the Schengen area already by the end of 2007. In December 2006, the interior ministers of nine countries (incl. Estonia) decided to join the Schengen area as soon as possible. The decision was followed by an intense period of work, which entailed a change of plan in the developments of the Estonian SIS and the Police Information System. At the same time, preparations are being made to join the SIS II.

The **Police Board** enhanced the infrastructure of the Police Information System; conducted a procurement for software licences and a hundred kits of *e*Police equipment for the police vehicles; trained the technical staff and users; updated 550 computer workplaces, and developed a software solution for police officers for making queries to the Schengen information system directly via the Police Information System.

The SIS contains data categories that have been in use in the Estonian police for several years: data on fugitives (Article 95 of the Schengen Convention); stolen and lost motor vehicles, documents, firearms etc. (Article 100); persons reported for being refused entry (Article 96), and persons who need to be located (Articles 97–99). The SIS extends access only to similar data of other member countries.

The compensatory measures of the Schengen agreement needed to be integrated in the daily activities of the police. To this end, it was necessary to identify and supplement the daily work processes of the police and build additional interfaces to the Police Information Systems POLIS[6], KAIRI[7], *e*Police[8], etc. The development of police information systems was facilitated by other aid programmes, such as EU structural funds.

The **Border Guard Administration** implemented various projects in 2007. For instance, the ICT infrastructure of the eastern border of Estonia and the data communication systems used for the protection of the eastern and sea border were significantly improved. In terms of the Schengen border rules, the Estonian-Russian border is an external border of the Schengen area. Other external borders of Estonia besides the territorial waters bordering the international sea area include the numerous ports and seven airports.

The accession to the Schengen area brought relatively few changes for the existing structure of the Border Guard Information System. Only the modules for making queries to the Schengen Information System had to be added. All third country (non-Schengen) citizens, and randomly also Schengen citizens, crossing the external border

[6] POLIS – information system of the Estonian police for the registration and proceeding of reports and offences.

[7] KAIRI – information system of the criminal and security police for the collection and processing of information, including queries to the information systems of other authorities.

[8] *e*Police – mobile workplace for making queries from the police patrol car about individuals and vehicles, including from the Schengen Information System.

points of the Schengen area must go through checkpoints where their passports and vehicles are checked against Estonian databases as well as the SIS. This enables the border guards to immediately identify persons who have been reported as not to be permitted entry or as fugitives within the Schengen territory.

In accordance with the Schengen rules, it is now also possible to make queries to the visa register by the number of visa to check people who enter the country with a visa. The earlier checking procedure involved the verification and registration of the visa, similar to the checking of passports, whereas now also the validity of visas is verified in real time via the central database of the Estonian visas. Upon checking, the border guard instantly receives verification of the (non)validity of the visa checked. If necessary, the border guard can also use the Schengen visa consultation system.

The new query-making procedures were integrated in the existing work environment so that it would be as user-friendly as possible and would not delay the operation of checkpoints.

Since the late spring of 2007, trains arriving from Russia undergo online border control. The border guard enters the train with a laptop and a passport scanner. The check is performed in real time via a WiFi network. Currently, even more compact (in the size of a notepad computer) mobile check equipment are being procured. The process of providing border guards' workplaces with automatic passport readers is also under way. The readers are tailored to read electronic biometric data from biometric passports.

The joining of the Schengen area set new requirements to the availability of the Border Guard Information System. In case the Border Guard is unable to make queries to the Schengen Information System, citizens of the third countries are not permitted to cross the Schengen border. In connection with that, in 2008 the central servers of the Border Guard Information System will be replaced, the software of the servers will be upgraded and the X-Road servers of the Border Guard as well as part of its network equipment and connections will be duplicated.

Checking of travel documents in a Moscow-Tallinn train at the Narva checkpoint

For the **Citizenship and Migration Board**, in terms of ICT, 2007 was the year of implementing changes in the Board's registers and infrastructures.

In autumn 2007, the new visa register was launched, which enables to acquire and compare biometric data (facial and fingerprint images) with the biometric information available. This provides for more definite identification of foreigners applying for a visa and thus reduces the possibility of issuing an Estonian visa to *persona non grata*.

With the implementation of the new visa register, a national electronic system for co-ordinating the issuance of visas was introduced. This is used by the internal security authorities to perform preliminary control of Estonian visa applicants.

One of the underlying principles of the Schengen Convention is the single visa policy. Thus, the Schengen area is often referred to as the Schengen visa area. The single visa policy means that citizens of third countries need only one visa for all the Schengen member countries, whereas these visas are issued according to common rules. The Schengen countries are also using a consultation system called VISION for issuing visas.

At the end of 2007, VISION was put to use in Estonia and is now used by internal security authorities to perform preliminary control of individuals who apply for a Schengen visa from another EU Member State.

In addition, the new visa register ensures Estonia's readiness for joining the common visa information system (VIS) of the EU.

When Estonia acceded to the Schengen area in December 2007, the Citizenship and Migration Board ensured readiness to submit data to the SIS on foreigners to whom Estonia has prohibited entry to the Schengen territory. The Board's information system transfers data to the SIS also on travel documents invalidated due to loss or theft as well as travel document forms.

At the beginning of 2008, the Board launched a single personal identification procedure, including the comparison of the biometric data of facial images. This was done to bring the quality of personal identification to a whole new level and introduce the systematic management of the identities of individuals in possession of identity documents and identified by the state.

The **Ministry of Foreign Affairs** allocated funds received from the Schengen Facility Programme to the updating of several foreign representations and consular posts. In addition, the Ministry enhanced data communication with foreign representations; provided them with security systems; obtained control equipment for documents and cash, as well as devices for recording fingerprints.

According to a press release of the Ministry of Internal Affairs, over two million queries to the SIS were made within four months, and 28 individuals with no permission for entry, 8 fugitives, 1 missing person and 19 requested vehicles were identified.

Other Schengen countries have located 6 persons requested in Estonia, 2 persons with no permission for entry to Estonia and 1 vehicle stolen here with the help of the Schengen Information System.

4.3. Company registration portal

The Company Registration Portal (CReP) of the Commercial Register is run by the Centre of Registers and Information Systems (RIK). Its main purpose is to make the life of the existing and future entrepreneurs easier and save them time spent on communicating with the Commercial Register. The portal provides for fast, convenient and easy registration of a company while retaining legal certainty. The key target group is the entrepreneurs, who wish to register a new company, submit company's annual report or change their information in the Commercial Register. Another major target group is the citizens, who wish to engage in entrepreneurship.

The European Commission's efforts to make the legal environment more competitive prompted various new initiatives in the Member States in 2006. As Member State's company law is largely confined to EU legislation, the simplification of the latter also eased the national company laws. Consequently, the Estonian Commercial Code was adapted so that instead of the former fifteen days, the entry of a company in the Commercial Register now takes maximum five days in the case of ordinary procedure. It is also possible to apply for expedited procedure, if the necessary business forms are completed and terms and conditions met.

The acceleration of the procedure largely owes to the systematic introduction of IT and electronic identification. This was done to set up a portal for entrepreneurs that would allow electronic use of data from the Commercial Register and other legal registers (which are public according to the law) while ensuring legal certainty of these data.

The amendments to the Commercial Code (incl. the possibility to register a company in an expedited procedure) entered into force on January 1, 2007. In parallel with the draft Act, the Company Registration Portal was launched, which serves as an electronic communication channel between entrepreneurs and courts' registration departments. Entrepreneurs can submit applications for entry and necessary additional documents, annual reports and changes in their contact data, supervisory board, list of auditors and area of activity.

It is also possible to apply for expedited procedure. In that case, the application for entry and related documents are reviewed within two hours. Expedited procedure may be requested to register private limited companies, general or limited partnerships or sole proprietorships as well as update the register data on sole proprietors, general or limited partnerships, public limited companies, commercial associations and subsidiaries. Expedited procedure does not extend to the registration of a public limited company.

Apart from registering a company, it is possible to submit annual reports through the portal. This may be done by members of the executive board, general partners, limited partners with the right of representation, heads of subsidiary, liquidators or trustees in bankruptcy. Annual reports can be submitted along with a confirmation of one of the above listed persons who can log in with an ID card or a mobile

ID or through an Internet bank. Once the report has been audited, the auditor can electronically confirm the report in the portal.

CReP entails security measures that provide the portal users with maximum safety. These measures include ID card or mobile ID based logging and digital signing. Applications for entry drawn up in the portal must be digitally signed and are legally equivalent to the earlier notarised applications for entry. The changing of contact data, list of board members or auditors and submission of annual reports requires authentication only.

With the creation of CReP, there is no more need to spend time on going to a notary to register a company. Notarised memorandums of association and articles of association have been replaced by standard articles of association in the portal. However, if necessary, changes can be made to the articles of association offered by the portal. Furthermore, it is no longer necessary to go to a bank office to pay the share capital and state fee. This can be done right in the portal via an Internet bank. Estonia is the first country where a company can be registered within such short time while retaining legal certainty. This has been achieved through the integration of legislative amendments, IT developments and changes in bureaucratic work arrangements.

The Company Registration Portal has been well received by users. In 2007, the first year of the portal, 29% of private limited companies were registered electronically. The record time of registration is nine minutes.

The first and foremost benefit of CReP is that it has helped entrepreneurs to considerably save on resources, as they can conduct most of the communication with the Commercial Register without having to leave their desk. Before the launch of the portal, company registration took quite a lot of time and paperwork. First, one had to wait for a visit to the notary and later complete numerous forms and take them to a court registration department where only paper documents were accepted. Then, all the information on the papers was manually entered into a computer, whereas a lot of time was spent on transferring the papers between different officials. All paper documents had to be stored in the document archives, which is why the archiving space in courts' registration departments had to be constantly enlarged. It should also be noted that CReP contributes to environmental sustainability, as it is no longer necessary to print and store all documents on paper. Before 2007, the registration process used to take up to fifteen days and involved a lot of paperwork, whereas now it takes maximum two hours and is fully electronic.

CReP has been designed so as to apply various automatic control mechanisms in the registration procedure to guarantee full compliance of the applications for entry or change of entry with all requirements. The portal does not enable to submit the application for entry if some important field is incomplete. The receipt of state fee and share capital is checked automatically. Just to give another example, if the founder of a company has indicated in the standard articles of association that the private limited company will have a supervisory board, then the portal will require that the board members be entered in the application for entry. The portal includes various other control mechanisms, which has sig-

nificantly reduced the workload of registering officials. That, in turn, helps to considerably spare time and effort, and money.

The Company Registration Portal is a sustainable and constantly developing application. In the future, CReP will serve as a single contact point for communication with the state. Another future perspective is to make the portal's content available also for non-residents. This will be possible once there will be appropriate solutions for the cross-border recognition of the digital signature. Estonia has every incentive to achieve that.

At the European Enterprise Awards 2007, a pan-European competition held in Portugal, the Company Registration Portal was acknowledged by the jury as one of the two best European projects aimed at reducing red tape.

Moreover, the portal was nominated from among the nineteen projects submitted to the preliminary line-up to represent Estonia as the *e*Government finalist in the World Summit Award 2007.

CReP was granted the Good Practice Label by the ePractice.eu portal and the right to use that label. CReP was highly appreciated both by the consortium of the competition and the visitors of ePractice.eu.

The portal is also available in English. Further information is available at *www.rik.ee/e-ariregister/ettevotjaportaal*.

4.4. Transforming the archival information system into a virtual research hall

The recent years have been revolutionary for the customer service of the National Archives of Estonia[9] (*http://www.ra.ee/?topic=25*). On one hand, services provided by the National Archives have undergone rapid development, but on the other hand, customer expectations have also been on constant rise. Ever-increasing possibilities for describing the archival material and making it easy to find and use have paved the way for relocating the archives' customer service from research hall to the web. The following is an overview of the three main stages of this development path.

Better searchability through the Archival Information System (AIS)

The first crucial step in the development of e-services provided by the National Archives was the creation and publication of the AIS web interface (*http://ais.ra.ee*; for the description in English see *http://ais.ra.ee/static/misonais_en.html*) at the end of 2004. AIS is the most important search tool for archive users, containing information about documents preserved in archives that form part of the National Archives. Although nowadays the possibility to make web-based enquiries is self-evident rather than ground-breaking, AIS stands out in the light of the existing practice. Earlier, users of AIS had to:

[9] **The National Archives of Estonia** (Rahvusarhiiv) is a government agency, which was founded on the basis of the Archives Act in 1999 by reorganizing the public archives services. The National Archives is a system of state owned public archives, including 13 archives in different locations of Estonia, and acts under the administration of director general, who resides in Tartu. The National Archives is a subordinate agency to the State Chancellery.

1) find an archival agency, which might hold materials for their research area;
2) go to that agency;
3) figure out, based on a printed reference book of archives funds or a card index, which archive creator may have the required information;
4) begin to work, line by line, on (often extremely voluminous) the paper-based registers of the respective archive creator trying to find archival records that could contain the sought-for information.

Now, everybody can find required documents fast and conveniently at home by entering search phrases in their home PC. Therefore, it is only natural that record keepers and experienced researchers understand the revolutionary nature of the AIS system better than general Internet users with little or no experience with archives. At the same time, these are namely the latter, from among whom archives have attracted many new grateful users as a result of the AIS information.

Furthermore, it has to be noted that as a central system AIS constitutes an important precondition for the creation and development of various additional e-services, i.e. for describing digitised materials, enabling specific web-based subscriptions, etc. Those developments will be elaborated upon later in the article.

By today, AIS contains information on nearly 5.2 million depository units or, in other words, the archival information system holds approximately 65% of all archival records. Day-to-day entering of information naturally continues, the next task being the improvement and unification of the already entered descriptions.

Better Access through Saaga (Digitised Family History Sources)

The possibility to search and find data on the web is an important, yet clearly only the first step towards more convenient customer service, as it enables to obtain information solely on the availability of data, not to search the information itself. In order to enable the latter, the Estonian Historical Archives launched, in May 2005, a digitalised family history collection *Saaga* (*http://www.eha.ee/saaga*), creating thus access to digital copies of its most widely used archival documents. Having quickly received a warm and enthusiastic reception from researchers, the importance of the solution for the customer service became notable in only one and a half year: while the number of users of the Historical Archives increased several times, the attendance of its research hall decreased by nearly one fourth. In addition to the ever increasing number of users and growing level of virtualisation of the customer service, improved preservation of original records is another important benefit of the implementation of *Saaga*.

By today, *Saaga* allows to scan through nearly 2.2 million digital pictures (2619 GB) with new data constantly being added. While the initial objective of *Saaga* was to consolidate all user copies of most important sources for genealogical research, researchers now can use *Saaga* for scanning parish registers of Lutheran and Orthodox churches, soul revision lists, wacka-books *(Wackenbücher)* and lists of draftees. Currently lacking yet most widely used family history sources will be entered in *Saaga* in 2008.

There are presently 27,000 registered users in *Saaga*, of whom approximately 70 are usually logged on simultaneously.

Since spring 2007, researchers have been able to use the technically improved test version of ***Saaga 2***,

where users can, for instance, bookmark references, open and save digital images in pdf-format, cut out and save details of images, change contrast, etc. The year 2008, too, will bring along significant innovations in terms of creating web-based access to digital user copies of records. Namely, beginning from 2008, researchers will be able to use a cross-archive **digital content portal** (DGP), which contains, in addition to Saaga, digitised sources meant for other target groups of the archive.

The main components of the DGP portal are the following:

1. the renewed *Saaga*;
2. a sample of most interesting and most widely used records from the collections of the National Archives;
3. the so-called *Estica* collection or a sample of most important sources about Estonia from foreign archives (initially from Latvia, Denmark and Russia);
4. images of: a) Baltic- German coats of arms and b) construction projects of buildings in Tartu city that already exist in the databases of the Estonian Historical Archives. The purpose is to provide information on visually eye-catching sources without knowing their description data;
5. digital images of maps preserved in the Historical Archives.

A glance into the future through Virtual Research Hall (VRH)

Although AIS and *Saaga* have created new possibilities for the use of archives, it is still not always easy for users to find their way in the multitude of information and services provided by different archives. Therefore, in terms of customer service, there is still room for development.

Considering the above-mentioned, the National Archives set itself a priority in 2007 to develop a universal customer service environment, which would develop further the already existing services and enable smooth communication, co-operation and information exchange in three directions: from archive to customer, from customer to archive and from customer to customer. The planned customer environment was called, pursuant to its objectives, **Virtual Research Hall** or **VRH**. VRH's detailed specification was completed in autumn 2007 and once the executor of the project will be chosen, the system will gradually be opened for its users within 2008.

In simple terms, VRH will serve as a gate through which users can enter the virtual archive. The structure of VRH will be three-dimensional, containing an archival view, a personal view, and a social view.

The following is a short overview of all planned components of these views:

1. Archival view

a) Institutional view: general information on what is VRH, for whom is it, what kind of information does it contain etc.;

b) Service view: paid services (notifications, copies, online store) and free services (FAQ, glossary, feedback);

c) Target group view: help texts aiming to guess visitors' objectives and offer solutions for them, typical problems and solutions thereof;

d) Content view: references to archive applications – information systems, databases, digitised materials, etc.;

e) Topical information view: news, press information, innovations in the VRH environment etc.

2. Personal view

a) User account: each user will be able to change the personal data he or she has submitted upon registration, change password and certain settings, view the

history of his or her subscriptions etc.;

b) Links: each user will be able to save links to specific VRH pages he or she considers important. A respective note will appear next to the link if the information on those pages has been updated;

c) Databases: each user will be able to make, based on a pre-determined standard and size limit, databases and share them with other users.

3. Social view

a) Forum: a communication environment, where VRH users can assist each other. Differently from questions that have been submitted through feedback, the archive will not assume obligation to respond to questions posed in the forum;

b) User databases: databases that have been created and published by users. The archive will not assume any responsibility for the accuracy of data in them.

As mentioned before, the programming of the VRH is a gradual process and not all above-mentioned functions will be implemented at once. Nevertheless, 2008 will be rather innovative year for the National Archives, representing a climax for several recent developments.

4.5. eNotary – an information system for notaries

Legal certainty – one of the fundamental principles of a modern democratic state – is ensured, among others, by notaries' offices. Notaries' offices came into being and were established so that governments could assign several of their functions, primarily maintaining legal peace by application of preventive methods, to an appropriate organisation in public law and its members. Therefore, the notary's work and its development go hand in hand with the development of a country. Centuries ago, governments were satisfied, when a notary was literate, while further development required legal knowledge and advisory skills and notaries were also trusted with the role of an arbitrator. Today when the modern state has reached electronic dimension, the notaries' offices performing the tasks assigned by the state also have to move in the same direction. The *e*Notary project described below is a step towards this goal.

The information system *e*Notary is computer software for the compilation of notarial deeds and simultaneously serving the basis for a digital archive, enabling communication with other registers, that guides and assists the notary upon obtaining and entering data necessary for the elaboration of a contract. For instance, by entering personal identification code (or the name of a person) into the box for the details of the party, *e*Notary finds the individual and completes, based on the data of the Population Register, the rest of the blank boxes – name, place of residence, data of the identification document, marital status. Upon the entry of a registered immovable number, *e*Notary finds and displays, based on the data of the electronic Land Register, other data related to the registered immovable – address, area, owner, encumbrances and restrictions, applications under procedure; finds and enables to add the plan of the registered immovable from the Land Cadastre's website (the page also contains information on potential restrictions related to the heritage conservation, nature conservation or other restrictions)

and the land use type data of the intended purpose of the cadastral unit; checks prohibitions on business and rights of representations from the Commercial Register etc.

The use of certain functions of the *e*Notary system is compulsory for notaries. At present, it is mandatory to keep the register of notarial acts and the register of deposits in *e*Notary as well as to use the system for forwarding applications, transactions and information to registers. As a next step, archiving of all documents subject to preservation in the digital notarial archive will be made mandatory.

What does *e*Notary do?

- Requires data about parties to a transaction and the object of a transaction from other registers;
- keeps the notary's calendar;
- registers notarial acts;
- helps the notary to compile notarial deeds;
- helps to calculate notary fees and state fees;
- draws up invoices for the payment of notary fees and pre-filled payment orders for the payment of state fees;
- helps the notary to keep account of the amounts of money deposited at the notary;
- sends data about a transaction to other national registers;
- saves the transaction together with the related data in the digital notarial archive;
- compiles notarial statistics;
- assists the notary's accountant.

How does *e*Notary work?

The preparation of contracts is easy, as the information system offers contract templates and necessary data comes from different registers with just a few mouse clicks. Once the contract has been signed, the notary makes a digital copy of the digitally signed contract and saves it in the digital archive. But the digital copy of the contract is not for the preservation in the archive only. The contracts in the digital archive or certain data thereof are forwarded electronically by the *e*Notary information system to other relevant registers – the land registry department, the registry department, the register of wills. In addition, a digital copy of the contract may be forwarded e.g. to state agencies having the right of pre-emption etc.

The work of the land registry department is considerably simplified, since information no longer needs to be entered from paper – it is automatically in an appropriate location in the land register information system and the paper register has ceased to exist. An electronic response is received from the land registry department or registration department regarding the registration of the contract, ensuring a ranking. The cross-usage of data increased the efficiency of working processes also in other state registers.

By today, 100% of registration applications are circulated in the electronic form.

Project

The *e*Notary project was initiated in 2004. It was commissioned by the Chamber of Notaries and executed by the Centre of Registers and Information Systems (RIK). The project organisation was formed of three parties, with co-ordinating and supervising tasks assigned to the Ministry of Justice. In addition to the steering group that consists of three parties, a working group was established. The latter comprises, in addition to the representatives of the Ministry of Justice and RIK, of notaries and other staff from several notary offices. The working group makes decisions

concerning the functionality of the system and solves problems that have occurred in the course of the development process. These were namely the enthusiasm and sense of duty of the members of the working group and development team that led the project to a successful completion. Constant feedback and proposals together with their rapid realisation have been of critical importance for the development of the project.

*e*Notary was implemented as a pilot project in 2006 in two notary offices and its first functionalities became obligatory for all notaries as from February 1, 2007. The goal of the project was to increase the efficiency of transactions for all parties, so everybody hoped to benefit from it. According to the estimations given by the representatives, this goal has been achieved.

Benefits of *e*Notary

The participants of the project made a joint effort to reach common goals: simplicity, speed and efficiency in performing their tasks. Notaries wished to obtain information from state registers and information systems as fast and simply as possible through a so-called single point of contact. The Ministry of Justice under the jurisdiction of which are the land registry department, the registry department of the Commercial Register and other institutions in the field of state administration and legal policy, wished to digitise paper applications and data exchange and increase the efficiency of business processes of registers. RIK as the administrator and developer of IT matters in the jurisdiction of the Ministry of Justice wished to make the administration of registers more efficient, simple, secure and innovative.

As a result of the co-operation, *e*Notary system was completed and interfaces were developed to the Land Register, Commercial Register and other information systems of the ministry. In addition to the jurisdiction of the Ministry of Justice, *e*Notary was interfaced with databases of the Ministry of Environment and other ministries.

The benefits of *e*Notary for citizens and notaries are best described in a letter from Ivi, an employee of a notary office and a member of the working group:

eNotary has improved the quality, speed and security of the customer service. The user – a notary or an employee of a notary office – has the possibility to quickly and conveniently obtain information about a particular person or object. In order to obtain the same kind of information earlier, the notary hade to surf on different websites and necessary data (name, address etc.) had to be entered on every single one of them individually. Besides, since most of the necessary websites were password-protected, one had to memorise quite a number of passwords. But you know those pencil pushers – who could learn all those hundreds and thousands passwords by heart and, thus, passwords were kept, neatly written on an A4 sheet in the upper drawer or stuck with a yellow post-it on the rim of the monitor or under the keyboard. In eNotary, however, authentication is ID card based and for search, one-off entry of personal identification code coupled with 6-7 clicks are sufficient to have all the necessary information for preparing a contract.

Is the person making a transaction at the notary really the one he or she claims to be; is the passport presented to the notary real or forged; is the passport still valid or stolen – there is nothing easier than to check it through eNotary. The validity of the client's passport, passport picture and sample of signature all come directly from the Citizenship and Migration Board and the Population Register and comparing them with the physiognomy of the customer and the document he or she has presented makes the life of forged

passport users and other rascals a hell. You are buying immovable, but how can you be sure that the seller is not ill-intentioned and has not just stepped out from another notary office, having already sold the immovable? Fortunately, the notary has eNotary, where he can check, practically in real-time, immediately before the conclusion of the contract for the purchase or sale of the immovable from the Land Register, whether any transactions have been performed with the given immovable or not.

In order to not to get down to technical details, it can be said that as fast as one can obtain information from relevant registers through eNotary, these registers also receive information on certified transactions from the eNotary system. All kinds of cover letters, envelopes and postage stamps have also fallen into oblivion. Thus, eNotary does the job of many postmen as well.

The citizen comes to the notary to register a succession. Instead of keeping him or her running between different state agencies and fetching necessary documents from the Vital Statistics Department, the notary receives the required information from the Population Register through eNotary. Within 30 seconds eNotary also enables to check whether a succession file has already been opened at some other notary and whether the bequeather has made a will or the succession will take place by law. There are no delays of several days in order to make enquiries to the register of wills. Neither is there any waste of notary's or citizen's time, but the customer can obtain operative information for his or her further steps.

Any member of the customer service staff can probably affirm that nothing human is alien to the customer – it sometimes happens that a child does not know his mother's or father's date of birth; that a man cannot recall the date of his wedding; that a person cannot recall the date on which he or she bought an immovable, and sometimes people do not even know in how many trading companies they hold shares. Earlier, obtaining data required for a transaction was a real headache for employees of notary offices and a rather brain-racking task for the customer. The customer often had to run between several agencies in order to reproduce his or her documents on paper. eNotary provides a solution to all those matters. As all the data contained in eNotary are secure and information received from the system corresponds to the data maintained in the registers, using eNotary often covers the information needs related to a transaction. Both the citizen and the notary win.

What does the future hold for *e*Notary?

- Parties to a transaction will be able to have a copy of the contract with legal effect also in the digital form (the legislation currently allows to issue first transcripts only on paper);
- each individual will be able to access, through the State Portal, contracts in the certification of which he or she has participated (for reading and copying only, not for changing);
- notary will become a single point of contact for entrepreneurs. Entrepreneurs will be able to manage, in addition to notarial deeds, all other affairs with the state, for instance submission of annual reports to the Commercial Register, through *e*Notary.

Summary

*e*Notary provides notaries support in acquiring information from databases serving as the basis for a contract, wording of the contract, forwarding the contract to various registers, and monitoring the implementation process of the contract. The information system

is compatible with and supports other registers while observing the information of the registers directed towards the electronic state format, processing of information and amending the information in registers. As a technological solution, *e*Notary also helps to ensure legal certainty.

The system's good functionality and user-friendliness were brought out in a recently organised survey also by the users of *e*Notary.

In October 2007, RIK organised a user satisfaction survey, according to which 70% of respondents work with *e*Notary 5-8 hours per day. Last experience with *e*Notary was perceived as positive by 84% of respondents.

The implementation of *e*Notary is compulsory, but its take-up is made gradual. Thanks to an in-depth preparatory work and testing, eNotary has been implemented rather smoothly. It is only natural that faults are found in the development of any information system, but as strength of the *e*Notary project, constructive co-operation between the following partners has to be mentioned: the Centre of Registers and Information Systems, *e*Notary working group, Chamber of Notaries, notaries, Ministry of Justice, and the land registry and registration department of the court.

The Estonian *e*Notary system is entirely unique in the world and has attracted considerable interest from several European countries as well as from the USA.

4.6. Internet-based information systems in education

In the academic year of 2006-2007, there were 601 general education schools, 48 vocational schools and 35 higher education institutions, including 11 universities, with altogether more than 260,000 students in Estonia.

The rapid development of IT affects the essence and quality of education, considerably changes expectations on the role of teachers at school, presumes the use of appropriate teaching methods and reconsideration of educational literature, especially the roles of the textbook and the workbook, in the light of this development.

Implementation of IT in the learning process and the organisation of that has been promoted, via several national and private initiatives and programmes, ever since the first years of the regained independence 1992-1993. Outside Estonia, the *Tiger Leap* programme (1997-2000)[10] for the development and implementation of ICT infrastructure and native language electronic learning materials in general and vocational education schools has probably become the most well-known. Also known are its follow-up programmes and development plans, such as *Tiger Leap Plus* (2001-2005) and *Learning Tiger* (2006-2009), as well as an ICT programme for higher education called *Tiger University* (2002-2004) with its follow-up programme *Tiger University*+ (2005-2008).

As a result of those programmes, the ICT infrastructure in Estonian schools has improved considerably: there are, on average, 17 students per computer intended for studying purposes, two teachers per teacher computer, and a computer for every principal. 99% of schools have

[10] See a collection "Tiger Leap 1997-2007", Tallinn, 2007, published on the 10th anniversary of the Tiger Leap Foundation: *http://www.tiigrihype.ee/static/files/6.tiigrihype2007ENG_standard.pdf*

broadband Internet and 98% of all computers in schools have Internet connection. Majority of schools maintain a website and many of them have their own information system or they are clients of some virtual learning environment or Learning Management System.

75% of Estonia's teachers have undergone a 40-hour ICT training *Arvuti Koolis* (Computer at School).

Schools have received more than 100 items of educational software, multimedia based handbooks and textbooks (of which 70 are native language originals). There is an **educational portal *Koolielu*** (School Life; for a short overview in English see: *http://www.koolielu.pages.php/0702*), several projects have been carried out to modernise manual training and technology lessons, etc.

This article focuses only on some of the most significant web-based Learning Management Systems and educational information systems in Estonia that have been implemented by many schools, teachers, students, parents and institutions operating in the field of education.

One of the most popular virtual learning environments used by over 50 general education schools is a **web-based learning environment called VIKO** (acronym for Virtuaalne Kool, i.e. Virtual School). VIKO, developed in view of the needs of general education schools, was created by the centre of education technology in the Tallinn University.

The learning environment allows teachers to make learning materials, study information and timetable accessible on the web for students. In addition, the environment offers communication possibilities in the form of forums. VIKO contains the following modules: Courses, Students, Lessons, Materials, and Forum. In addition, there is a support system for teachers introducing web-based learning process and development of study materials.

The use of VIKO is organised under the GNU GPL licence through the Estonian Educational and Research Network EENet. Since 2007, EENet offers the possibility to use VIKO on its server for free for all general education schools as well as for other qualified agencies and organisations. Expenses are covered by the Tiger Leap Foundation, which also supported the elaboration and development of VIKO.

VIKO will be developed further as a community-based freeware project by a team comprising the students of the Tallinn University and other voluntary developers.

EENet offers educational, cultural and science institutions the opportunity to use a **web-based learning management system IVA**, which allows to create, administer and use e-courses[11], and **a content management system for schools KooliPlone**, which allows to conveniently create, change and manage one's website. For example, the system has tools for drawing up and publishing a timetable, a virtual school newspaper, a warehouse for e-learning materials etc.

Since February 2008, EENet also provides a service called HAVIKE (acronym for Hariduse VirtuaalKeskkond, i.e. Virtual Environment for Education), which was developed in co-operation with the Tiger Leap Foundation. HAVIKE (*http://havike.eenet.ee* – only in Estonian) is a virtual server environment, which offers diverse selection of pre-installed software.

The main objectives of HAVIKE are the following:

- to offer a diverse selection of software in support of learning process;
- to offer and promote software that has been developed in Estonia or localised;

[11] E-course – a course carried out either partly or wholly in a web-based learning environment (usually in a Learning Management System)

- to offer an easy-to-use control panel with menus in order to ensure that non-specialists, too, would be able to install software;
- to make choosing the software a flexible process, i.e. EENet will add new software packages according to the needs of users and co-operation partners.

HAVIKE is free of charge for users in the field of education. Commercial use on HAVIKE is ruled out.

*e*School

*e*School is a simple and convenient Internet-based education information system that connects all parties involved in the learning process: principals, teachers, class teachers, students and parents.

Using *e*School, teachers can enter grades, reprimands to students, missed classes and homework in the class register and make them available both for students and parents. Class teachers can add reasons for missed classes and enter grades for diligence and behaviour.

Parents can have a quick overview of their child's grades, reprimands, missed classes and homework, while students can see their grades, missed classes and homework.

*e*School is currently used by more than 220 general education and vocational education schools all over Estonia. As the learning process differs by schools, the system is made to respond to each school's individual needs. Beginning from the system of symbols expressing the solidarity of a school till defining a school's system for grading and entering missed classes – each school can adjust *e*School to its own learning process and requirements.

The use of *e*School is managed by Koolitööde AS, which also has created and developed the system. The development of the system was supported by the Look@World Foundation. Differently from the afore-mentioned Learning Management Systems the use of which is free for schools, users of *e*School have to pay for the system. Since all schools share the same servers, their purchase and administration costs are also divided between them, making the price of the service acceptable for every school. To use *e*School, each school signs a service-level agreement, which sets out all requirements on the quality and availability of the service.

The main functions of eSchool are the following:

- class register, where the teacher enters grades, missed classes, late arrivals, reprimands to students, accounts of lessons, homework and tests;
- study book, which contains term, course, year, exam, and preliminary exam grades as well as grades for diligence and behaviour;
- missed classes register is a tool for the class teacher, who can enter reasons for missed classes and excuses. Missed classes are entered by the subject teacher in the class register and generated in the missed classes register automatically;
- student grade sheet (student diary) is a student-based excerpt of the class register, which contains the student's grades, missed classes, reprimands to the student, homework, and final grades;
- timetable;
- forums;
- contact data of students and parents (contact database);
- reports to the class teacher and principal that have been drawn up considering the daily reporting needs of a school.

To increase the efficiency and convenience of the service for students and parents, the developers have made it possible to use the service also via the mobile phone.

Through the mobile it is possible to obtain a quick overview of the time-

table, homework, current and term grades, reprimands to the student, missed classes and messages from the teacher. Just like in the computer. But parents and students always carry their mobile with them and it is always at hand.

Differently from the home PC, students can share their progress through the mobile with friends, parents or grandparents. All operative messages from the teacher or the school (i.e. cancellation of a lesson) can be accessed via the mobile.

The use of *e*School is person-based. Users are identified either with the ID card or identification codes of Internet banks. To activate the mobile service, a user who has logged into the *e*School environment enters his or her mobile number, which opens him a person-based view to *e*School data.

The first 30 days of using *e*School through the mobile are free of charge. Thereupon, the user has to buy either a monthly ticket in the value of 9 kroons (0.58 euros) or a day ticket for 1.5 kroons (0.1 euros).

Estonian Information System for Education (EHIS)

The development and use of EHIS have been covered in earlier publications of yearbooks (2004, 2005)[12].

EHIS is a web-based information system, which contains registers with data on students, teachers, infrastructure of educational institutions, curricula and final acts of all levels of educational institutions. In the development of the system the following principles were taken into account: data must be entered as effectively as possible exactly where they are generated; the whole system must be integrated with other state information systems; it is not the collection of data that constitutes the ultimate goal, but genesis of new knowledge and statistical information as a result of their analysis instead.

Having logged in either with the ID card or a password, authorised representatives of educational institutions enter data within five days after they have been generated or altered. Non-sensitive data is visible for all citizens. Every citizen can see, through the X-Road, data about himself or herself in the information system and authorised representatives and information systems of schools, school administrators, institutions and enterprises can use data within the limits of their rights.

Most of the data that has been consolidated in EHIS can be accessed with a personal user ID. One user in each educational institution has the administrator's rights and can add and remove user rights within his or her institution according to the decision of the leader of the institution. Each institution may have several EHIS users. Every user may have different rights in different subsystems. For instance, if the administrator gives access rights to an employee, who does not need to enter data, but only use them, it is recommended to render him or her solely the view-only right.

EHIS consists of five sub-registers:

- Sub-register of documents certifying education consolidates data about all final acts of general education. Educational institutions can use the register's data for printing out basic and upper secondary school graduation certificates and results reports. In addition, the register enables the issuing of duplicates of graduation certificates.
- Sub-register of teachers contains data about teachers. The register also holds information about vacancies that need to be filled. The data entered in the register helps to keep account of teachers' qualifications and forecast training needs.
- Sub-register of pupils, students and resident physicians con-

[12] See *http://www.riso.ee/en/publications/natpublications*

solidates data about pupils, students, external students and resident physicians. The data of the register is used, first and foremost, for forecasting state commissioned education and making education policy decisions.

- Sub-register of educational institutions consolidates data about educational institutions. The register reflects changes in the Estonian school network, i.e. about joining or closing of schools. This data serves as a basis for the analysis of the education system and organisation of educational life.
- Sub-register of curricula and education licences consolidates data about the curricula, programmes and education licences of educational institutions. Processing of new curricula and education licences in the register allows to revise applications faster and gives a good opportunity to inform the applicant of the state of affairs. The data of the register gives a good overview of learning opportunities throughout Estonia and are, thus, useful for all willing to continue their studies or upgrade their skills.

EHIS is in constant development. For instance, it is planned to be linked with the state examinations' information system, which is currently still a separate register. The Ministry of Education and Research initiated the EHIS project in 2002, the system was launched as a functioning information system in autumn 2004 and has since been considerably improved.

EHIS was developed with two objectives:

- to provide reality-reflecting information for all decision-making levels in the education system (Ministry of Education and Research, county governments, local governments and others in need of information) in order to make sound management decisions;
- to provide automatic access to personal data for all stakeholders needing it for the performance of their duties (Health Insurance Fund, Social Insurance Board etc).

Admissions Information System (SAIS)

SAIS (*https://www.sais.ee/index_en.html*) is a **complex e-service**, which enables electronic submission of applications over the Internet. After the submission of the application, SAIS also helps to organise the rest of the process up to the admission to a higher education institution, including the exchange of messages between the applicant and the higher education school, the acceptance or rejection of a study place etc.

There are currently 16 higher education institutions joined with SAIS.

As users can log onto the SAIS system through the State Portal *http://www.eesti.ee* either with the ID card or via Internet banks, the system does not require separate registration. Everybody, who logs in is therefore unambiguously identified and all the data and applications submitted via SAIS are equal to those presented on paper or by any other means.

SAIS is linked to other national databases (EHIS, state examinations' information system REIS, the Population Register) and in case the required data already exists in them, there is no need to prove past education, grades of state exams, previous higher education grades, etc. Even if the data does not exist in other registers a **pre-filled application form** can be submitted in SAIS, with which evidence is presented to one higher education school regarding the correctness of missing data (i.e. a previous higher education diploma). It is enough to present evidence to one higher education school, since once it is

entered in SAIS, and the data is confirmed by one higher education school, it is possible to submit the information with admissions applications to other higher education schools interchangeably with data received from state registers.

The fact that the applicant receives data on the offers of a study place electronically facilitates and accelerates the admissions process, as this allows the applicant also to **accept or reject the study place offer** through SAIS. If the applicant rejects the study place, it can be offered almost momentarily to the next applicant on the list.

SAIS is secure. After logging in, the entire information exchange between the applicant and the information system takes place in a secure encrypted X-Road data channel. It should also be emphasised that though SAIS allows to apply to several universities simultaneously, no university can see applications submitted to other universities.

SAIS belongs to the Ministry of Education and Research and is administered by the National Examination and Qualification Centre. The development of the system was funded within the framework of the *Tiger University* higher education support programme financed by the European Regional Development Fund (ERDF) measures for the "Development of the Information Society". Now, universities that have joined SAIS cover the system's development and administration costs itself proportionately to the number of applicants. The system was completed in 2005.

In the 16 universities that have joined SAIS, nearly 16,300 new students were accepted in 2007, amounting to 88% of all university entrants in Estonia. Approximately 10,000 or 62% of all entrants to schools having joined SAIS submitted their application through SAIS.

4.7. Development of e-services in Tallinn

The co-operation of central and local governments is centred on the resident of Estonia for whom we must ensure high-quality, readily available and flexible public services; or in the modern world – e-services.

The term ***e-service*** is often used in extremely different meanings and contexts, which may create a misleading impression as if this was something of a simple complement to already existing services. However, an e-service cannot be generated out of nowhere, i.e., on one hand, its generation is usually dependent either on the development of a new information system or the execution of development work for an already existing one. On the other hand, an e-service is based on the business process or the main activity process of a specific institution, where the provision of services, including public services, constitutes only a part of the output of the given process. Thus, in most cases, an e-service is not just a simple "superstructure" for the existing services, but has to be regarded, in terms of availability or delivery channels, as an entirely new form of service that needs a critical analysis of the whole service chain, introduction of logical changes as necessary, and, to a greater or lesser extent, changing the whole working process. Hence, as a rule, the development of e-services is neither simple nor inexpensive.

Most local governments in Estonia lack resources for the development and administration of information systems providing e-services. The solution can only lie in close co-op-

eration between state institutions and local government agencies (see also Chapter 1.2). In many cases, public services are provided for citizens through local governments, while at the same time, local governments can offer high-quality services only on the assumption that for the acquisition of source data, they use state registers or information systems (e.g. Population Register, Register of Construction Works etc.), which in turn are formed of data collected in the administrative areas of local governments.

As a positive example, one could mention the development of an information system called STAR (register of social services), launched in co-operation between the Ministry of Social Affairs and the city of Tallinn, that is expected to replace, in the nearest future, the outdated Social Register, and provide all local governments with the opportunity to organise and process data related to social welfare in the modern way.

Steps taken by the city of Tallinn for speeding up the development of the information society

The city of Tallinn provides more than 400 public services, including many e-services, for its residents. Information services are accessible on the website of Tallinn at: *http://www.tallinn.ee/eng* as well as through the State Portal at *http://www.eesti.ee.*

The first system providing e-services and simultaneously serving as a base system for many other services provided by the city was the **electronic document management system for administrative agencies of the city of Tallinn,** launched in 2001. Today, all documents circulated in the city's administrative agencies and all the city's legislation are processed only through this system. Naturally, paper documents have not yet ceased to exist, but new modern working methods are gaining ground.

All public documents can be accessed through the **Tallinn Legislation Register**; materials of City Council and City Government sessions, committee meetings, etc. are also available.

Registration of one's place of residence was the first fully electronic service, allowing to register one's place of residence in Tallinn by sending a digitally signed application together with accompanying documents to a relevant city official.

Of social benefits, **applying for the one-off childbirth allowance and birthday allowance** were realised as e-services in 2007. Respective e-applications can be submitted through the State Portal *http://www.eesti.ee*. The following is a short overview of the one-off childbirth allowance.

Applying for the one-off childbirth allowance in Tallinn

Pursuant to a regulation of the Tallinn City Council, the City Government pays, since 2003, to young parents the one-off childbirth allowance in the amount of five thousand kroons (approx. 320 euros). This benefit is considered to be one of the factors having positively influenced the birth rate in the city of Tallinn.

Up to the beginning of 2006, there were separate procedures for the registration of birth and applying for the childbirth allowance. The parent had to, after the registration of birth in the Vital Statistics Office, turn to the social welfare department of the city district government of his or her residence to apply for the childbirth allowance.

In order to make receiving the allowance as simple as possible, a procurement was organised for the development of a respective service. As an outcome, an information system was developed, enabling web-based automation of the procedure

of applying for, determining and paying the one-off childbirth allowance. By August 2007, a possibility to submit respective e-applications through the State Portal *http://www.eesti.ee* was completed in the framework of the same project.

Once the applicant has been authenticated, it will be checked against the data of the Population Register, whether he or she meets the requirements set out in the regulation – the relation between the child and the parent, the child cannot be older than six months, one of the parents must have lived in Tallinn for at least a year before the child was born, the child must be registered on the same address with the parent.

In case the applicant is eligible for the childbirth allowance, most data fields will be filled automatically with data from registers. The parent only needs to add his or her phone number and bank requisites. In addition, the applicant must enclose a medical certificate as set out in the regulation. Hopefully, in the future it will be possible to obtain the latter through an automatic enquiry from the *e*Health information system.

Then, all the parent has to do is to wait for the receipt of the benefit. The parent can follow, through the State Portal, changes in the status of the application (registered, being processed, being paid).

During the first three months after the launch of the service, over 40 young parents in Tallinn applied for and received the allowance through the State Portal *http://www.eesti.ee.*

Web map – local government's tool for communicating with residents and visitors

Since most of Estonia's citizens live in Tallinn and its neighbourhood and as most of them use the Internet, it is vital to convey information to them in the modern way – through a web map (*http://www.tallinn.ee/eng/g3455s31096*).

There has been an official web map on Tallinn's website since 2002. In the course of the time, the functionality of the map has been improved and additional data and thematic information layers have been added to it. Since autumn 2005, there is a trip planner on the map both for public transport and cars. In addition, there is a module for regional news, based on a database containing operative information concerning Tallinn, updated daily by managers of communication channels and officials issuing permissions for mining and street closures. All this information is displayed on the web map in the form of operative events. Based on the database, each citizen can subscribe (by e-mail) to operative information about events concerning the location he or she has defined on his/her map interface.

Getting the above-described data on a local government's web map is logical and necessary. Namely, the map makes it much more convenient to find an administrative agency providing a required service, nearest catering establishment or sports facility; to obtain information on services provided by the city; to learn, what company is responsible for cleaning one's home street and for refuse collection; what are the opening hours of the closest waste management centre, etc. Respective layers on the map open with just a few clicks in a couple of seconds, excluding thus the need to surf in the jungle of information provided on the websites of administrative agencies.

The public transport trip planner is one of the most popular information services on Tallinn's website, used by over 1000 people per day. In addition to public transport timetables, the trip planner enables to outline one's journey in the city from point A to point B. Modes of public transport together with relevant timetables are suggested and an optimal route to be covered is drawn on the city's digital map.

In addition to the city of Tallinn, the trip planner also covers the bus routes of the Harju county.

Public transport timetables can also be used without the web map, by choosing the following path on the website of Tallinn (*http://www.tallinn.ee/eng*): I need ⇨Transport ⇨ Timetables.

In the development of web map applications, open source software (OSS) was decided to be used as much as possible. Thus, the applications are based on architecture meeting the requirements of OpenGIS WMS (web map service), the map server runs on OSS MapServer/phpMacScript and the database server uses OSS PostgreSQL database. For the synchronisation of data from other data resources OSS MySQL database is used.

Below is a short overview of other most well-known e-services in Tallinn:

Mobile parking (mParking)

The mParking project, based on the use of the mobile phone, was launched in Tallinn on May 1, 2000 and constitutes one of the best innovative solutions in the management of life in the capital. mParking has sustained the test of time and by today, the solution is used, in addition to Tallinn, by five other Estonian towns. Furthermore, the service is to be launched in Antwerpen, Belgium.

In 2006, 54.1% of the total of parking revenues in Tallinn were received through the mParking solution.

ID ticket for public transport

The ID ticket is based on the possibility to use the Estonian ID card for electronic personal identification. The simplicity, convenience of use and other similar qualities have made the ID ticket extremely popular among the residents of Tallinn. Each day, the ID card is used by more than 100,000 public transport passengers in Tallinn. In 2006, more than 72% of public transport users in Tallinn had the ID ticket. More information about the ID ticket can be found at: *https://www.pilet.//* (partly in English).

In 2006, approximately 62% of the ticket income of the budget of Tallinn was received through the ID ticket system.

The above-given examples of the city's willingness to give its residents the best possibilities to communicate with the town and spend less time on this than years ago, constitute only a tiny part of the number of services to be transformed into electronic form in the coming years.

Information society related development projects in Tallinn have gained reputation both in the EU and elsewhere.

In 2007, a US-based think tank Intelligent Community Forum (ICF) recognised the development work of Tallinn in the implementation of information society projects by including Estonia in its *2007 Top Seven Intelligent Community* list. It is noteworthy that ICF did not refer to Tallinn as to a local government, but evaluated it as a community (state, local governments, enterprises).

In addition, in 2007 Tallinn received the mWatch prize, awarded by LivingLabs, for being the most innovative mobile region.

In conclusion, it is good to admit that in 2011 Tallinn will be one of the EU cultural capitals – a fact that serves both as recognition and responsibility at the same time.

5. Cyber war – a new phenomenon of the information society?

5.1. *Cyber attacks against Estonia* – overview and conclusions[1]

Background information

The cyber attacks against Estonia should be viewed in the general political context in April-May 2007. After the decision of the Estonian Government to relocate the World War II monument *Bronze Soldier* to a military cemetery, riots started on streets. A day later attacks began in the cyber room.

Overview of the cyber attacks

From 27th April to 18th May 2007 Estonia fell under a large-scale cyber attack. The cyber attacks were targeted at the websites of several government agencies and private companies, mail servers, DNS servers, and backbone routers. At peak moments, the amount of cyber traffic from outside Estonia targeting governmental institutions was 400 times higher of its normal rate. The period of the cyber attacks had two distinctly different phases.

Phase I – Emotional Response (27 – 29 April 2007)

During the first phase, most of the attacks were relatively simple Denial of Service (DoS) attacks against government organisations' web servers and Estonian news portals. At the beginning of the conflict different news portals went offline for a period of time. There were also a few cases of targeted web defacement attacks, e.g. the website of the party of the Estonian Prime Minister http://www.reform.ee was defaced during the first hours of the attacks.

Phase II – Main Attack (30 April – 18 May 2007)

During the second phase, much more sophisticated, massive (use of larger botnets) and co-ordinated attacks began. The most dangerous ones were Distributed Denial of Service (DDoS) attacks against some of the components of the critical information infrastructure – against the backbone routers of data communications network and DNS servers. Some of these DDoS attacks were successful for a very short time period – there were few less than 5 minutes' interruptions in the data communications backbone network.

Cyber attacks (mostly DDoS) also continued against government organisations' web servers. On 10th May 2007, DDoS attacks against two Estonian largest banks started. One of them was attacked for almost two days and Internet banking services were unavailable for 1.5 hours. For several days, restrictions were applied for accessing Internet banking services from other countries.

Several attacks were also made against the websites of media

1 The article was published in CIIP MERIDIAN Newsletter Vol. 2 No.1, January 2008. The author of the article is Toomas Viira, information security manager in the Estonian Informatics Centre

companies, e.g. DDoS against web servers and comment spam against media portals. There were periods, when media companies limited commenting in their portals and when it was not possible to access websites from other countries.

General assessment of the attacks

In general, there were two separate phases that were tied together by the same political event. The attacks came in waves, with the strongest ones co-ordinated near the politically significant dates. The more massive attack waves were made after 9th of May, when the Day of Victory in World War II is celebrated.

According to the information available, other objects of the critical information infrastructure were not attacked and their operations were not disturbed. The functioning of most important state registers, databases and information systems was not interrupted. The main objective of the politically motivated attacks was to bring down governmental websites by overloading these and at least try to damage the data communications network infrastructure.

In general, it is possible to conclude that while the first phase of the attacks was mainly an emotional and spontaneous response of simple hackers to the political events, more highly skilled cyber attack specialists were involved in the second phase. Many attacks were well co-ordinated, which usually requires better skills and more resources.

Who were the attackers?

In case of DDoS attacks, it is very difficult to discover the initiator of the attack and persons behind it. During the DDoS attacks mainly compromised home user computers (zombies) are used, which are managed by Command and Control Centre servers. From logs one can see only the IP addresses of home user computers from all over the world. In general, the distribution was very similar to the statistics of botnets distribution issued by several organisations (e.g. Symantec Internet Security Threat Report). It is very complicated to discover the real attacker – a person or a group, who initiates the attack, or a person, who would order such an attack.

Safeguards

During the cyber attacks we applied several safeguards and performed, among others, the following activities:

- We restricted access to governmental web servers from other countries. There are two types of websites – the first group comprises homepages that do not necessarily need to be accessible from other countries, while the other group consists of websites that have to be accessible from all over the world. We made huge efforts in order to guarantee the smooth running of most important websites. Access to less important websites was restricted from abroad. We did not have problems with providing web content to Estonian Internet users.
- We installed more specific filtering capabilities to be able to better fight against attacks.
- We increased the resources of web servers and the capability to serve more Internet users simultaneously.
- We increased several times the data transfer rate of the data communications network of government agencies, especially for foreign connections.
- Efforts made by Estonian ISPs and CERT-EE to fight against the attacks were noteworthy and CERT-EE worked in partnership with other CERT teams worldwide.

Conclusions

1. The cyber attacks against Estonia should be viewed in the general political context in April-May 2007.
2. Despite the enormously increased traffic in the data communications network, no significant damage was caused to the critical information infrastructure of Estonia.
3. The cyber attacks against Estonia posed a limited risk to the security of different IT systems. However, without applying crucial security safeguards the situation could have turned out more critical. Had the downtime of several services been longer, the consequences could have been very serious.
4. The cyber attacks did affect, on a limited scale, some of the operations of governmental institutions through the unavailability of web pages and disturbances in the functioning of some mail servers.
5. The effect of the cyber attacks on the everyday life of people was limited. For the general public, attacks against the banks were the most perceivable (over 95% of all bank transactions in Estonia are done online). The attacks also caused temporary problems for people abroad, when they were not able to access Estonian media portals.
6. The Estonian Government's strong political statements and actions on the cyber attacks brought the issue to the wider political arena and made the international community to pay more attention to issues related to network security and threats posed by cyber attacks in general.

General conclusions and suggestions

7. The Internet will be a perfect battlefield of the 21st century. Countering cyber threats requires a significant increase of assets in terms of improving awareness, training, investments in technology, as well as advancing conceptual and doctrinal approaches.
8. Increased dependence on e-services, IT and the critical information infrastructure in general makes modern societies increasingly vulnerable.
9. It is quite simple and possible, with a small amount of resources (renting of a botnet is relatively cheap), to attack somebody in the Internet. More effective countermeasures against botnets and their usage during the attacks should be taken.
10. Politically motivated cyber attacks pose a challenge to governments, as cyber attackers attempt to destabilize the society.
11. As a result of effective political propaganda, a significant number of people could be motivated to launch a massive cyber attack almost instantly. Hence, it is possible to inflict serious damage to the critical information infrastructure even in case of *ad hoc* and amateur level attacks.
12. The usability of the existing political, diplomatic and legal framework is limited as it is difficult, if not impossible, to track down the origins of an attack. Dealing with cyber attacks is even more complicated as there is no common definition for the phenomenon.
13. Efficient response to cyber attacks requires pre-existing international arrangements between states and between states and its private entities, as well as rapid reaction.
14. It is vital to establish a commonly agreed legal definition of cyber warfare and other related items.

5.2. "Cyber war" and Estonia: legal aspects

Year 2007 was an extraordinary and exciting year for the Estonian ICT sector because of the cyber attacks targeted against Estonia in spring. At the first glance, the events in the cyber environment appeared to be much more peaceful compared to the street riots in Tallinn. Looking back now, we may say that the incidents in the Internet outpaced the unrest in the streets both in terms of volume and insecurity.

Background and terms

No other country in the world has experienced such large-scale cyber attacks as Estonia did in spring 2007. This was the first time in history when such attacks were aimed at an entire country and involved a variety of instruments, techniques and strategies in the service of a political battle. The attacks were especially harmful in the sense that they addressed a country famous for its dependence on information and communication technology.

This experience is difficult to define in legal terms, since it is not clear whether it should be treated under national or international law. The picture gets even more complex owing to the abundant use of such terms as "cyber war", "cyber terrorism" and "cyber blockade" by the Estonian media and politicians to describe the events back then. In that context, these terms rather have an emotional value, which however does not contribute to the legal analysis of the problem. Drawing parallels to the use of terms like "war" or "terrorism" in the law of national defence and international humanitarian law, it should be borne in mind that treating a situation as a military action calls for taking various national and international legal actions.

The main problem related to the 2007 attacks was the lack of sufficient regulation on cyber attacks and computer crimes. Neither was there any such global legal framework in place, as far as international and humanitarian law is concerned. The underlying reasons may well include differences in countries' development levels, lack of political will or the fact that the history has not seen anything like that before. Thus, the existence of a relevant regulatory framework would have belonged to the field of science fiction.

These attacks should, by no means, be considered merely as random and occasional computer crimes but clearly as co-ordinated activities. At the same time, there is no legal ground in the Estonian or international law to treat them as anything else but computer crimes, owing to the lack of necessary elements of criminal offence to qualify these activities as such by their nature, extent and purpose.

Legal effects of cyber crimes

The cyber attacks witnessed in 2007 caused several problems. On the one hand, it was difficult to identify the exact persons behind these attacks. On the other hand, it was difficult to qualify the offences because until March 2008 computer crimes used to be treated in Estonia as criminal offences against property, not against the state.

The possible solution was to amend the Penal Code and add the qualified elements of attacks against computers or computer systems, so as to be able to differentiate the cyber attacks targeting critical infrastructures from ordinary computer crimes. Here, it is important to understand that attacks against the state may significantly disturb the exercise of official authority or provision of public services. It is as harmful as terrorism ("act of terrorism" pursuant to Section 237 of the

Estonian Penal Code) and therefore calls for additional protection.

The existing gap in law and the need for a new regulation has been also on the international agenda.[2] However, the current position is that such a need does not really exist and that it would undermine the available cyber crime convention and its new potential members.

Available protective measures

As most cyber attacks take place via the Internet, the analysis of their implications must proceed from Internet service providers (ISP) and the responsibility they have to take with regard to their activities.

An analysis carried out by the Estonian Informatics Centre and CERT (Computer Emergency Response Team) revealed that factual co-operation between ISPs and service users worked very well in crisis situations. However, ISPs pointed out that there are actually no legal grounds for the transfer of data or closing of Internet points. Then again, it is not really a matter of implementing regulations but rather concluding private law contracts between ISPs, the state and other service users.

One possible solution to amend the legal framework is to regulate co-operation between ISPs and the state in crisis situations. For instance, ISPs would be obliged to give priority service to the critical infrastructure and take that into account in concluding contracts with ordinary customers. The issues to be addressed at the level of law-making include making the acquisition of equipment for analysing external channels and/or the availability of a national duplicate connection obligatory, as well as the preservation of data logs (in terms of volume and time).

Establishing requirements to the services of ISPs and ensuring compliance thereof; monitoring within the ISP's own network; analysis of attacks and underlying reasons, and other such issues to be addressed through special regulations for ISPs still call for supplementary situation and impact analysis.

Conclusion

Although the amendment and implementation of laws might seem easy at the national level, from the standpoint of international organisations the different regulations adopted in the Member States need not provide sufficient and co-ordinated protection in the case of cyber attacks. Moreover, it should be taken into account that legal solutions are first and foremost aimed at contemplating different interests and making fair decisions. Estonia's advantage here might be the conservative approach in deliberating the alternatives, on the one hand, and flexibility in finding solutions, on the other. Based on these two approaches, it has been decided to regulate as little as possible and as much as necessary.

By the end of March 2008, the Government should adopt a strategy for cyber security and the detailed implementation plan for the strategy, which includes proposals from legal experts on cyber protection for the elaboration of necessary legislation and changing IT policies. This involves a closer analysis of the attitudes of EU members towards adding a context of terrorism to certain crimes and towards other exceptions to the law in force that may affect fundamental rights yet safeguard the public security. Estonia will also continue to monitor legal developments related to cyber safety in other countries and at the EU level to take them into consideration, if possible, in Estonia's own law-making process.

[2] On November 11, 2001, the Council of Europe adopted the Convention on Cyber-crime. The Convention was opened for signing on November 23, 2001, in Budapest. On the very same day it was signed also by the Republic of Estonia among others. The Estonian Parliament ratified the Convention on February 12, 2003.

6. Surveys on the information society and ICT developments in Estonia

In 2007, various surveys of developments related to the information society, ICT market and applications were conducted in Estonia. The following gives a summary of the more important ones.

The Department of State Information Systems of the Ministry of Economic Affairs and Communications commissioned various analytical surveys: an *e*Track survey on the computer and Internet use of Estonian households; a survey of the use of ICT in Estonian enterprises; a survey of the use of and satisfaction with public sector e-services among residents, and an analysis of the digital divide in the society, focusing on information stratification and people who never or seldom use the Internet.

Computer and Internet usage in 2007

According to the *e*Track survey conducted by TNS Emor, 55% of Estonian households had a PC at home in November 2007 (year-on-year growth of 7%). The trend is that the number of PC owners increases primarily among larger households with children and among families with lower income.

66% of people aged 15 to 74 have used the Internet over the past six months, which marks a 7% growth year-on-year. Internet usage at home keeps growing, as the number of households with an Internet connection is also constantly rising (51% of Estonian households, i.e. every second family, has an Internet connection at home). 91% of households who have a PC also have an Internet connection. In autumn 2006, 80% of Internet users used it at home, and in autumn 2007 – as much as 86%.

The majority of computer and Internet users are regular users: 90% use the computer and 89% use the Internet at least once a week. Compared to other groups of residents, computer and Internet usage has increased more among people aged 35 to 49 and residents of South and Northeast Estonia and rural regions. The Internet is used more frequently by employees and students aged 15 to 34, residents of Tallinn, and people whose monthly income exceeds 6,000 kroons (over 380 euros) per household member.

48% of residents aged 15 to 74 are frequent users who use the Internet at least five days a week. Year-on-year, the number of frequent users has grown by nearly 62,000 people (standing at 43% in 2006). Frequent users account for 72% of all Internet users. It is noteworthy that 40% of people aged 15 to 74 use the Internet every day.

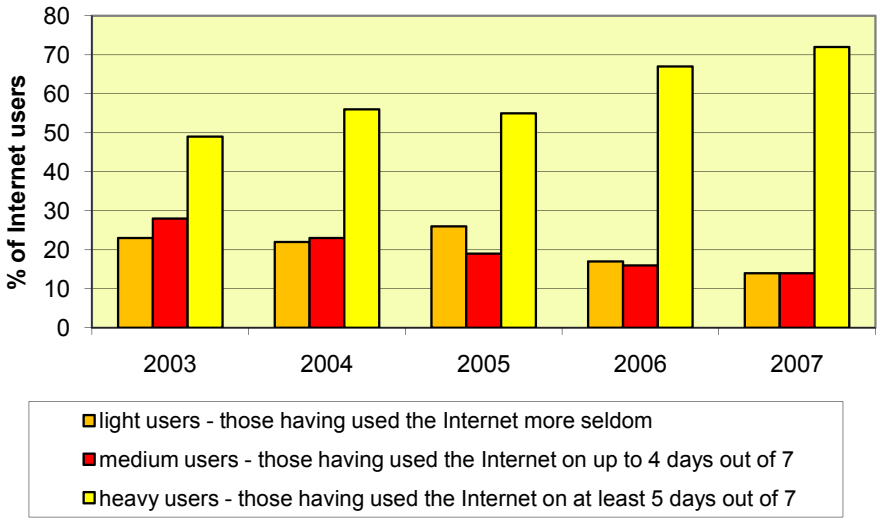


Figure 6.1. Segments of Internet users

There are a number of reasons for using the Internet frequently. The most popular activities are e-mail communication, Internet banking, information search and visiting Internet portals. Compared to autumn 2006, the use of search engines and reading Estonian Internet publications has gained popularity. In addition, Estonian people have gradually started to use the Internet for shopping and the number of those interested in e-commerce has risen over the year.

In connection with Internet usage, it is vital to acknowledge the related security risks. In relation to that, the Ministry of Economic Affairs and Communications asked TNS Emor to study – already for the third consecutive year – Estonians' awareness of security. Compared to autumn 2006, the share of residents with a firewall in their PC has risen, but the number of antivirus software users has remained unchanged (although the number of computers connected to the Internet has increased). Similar to 2006, in 2007 every fourth resident with an Internet connection experienced problems caused by computer viruses. The share of spam receivers has grown.

Use of ICT in Estonian enterprises

In spring 2007, TNS Emor conducted a phone survey to map the use of information and communication technology in Estonian enterprises. This was a regular customer survey for the Ministry of Economic Affairs and Communications to find out about the use of and satisfaction with public sector e-services provided to the corporate sector as well as related security issues. Comparable data is also available from 2005. The target group included Estonian enterprises that have at least one computer. Altogether 501 interviews were conducted.

71% of all companies surveyed had used e-services for communication with the state. The most popular e-services included search of information from public sector web sites (63%) and submission of documents (63%). Various registration operations related to business activities were somewhat less popular (39%). It should also be noted that the use of e-services has not grown substantially within the past two years.

Companies' satisfaction with the existing e-services is still high. In 2005, 22% of all companies who had used e-services were very satisfied and 71% were satisfied; in 2007, 25% were very satisfied and 65% were rather satisfied with the services. The number of companies who were uncertain of their judgment has slightly increased too.

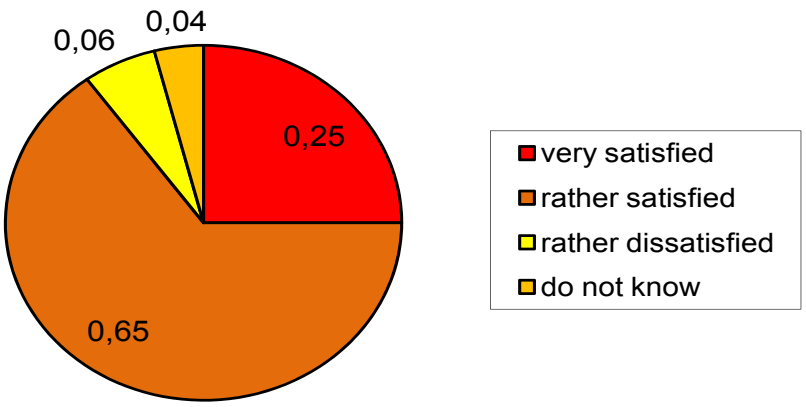


Figure 6.2. Satisfaction of businesses with public e-services (% of companies having used e-services in communication with the state)

The use of ID cards in enterprises has become much more popular. In 2005, only 2% of companies used the ID card for user identification and 1% for digital signing. The 2007 figures, however, were as high as 22% and 18%. Service providers and large companies tend to use the ID card more often.

In addition, the survey aimed to establish whether enterprises that are connected to the Internet had experienced any computer security problems within the prior three months. 87% of them claimed to not have had any security problems. Compared to 2005, the share of such companies has increased 29%. Some of the more common problems have been related to computer viruses and spyware. However, the share of companies that have an Internet connection and have experienced such problems has gone down from 36% to 9% in the case of viruses and from 13% to 3% in the case of spyware.

16% of companies connected to the Internet have done nothing to make the connection safer. 77% of them are using an antivirus software and 66% have installed a firewall.

The amount of spam, that is unwanted commercial mails, has not grown over the past two years. 78% of companies connected to the Internet are still receiving spam but they have started to fight it. 68% of companies who have received spam have taken adequate measures.

Use of and satisfaction with public sector e-services among residents

The Ministry of Economic Affairs and Communications also commissioned a survey to monitor the use of and satisfaction with public sector e-services among residents. The results of the survey serve as an input for the Implementation Plan for the Estonian Information Society Strategy. The information society development is facilitated by regular monitoring of various indicators, which helps to propose new action lines and revise the existing ones.

The survey of the use of and satisfaction with public sector e-services conducted by TNS Emor focused on two key issues. First, the general awareness, use and usefulness of public sector e-services. Second, citizens' awareness of and satisfaction with national portals and their functions.

In short, the survey revealed low awareness of public sector e-services and state portals, whereas the usability, simplicity and user-friendliness of e-services received high evaluations. 49% of Estonian residents aged 15 to 74 have used the Internet for communication with state or local government agencies – mostly to search information on web sites but also to download and submit electronic forms.

It was the first time when people's awareness of public sector e-services was examined. The awareness rate for all respondents was 43% and somewhat higher, 58%, for Internet users. The best known e-service appeared to be the *e*Tax-Board. Finance and taxation related e-services are also in general the most popular e-services – nearly two thirds (470,000) of Internet users have used them. Compared to 2006, the use of nearly all services has grown considerably, except for expression of opinion and participation in public debates with the state or government agencies: 24.6% of respondents had done that in 2006, and 20% in 2007.

The following table ranks more popular public sector online services in 2007.

Table 6.1. Use of e-services (% of users)

Service	2006	2007
Submitting tax return	75.5	95
Communicating with the school and teachers (see also Article 4.6)	40	89
Paying for public services or state fees through an Internet bank	70.9	79
Searching for medical information	54.2	72
Searching for geodetic and topographic information	46.8	55
Applying for identity documents (passport, ID card)	24.5	52
Enrolling in a school, university or course	36.1	51
Making a doctor's appointment	15.7	40
Communicating with the motor vehicle registration centre	21.7	40
eVoting / eElections	9.8	39
Applying for a European health insurance card	20.2	37
Participating in electronic courses or trainings	13.5	30
Communicating and consulting with doctors by e-mail	10.7	23
Ordering final examination results via SMS or to an e-mail address	9.7	21
Expressing opinion or participating in a public debate with the state or government agencies	24.6	20
Registering to state examinations	4.4	14
Applying for a supplementary benefits for medicinal products from the health insurance fund	3.1	13
Applying for family allowances or parental benefits	6.3	13
Applying for medical prescriptions	1.9	5

The fields were people expect more e-services from the state are similar to those pointed out in 2006. These include health care, taxation, communication with the police and search for work. However, as many as 56% of all respondents could not or did not point out any such fields.

People's satisfaction with available e-services is relatively high. 67% of those who had used one or another e-service, rated it with 4 or 5 points on a 5-point scale. At the same time, there are no differences across e-services in that respect. In general, the e-services available are considered useful, as they save time and money as well as provide quick answers and information. Furthermore, 53% of service users are satisfied or very satisfied with the findability of online services. It is pleasing to report that 80% of those who have used one or another e-service cannot name any unsatisfactory service.

Nearly the same trends apply to state portals: people are not that well aware of them but the existing users value their content and user-friendliness very highly. The most well known portals are *http://www.riigiteataja.ee* (State Gazette) and *http://www.riik.ee* (eGovernment portal) – 36% of residents aged 15 to 75 have heard about them. Every fourth of this age group also knows the State Portal *http://www.eesti.ee*. Awareness of different portals is considerably higher among In-

ternet users – 51% in the case of the two more popular portals mentioned above.

86% of users regard the use of e-services in the State Portal *http://www.eesti.ee* or via the data exchange layer X-Road as easy or very easy. Similar to 2006, checking one's own personal data in state registers and state examination results as well as applying for a European health insurance card were the most popular services also in 2007. People still prefer to access personal e-services in the State Portal or via the X-Road through Internet banks (74%); only 25% use ID cards for that matter.

To conclude, the main problem currently is people's low awareness of available e-services, even though there are plenty of them and users are generally very satisfied with them.

Survey of digital divide

The indicators used to measure information society developments (e.g. number of PC users or Internet connections at home) largely focus on technological aspects. Another important aspect is to bring the benefits of information society to everyone. Lack of access to computers and the Internet and the resulting digital illiteracy may lead to a society of the information rich and the information poor. This kind of digital divide arises from the uneven distribution of phones, PCs, Internet access and relevant skills among the population.

The Ministry of Economic Affairs and Communications asked the PRAXIS Centre of Policy Studies to examine the digital divide and the possible solutions to bridge the divide. The survey was completed by the end of 2007.

The first time when the social aspects related to the use of ICT were studied and relevant policy proposals made was in 2002, when the Open Estonian Foundation, the State Chancellery and the Look@World Foundation held a competition for conducting a survey of the social aspects of ICT. The survey focused on the non-users of the Internet and was carried out by TNS Emor and the PRAXIS Centre of Policy Studies. The survey of the digital divide in Estonia and possible solutions to bridge it revealed lack of motivation (respondents could not name any fields where they would personally benefit from Internet use) and insufficient skills and access (mostly because of limited financial resources) as the main reasons for not using the Internet.

A similar survey conducted five years later shows a significant change in attitudes: people who do not use the Internet or use it very seldom, do not believe the lack of necessary information to be the underlying reason. Quite the contrary – the Internet is regarded as an important source of information and vital for being "in the core of life".

Awareness of the use options of the Internet has grown substantially compared with five years ago. In 2002, many used to believe that computers and the Internet were only useful for children for doing schoolwork or for adults at work. Now, this understanding is rather exceptional and the non-users of the Internet realise that the Internet can potentially make their lives better.

The preliminary results of the 2007 survey highlight insufficient skills as the main reason for not using the Internet.

Survey of Estonian computer users' attitude towards software piracy

Estonia has been fighting software piracy already for years. Nevertheless, the use of illegal software has remained virtually at the same level over the past five years, constituting slightly more than half of entire software usage. To find out why this situation persists, the Estonian Commercial Software

Society commissioned a survey[1] from the market research company Turu-uuringute AS in spring 2007, so as to get a clear picture of computer and software use in Estonia. The survey sample included 1,008 people.

Results showed that the use of computers as well as the frequency of use decrease considerably with age. Namely, the share of computer users is close to maximum among the young (92% of the young aged 15 to 19 use the computer, 75% being daily users), whereas less than 50% of respondents aged over 50 and only 18% of people aged over 60 use the computer.

For 94% of the young (aged 15 to 19) surveyed, home is the primary place where they can use the computer. The secondary place for computer use is the school (58%). Surprisingly many use it when visiting acquaintances or relatives (41%).

The survey also indicated that people who use the computer at home, but not at work or school, much more often mention computers games in terms of software use (70%) and seldom any other type of software. Those who use the computer both at work and at home, on the other hand, brought games up more seldom (49%) and named considerably more other types of software. This confirms the hypothesis that home PC users are more oriented to entertainment.

However, it should also be noted that out of the different types of software, security programmes were outlined most frequently by those who use the computer only at home (76% against the 70% for games). Thus, the majority of home users are aware of security risks and protect their PCs (see also Table 6.2).

Table 6.2. Other software available in PCs besides the operation system

	Age (years)					
	15 to 19	20 to 29	30 to 39	40 to 49	50 to 59	60+
Games	63	67	73	52	53	50
Office software (e.g. word processing and spreadsheet programmes)	53	78	71	58	59	58
Special software (e.g. design, photo editing and accounting programmes)	54	59	58	56	45	44
Security programmes (e.g. anti-spyware and antivirus programmes)	72	91	84	80	77	73
Do not know	10	4	7	13	15	10

As regards the origin of software, nearly half of respondents obtained programmes (or at least some of them) along with the purchase of a computer. Another common way of receiving software is downloading from the Internet (42%). There is a clear tendency that the younger the respondents, the more often they acquire software from the Internet. For instance, among younger age groups (15 to 19 and 20 to 29 years old) this indicator exceeds the average by a third (56% vs 42%).

Considering the cross-usage of software distribution channels, people who have obtained software from the Internet (mainly younger respondents) appear to be either the most active software acquirers or just the most aware of various options, as they exceed the average level in terms of all channels.

[1] An English summary of the survey is available at *http://www.tarkvaraliit.ee/study2007en.pdf*.

However, respondents who have received software from service or maintenance points, have much more seldom obtained it also from somewhere else (compared to average).

Younger people install most of their software themselves, instead of going to a service or sales point (22% of the young aged 15 to 19 and 29% of those aged 20 to 29, while the average is 16%). Self-installers are also more common among men (28% of men and only 5% of women).

Attitude towards piracy

The results of the survey indicate a clear correlation between age and attitude towards piracy. Although the general attitude towards the use of illegal software is disapproving, there are significant differences across age groups. Young computer users tolerate software piracy much more often than older respondents. The survey results refer to 30 years of age as the borderline between the attitudes. It should also be noted that the share of those who do not wish to express their opinion has changed. The youngest age group (15 to 19 years) includes the most such respondents (22%). A fourth (26%) of the young accept software piracy, a third (33%) disapprove of it, whereas only a fifth (19%) deem it worthy of punishment.

Every fourth respondent (24%) does not consider legality important in the case of PCs; among younger respondents (20 to 29 years) as much as every third (34%) is of that opinion. Neither is it surprising that only a third of younger respondents regard the use of legal programmes important (22% of 15 to 19 year-olds and 21% of 20 to 29 year-olds vs the average of 32%). In terms of workplace computers, the differences are not that big. What is more, is that respondents themselves also think that illegal software is most common among the two youngest age groups.

All in all, the survey results confirmed that more attention should be paid to shaping the attitudes of the most active computer users – the young – towards software piracy.

Survey of the Estonian ICT sector in 2006

The above described surveys were conducted in 2007, whereas the following survey is based on the growth figures of the Estonian ICT sector for 2006.

Year 2006 was good news for the Estonian ICT sector, as both turnovers and profits increased. Nevertheless, some old issues remain on the agenda: the decreasing number of qualified labour force, the accompanying rise in wage costs and low profitability of IT companies.

Although there are approximately 2,000 ICT companies in Estonia, the 2006 survey is based on the data of the annual reports of 600 enterprises. So far, this has been the largest reference base used. The total turnover of this sample stood at 22.2 billion kroons (1.42 bn euros) and the number of employees at 9,500 in 2006.

However, the turnover of this sample cannot fully be attributed to the field of ICT, since various of these companies were engaged also in other fields of activity, such as the sales, logistics and transport of office equipment, domestic appliances, medical equipment and so on. Additional corrections arise because of the need to add the estimated turnover of those companies who have not submitted data and sole proprietors as well as deduct the double turnover of national distributors. Thus, the actual profit of the ICT sector in 2006 is approximately 20 billion kroons (1.28 bn euros).

In Estonia, only 6 major ICT companies out of the 2,000 get a piece of the pie, accounting for 52% of the total turnover and making 79% of the sector's total profit. The next

25 companies hold half of the rest of the turnover, i.e. 25%, whereas their share in profit is only about 8%. Considering 90% as the borderline for market shares, another 67 companies fit in with a 15% share in the turnover and 8% share in profit. The remaining 10% market share and 6% profit divides between 1,500 ICT companies.

Earlier, the turnover of telecoms used to form about 60% of the total turnover of the ICT sector. In 2006, that figure had declined to 50%. It is unfortunate to note that over 80% of the turnover still goes to the telecom sector. Although the turnovers of the IT and ICT sectors have levelled off, the profitability of IT is still too low to guarantee investments, product development and a breakthrough to external markets without having to include foreign capital.

Turning to the figures, IT companies earned 4.9% profit (less the income tax and divided by the turnover) and telecoms 22.0% in 2006 (in 2005, 5.3% and 19.8%, respectively). In absolute terms, the total profit of IT companies increased 14% year-on-year, but the growth is following a downward trend given the 21% increase in turnover. Moreover, also the profit margin of IT companies declines along with the growing turnover.

Software developers are relatively better off compared to other IT entrepreneurs, as they have managed to maintain around 10% profitability on average. The same can be said about various IT service providers. The margins of hardware sellers are going down all over the world. Only those who can provide some added value service are successful in their field.

The shortage of qualified labour has been on the agenda for a while now, whereas less and less new labour is expected to enter the market based on the demographic projections for the next ten years. The first indication of the ongoing market changes is the steep rise in labour costs, which is already undermining the competitiveness of Estonian companies.

The cost of labour has gone up at a similar rate in the whole ICT sector, but telecoms outdo IT companies also in that respect, as their turnovers and profits have been outpacing labour costs. At the same time, the year-on-year growth in labour costs of IT companies has reached as much as 33%, which is over two times higher than considered reasonable.

From a global perspective, the growing lack of labour might actually be useful, forcing companies to enhance effectiveness and engage in co-operation. Furthermore, ICT solutions can significantly support the implementation of structural changes needed in other sectors of the economy and the production of higher value added.

International information society surveys and Estonia's rankings

Information society developments are also examined in a number of annual international studies. One such study is the Global Information Technology Report of the World Economic Forum[2], which ranks countries by various IT related indices. Estonia ranked 20th in the Networked Readiness Index in 2007[3] (23d in 2006 and 25th in 2005). However, a highly questionable survey has been published by the Brown University in the US, placing Estonia at the same level with, for instance, Kyrgyzstan, Mongolia and Samoa in terms of IT.[4]

[2] *http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm*

[3] *http://www.weforum.org/pdf/gitr/rankings2007.pdf*

[4] *http://www.brown.edu/Administration/News_Bureau/2007-08/07-011.html*

As for more serious surveys, The User Challenge, Benchmarking the Supply of Online Public Services[5] ordered by the European Commission and conducted by Gapgemini should be mentioned.

According to the European Interoperability Framework, there are four stages of services: information, forms available online, forms completed online and web services. Earlier studies used four levels to assess public sector online services; in 2007, a fifth level – that of personalisation – was added. This was done primarily because of new technological advancements that enable to personalise e-services and make them more proactive.

The abovementioned survey, comprising the 27 EU countries as well as Iceland, Norway, Switzerland and Turkey, benchmarked the online sophistication of twenty public sector e-services at national level. Other indicators measured included the number of fully electronic services[6], user-centricity and assessment to national portals.

The average level of public sector online services in Europe is 76%, meaning that the majority of e-services available stand somewhere between forms completed online and web services. Austria is the most successful in that respect, followed by Malta and Slovenia. Estonia ranks eighth. The number of fully electronic services has gone up, year-on-year. In 2006, 50% of the 20 services assessed were fully electronic; in 2007, this figure stood at 58%. Again, Austria, Malta and Slovenia take the lead in that respect; Estonia ranks ninth. Apparently, the level of online sophistication of services is closely related to the number of services provided fully in an electronic environment.

As regards Estonia's position in the Capgemini's benchmark survey, 70% of our public sector services are fully electronic and their level of online sophistication reaches 87%. The level of services offered to citizens and entrepreneurs in Estonia exceeds Europe's average. The indicator of user-centricity and the assessment to the national portal *http://www.eesti.ee* are also above the average. This portal serves as the gateway for the majority of Estonian public sector services.

[5] *http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf*

[6] Services are considered fully electronic starting from stage four; that is, online services provided fully in an electronic environment.

7. Annex

7.1 IT contacts in public administration agencies

Agency	Contact person	Phone/mobile	E-mail
Office of the President	Ivo Vellend	(+372) 631 6238	Ivo.Vellend@vpk.ee
Chancellery of the Riigikogu	Raul Volter	(+372) 631 6400	raul.volter@riigikogu.ee
Chancellery of the Legal Chancellor	Kertti Päeva	(+372) 693 8434	kertti.paeva@oiguskantsler.ee
Public Prosecutor's Office	Raul Meriloo	(+372) 613 9413	raul.meriloo@prokuratuur.ee
Supreme Court	Jaak Sitska	(+372) 730 9047	jaak.sitska@nc.ee
State Audit Office	Markko-Raul Esop	(+372) 640 0794	markko-raul.esop@riigikontroll.ee
State Chancellery	Ülle Laur	(+372) 693 5803	ulle.laur@riigikantselei.ee

Ministries

Ministry of Education and Research	Jaanus Christoffel	(+372) 735 0172	jaanus.christoffel@hm.ee
Ministry of Justice	Kaili Katmann	(+372) 620 8179	kaili.katmann@just.ee
Ministry of Defence	Mihkel Tammet	(+372) 717 0189	mihkel.tammet@kmin.ee
Ministry of the Environment	Vahur Eenmaa	(+372) 626 2830	vahur.eenmaa@envir.ee
Ministry of Culture	Indrek Eensaar	(+372) 628 2280	indrek.eensaar@kul.ee
Ministry of Economic Affairs and Communications	Kalev Truusalu	(+372) 625 6363	kalev.truusalu@mkm.ee
Ministry of Agriculture	Jaanus Kuusler	(+372) 625 6111	jaanus.kuusler@agri.ee
Ministry of Finance	Sven Rea	(+372) 611 3070	sven.rea@fin.ee
Ministry of the Interior	Hannes Märtin	(+372) 612 5047	hannes.martin@siseministeerium.ee
Ministry of Social Affairs	Allan Poola	(+372) 626 9299	allan.poola@sm.ee
Ministry of Foreign Affairs	Malle Ling	(+372) 637 7330	malle.ling@mfa.ee

National boards

Agency	Contact person	Phone/mobile	E-mail
Security Police Board	Edgar Reindla	(+372) 612 1422	edgar@kapo.ee
Defence Resources Agency	Alari Alviste	(+372) 717 0708	alari.alviste@kra.ee
Citizenship and Migration Board	Agu Leinfeld	(+372) 612 6980	agu.leinfeld@mig.ee
Estonian Competition Authority	Ivo Jaama	(+372) 680 3963	ivo.jaama@konkurentsiamet.ee
Civil Aviation Administration	Anne-Ly Käi	(+372) 610 3582	anne-ly.kai@ecaa.ee
Land Board	Viljo Roolaht	(+372) 665 0650	viljo.roolaht@maaamet.ee
Road Administration	Andrus Kross	(+372) 611 9314	andrus.kross@mnt.ee
Tax and Customs Board	Erkki Erend	(+372) 630 3910	erkki.erend@emta.ee
National Heritage Board	Urve Russow	(+372) 640 3012	urve.russow@muinas.ee
Patent Office	Jaanus Kasper	(+372) 627 7915	jaanus.kasper@epa.ee
Border Guard Administration	Martti Allingu	(+372) 614 9089	marti.allingu@pv.ee
Police Board	Virgo Riisipapp	(+372) 612 3301	virgo.riispapp@pol.ee
Agricultural Registers and Information Board	Olaf Laurisson	(+372) 737 1230	olaf.laurisson@pria.ee
Rescue Board	Andres Selli	(+372) 628 2016	andres.selli@rescue.ee
Public Procurement Office	Toomas Laigna	(+372) 620 1845	toomas.laigna@rha.gov.ee
State Agency of Medicines	Ly Rootslane	(+372) 737 4140	ly.rootslane@sam.ee
Social Insurance Board	Allan Poola	(+372) 626 9299	allan.poola@sm.ee
Statistical Office	Allan Randlepp	(+372) 625 9339	allan.randlepp@stat.ee
Consumer Protection Board	Kristiina Vaksmaa	(+372) 620 1708	kristiina.vaksmaa@consumer.ee

Agency	Contact person	Phone/mobile	E-mail
Estonian Technical Surveillance Authority	Sander Leivo	(+372) 667 2026	sander.leivo@tja.ee
Health Care Board	Allan Poola	(+372) 626 9299	allan.poola@sm.ee
Labour Market Board	Allan Poola	(+372) 626 9299	allan.poola@sm.ee
Veterinary and Food Board	Reimo Roosileht	(+372) 605 1747	reimo.roosileht@vet.agri.ee
Maritime Administration	Alar Siht	(+372) 620 5580	alar.siht@vta.ee

Inspectorates/centres

Data Protection Inspectorate	Henri-Paul Ariste	(+372) 627 4135	henri@dp.gov.ee
Estonian Motor Vehicle Registration Centre	Aldo Tatter	(+372) 620 1324	aldo.tatter@ark.ee
National Examination and Qualification Centre	Aivar Ilves	(+372) 735 0599	aivar.ilves@ekk.edu.ee
Estonian Informatics Centre	Margus Kreinin	(+372) 663 0220	margus.kreinin@ria.ee
Estonian Environmental Information Centre	Raivo Vadi	(+372) 696 2232	raivo.vadi@kki.ee
Centre of Forest Protection and Silviculture	Heiki Kivits	(+372) 733 9377	heiki.kivits@metsad.ee
Centre of Registers and Information Systems	Marko Lehes	(+372) 620 8170	marko.lehes@just.ee
Plant Production Inspectorate	Alar Kess	(+372) 671 2696	alar.kess@plant.agri.ee
Health Protection Inspectorate	Maie Otsmann	(+372) 694 3540	maie.otsmann@tervisekaitse.ee
Labour Inspectorate	Allan Poola	(+372) 626 9299	allan.poola@sm.ee

County Governments

Agency	Contact person	Phone/mobile	E-mail
Harju County Government	Tarmo Lõo	(+372) 611 8562; (+372) 516 7640	tarmo.loo@mv.harju.ee
Hiiu County Government	Monika Paljasma	(+372) 463 6048; (+372) 506 8398	monika.paljasma@mv.hiiumaa.ee
Ida-Viru County Government	Enno Leem	(+372) 332 1255; (+372) 503 1974	enno.leem@ivmv.ee
Jõgeva County Government	Nevel Paju	(+372) 776 6311; (+372) 5348 3576	nevel.paju@jogevamv.ee
Järva County Government	Vambola Annilo	(+372) 385 9655; (+372) 557 3713	vambola.annilo@jarvamv.ee
Lääne County Government	Kaido Kivioja	(+372) 472 5625; (+372) 5559 7670	kaido.kivioja@lmv.ee
Lääne-Viru County Government	Uuno Eiber	(+372) 325 8019; (+372) 501 0384	uuno.eiber@l-virumv.ee
Pärnu County Government	Valdor Telve	(+372) 447 9723; (+372) 524 0491	valdor.telve@mv.parnu.ee
Põlva County Government	Siret Rammul	(+372) 799 8942	siret.rammul@polvamaa.ee
Rapla County Government	Jaanus Milistver	(+372) 484 1140; (+372) 529 8694	jaanus.milistver@raplamv.ee
Saare County Government	Raivo Vanem	(+372) 452 0517; (+372) 506 5650	rvanem@saare.ee
Tartu County Government	Indrek Sarapuu	(+372) 730 5238; (+372) 521 9414	indrek.sarapuu@tartumaa.ee
Valga County Government	Kalev Härk	(+372) 766 6150; (+372) 502 7768	kalev.hark@valgamv.ee
Viljandi County Government	Kaupo Kase	(+372) 433 0413; (+372) 515 2723	kaupo.kase@viljandimaa.ee
Võru County Government	Kalle Jõgeva	(+372) 786 8331	it@mv.werro.ee

7.2. Information society contacts in the public administration

Ministry of Economic Affairs and Communications, Department of State Information Systems (RISO)

Margus Püüa – Head of Department of State Information Systems	
Estonia's representative in the i2010 eGovernment expert group and the related sub-group on eGovernment economics.	*Phone:* (+372) 639 7640 *E-mail:* margus.pyya@riso.ee

Mait Heidelberg – Ministry's Adviser on IT matters	
Estonia's representative in the i2010 High Level Group and the Management Board of the EU information security agency ENISA; development of broadband; information society priority in the Structural Funds	*Phone:* (+372) 625 6410 *E-mail:* mait.heidelberg@mkm.ee

Uuno Vallner – Head of IT Infrastructure Division	
Estonia's representative in the IDABC Management Committee; development of IT Architecture and Interoperability Framework; chairman of the Estonian eIdentity working group	*Phone:* (+372) 639 7635 *E-mail:* uuno.vallner@riso.ee

Rein Kauber – Head of Analysis and Planning Division	
Elaboration of information society strategy implementation plans; budgetary matters in the field of IT; information society priority in the Structural Funds	*Phone:* (+372) 639 7645 *E-mail:* rein.kauber@riso.ee

Katrin Edasi – Executive Officer of the Analysis and Planning Division	
Budgetary matters in the field of IT; IT potential of public sector institutions; contracts	*Phone:* (+372) 639 7643 *E-mail:* katrin.edasi@riso.ee

Taavi Valdlo – Executive Officer of the Analysis and Planning Division	
IT standardisation; eBusiness; organisation of work of the Estonian eIdentity working group	*Phone:* (+372) 639 7644 *E-mail:* taavi.valdlo@riso.ee

Katrin Hänni – Executive Officer of the Information Society Division	
Web and e-services; participation in OECD; Estonia's representative in Safer Internet Action Plan Steering Committee and eGovernet working group; analysis and surveys in the field of information society	*Phone:* (+372) 639 7604 *E-mail:* katrin.hanni@riso.ee

Monika Saarmann – Executive Officer of the Information Society Division	
Estonia's representative in the CIP ICT Management Committee, i2010 sherpa group and PSI expert committee; general EU co-ordination in the field of information society; analysis and surveys in the field of information society; paperless document management	*Phone:* (+372) 639 7647 *E-mail:* monika.saarmann@riso.ee

Estonian Informatics Centre

Epp Joab – Director	
General matters	*Phone:* (+372) 693 8200 *E-mail:* epp.joab@ria.ee

Kalle Arula – Deputy Director	
Planning and realisation of IT development projects related to components in support of the state information system	*Phone:* (+372) 663 0232 *E-mail:* kalle.arula@ria.ee

Riho Oks – Adviser	
Co-ordination of co-operation between state agencies in the field of information society	*Phone:* (+372) 663 0290 *E-mail:* riho.oks@ria.ee

Reet Oorn – Adviser	
Issues related to the regulation of databases, protection of personal data and cyber protection	*Phone:* (+372) 663 0266 *E-mail:* reet.oorn@ria.ee

Katrin Pärgmäe – Communication Manager	
Press contact, co-ordination and organisation of EIC's awareness raising activities	*Phone:* (+372) 663 0233 *E-mail:* katrin.pargmae@ria.ee

Agne Kivisaar– Programme Manager	
Organisation and implementation of the programme "Raising awareness about the information society", elaboration of related action plans	*Phone:* (+372) 663 0293 *E-mail:* agne.kivisaar@ria.ee

Toomas Viira – Information Security Manager	
Development of ISKE (three-level baseline system for information systems) and counselling work on its implementation; Estonian National Liaison Officer for the EU information security agency ENISA	*Phone:* (+372) 663 0243 *E-mail:* toomas.viira@ria.ee

Hillar Aarelaid – Head of the Department for Handling Information Security Incidents (CERT Estonia)	
Management of CERT Estonia	*Phone:* (+372) 663 0251 *E-mail:* hillar.aarelaid@ria.ee

Margus Kreinin – Head of the Department of Infrastructure	
Development and administration of infrastructure services for the state data communications network	*Phone:* (+372) 663 0220 *E-mail:* margus.kreinin@ria.ee

Anneli Touart – Head of the Administration Department	
Ensuring the functioning of the data exchange layer X-Road, state portals www.eesti.ee and www.riik.ee, and administration system of state information systems	*Phone:* (+372) 663 0280 *E-mail:* anneli.touart@ria.ee

Aili Ilves – Product Manager	
Issues related to the administration system of the state information system (RIHA)	*Phone:* (+372) 663 0284 *E-mail:* aili.ilves@ria.ee

Jaak Liivik – Head of Department of Structural Funds	
Organisation of activities related to the EU Structural Funds in the field of information society	*Phone:* (+372) 663 0230 *E-mail:* jaak.liivik@ria.ee

Rauno Temmer – Area Manager	
Issues related to the development of the portal www.eesti.ee	*Phone:* (+372) 663 0231 *E-mail:* rauno.temmer@ria.ee

Ahto Kalja – Project Manager	
Issues related to the data exchange layer X-Road	*Phone:* (+372) 564 67205 *E-mail:* ahto.kalja@ria.ee

Other

Arvo Ott – Director of eGovernance Academy	
Development and analysis of the information society	*Phone:* (+372) 641 1313 *E-mail:* arvo.ott@ega.ee

Tarvi Martens – AS Sertifitseerimiskeskus, PKI Business Manager	
Estonia's representative in the i2010 eIdentity sub-group and ID-ABC information security expert group	*Phone:* (+372) 610 1896 *E-mail:* tarvi.martens@sk.ee

Kaja Kuivjõgi – Ministry of Social Affairs, Head of eHealth Department	
Issues related to eHealth	*Phone:* (+372) 626 9160 *E-mail:* kaja.kuivjogi@sm.ee

Jaak Anton – Ministry of Education and Research, Adviser on IT matters	
Issues related to eLearning	*Phone:* (+372) 735 0135 *E-mail:* jaak.anton@hm.ee

Vahur Eenmaa – Ministry of the Environment, Head of Information Systems Department	
Issues related to eEnvironment	*Phone:* (+372) 626 2830 *E-mail:* vahur.eenmaa@ekm.envir.ee

Indrek Eensaar – Ministry of Culture, Head of IT Department	
Issues related to digital cultural heritage	*Phone:* (+372) 628 2280 *E-mail:* indrek.eensaar@kul.ee

Kädi Riismaa – State Chancellery, Head of Document Management Department	
Issues related to digital document management and archiving	*Phone:* (+372) 693 5593 *E-mail:* kadi.riismaa@riigikantselei.ee

Jaak Tepandi – Tallinn Technical University, Professor of knowledge-based systems	
Issues related to the Estonian Information Security Interoperability Framework. Estonia's representative in the Nordic eDimension working group on IT security; alternative member of the ENISA Management Board	*Phone:* (+372) 502 9028 *E-mail:* jt@tepinfo.ee

Tarmo Pihl – Invent Baltics OÜ	
National contact point for CIP-ICT and eContent	*Phone:* (+372) 501 9568 *E-mail:* tarmo.pihl@invent.ee

7.3. Useful links

Portals

*e*State portal: *http://www.riik.ee/en/*

State Portal eesti.ee: *http://www.eesti.ee/eng/?style=2*

Directories, Search

Electronic "Riigi Teataja" (State Gazette) – *e*RT (legal acts): *https://www.riigiteataja.ee/ert/intr/en.htm*

Estonian Legal Language Centre (legislation in English): *http://www.legaltext.ee/indexen.htm*

Public Administration Agencies

Ministry of Economic Affairs and Communications: *http://www.mkm.ee/index.php?keel=en*

Department of State Information Systems: *http://www.riso.ee/en/*

State Chancellery: *http://www.riigikantselei.ee/?lang=en*

Estonian Tax and Customs Board: *http://www.emta.ee/?lang=en*

Estonian Land Board: *http://www.maaamet.ee/*

Estonian Data Protection Inspectorate: *http://www.dp.gov.ee/index.php?id=14*

Division of Electronic Communications of the Estonian Technical Surveillance Authority: *http://www.tja.ee/?id=12386*

State Agencies and Foundations

Estonian Informatics Centre: *http://www.ria.ee/index.php?lang=en*

Centre of Registers and Information Systems: *http://www.rik.ee/index.aw/set_lang_id=2*

Estonian Educational and Research Network: *http://www.eenet.ee/EENet/EENet_en*

Estonian Environment Information Centre: *http://www.keskkonnainfo.ee/english*

Estonian Information Technology Foundation: *http://www.eitsa.ee/?url=eitf*

Archimedes Foundation: *http://www.archimedes.ee/index.php?language=2*

Tiger Leap Foundation: *http://www.tiigrihype.ee/?setlang=eng*

ICT Organisations

Certification Centre (AS Sertifitseerimiskeskus): *http://www.sk.ee/pages.php/020302*

Passport and ID card: *http://www.pass.ee/index.php/pass/eng/id_card*

Use of ID cards: *http://www.id.ee/?lang=en*

*e*Governance Academy: *http://www.ega.ee /*

Estonian Information Technology Society: *http://www.eits.ee/index.php?section=ws_eits_eng*

Association of Estonian Information Technology and Telecommunication Companies: *http://www.itl.ee/english/general/index.asp*

IT College: *http://www.itcollege.ee/?url=overview*

Estonian *e*University: *http://www.e-uni.ee/index.php?main=120*