Estonian digital infrastructure

as featured in

WIRED The Atlantic BBC THE WALL STREET JOURNAL. WSJ Forbes

enter
e-estonia

Published by Practus Institute of Public Administration, 2018

Images: visitestonia.com

This report is designed using the Estonian Brand guidelines. Materials and quotes from e-estonia.com were used in the introductory part of the chapters.

For questions or comments please contact us on contact@practus.eu our visit www.practus.eu

PRACTUS INSTITUTE
OF PUBLIC ADMINISTRATION

Rubiks Digital

Pre-word

The story of the e-Estonia, the most advanced digital society in the world, dates back to the 1990s when the newly born country was looking for ways to catch up with the rest of the world, enhance its citizens' well-being and bring itself back to the world map. They started from education by bringing computers to every single school of Estonia.

This radical move enabled access to Internet and computers for every kid in the country which in return raised up a generation of tech-savvy youngster that, a decade later, came to build Skype, Transferwise, Pipedrive and other successful startup companies. Add to that, they also started building their own perfect digital nation.

Estonia is often considered a government that is working like a company and indeed with around 130 000 public sector employees, Estonia could fit well in the middle of the fortune 100 corporations list. However, with only 1,3 million customers (citizens) paying the bills of the government, the county is forced to be agile, cost-effective and offer its customers the best value for their money. With their new e-Residency program, they have even figured out how to expand their customer base across borders.

Learning from the Digital Society

In an effort to capture the essence of this digital society, we have put together an extensive report of all of the key technologies and innovations behind the Estonian digital infrastructure. Going beyond the marketing hype, we were aiming to give an unbiased overview of the current state of developments with a full range of systems backing Estonian cloud state.

This eBook is a great source of inspiration for any **corporation** or **government** looking into transformation, eager to implement digital technologies. This ebook is created to be shared openly with anyone interested in transformation, open innovation and the Estonian digital story.

What this report is not about

Although Estonia is famous for its startup scene considered to have the biggest number of startups per capita in the world, this research, however, is primarily focused on the digital infrastructure of the Estonian public sector - services offered to its citizens from the government.

Strong digital infrastructure offers exponential growth and new opportunities for future technologies and thus Estonia has created dozens of strategic development plans to enhance the digital developments even further. However, for most countries and many corporations, even the current platform offers plenty of inspiration and learning opportunities. Thus, in this report, we have tried to focus on the current state of the digital infrastructure, not the future vision or technologies that are not yet implemented.

Erik Ehasoo
Innovation Advisor,
Founder of Rubiks Digital

Table of Contents

introduction

Introduction

The Estonian dream is to have as little state as possible, but as much as is necessary. Thanks to e-solutions, communications with the state are fast and convenient for all, and the country is more effective as a result.

e-Estonia's success relies on a clever infrastructure that has made it possible to build a safe e-services ecosystem. An important part of this ecosystem is flexibility, the ability to integrate its different parts, while improving e-services and allowing government systems to grow.

14,000+ visits per day in State Portal

1,500+ services are used over X-Road in Estonia

99% of public services online 24/7

Siim Sikkut, the Deputy Secretary General for Communications and State Information Systems at the Ministry of Economic Affairs and Communications: "Our luck has been than we built up the right and proper digital service infrastructure very early on, starting from nationwide digital ID and the data exchange platform X-Road. These made the digitization of various fields from health to police to taxes to voting much easier, faster, more secure, and cost-effective as well.

No country in the world has the core shared service platforms like we do, with the ability to authenticate and sign anything digitally and in a fully secure way, or connect the entire government together to enable the easy exchange of data.

In addition, there are world-class innovative digital services in many fields. Based on digital solutions, our tax system is the most effective in world. It is so easy to start and administer companies as you can do that online. And so on. Having said, there is still more to do, especially as technology jumps forward and opens up new opportunities for digitization. Thus, we have to keep redesigning and approving our digital government all the time."

Principles of Estonian e-Governance

Decentralisation — There's no central database and every stakeholder, whether a government department, ministry, or business, gets to choose its own system.

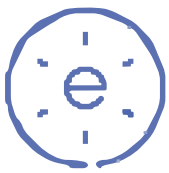
Integrity — All data exchanges, M2M communications, data at rest, and log files are, thanks to KSI blockchain technology, independent and fully accountable.

Interconnectivity — All system elements exchange data securely and work smoothly together.

Once-only — Data is collected only once by an institution, eliminating duplicated data and bureaucracy.

Open platform — Any institution may use the infrastructure and it works as an open source.

No legacy — Continuous legal change and organic improvement of the technology and law.



Transparency — Citizens have the right to see their personal information and check how it is used by the government via log files.

History of Estonian Digital Developments

1996

The **Tiger Leap** Program was launched by Toomas Hendrik Ilves, Jaak Aaviksoo and Lennart Georg Meri. The program was built on three pillars — computers and the Internet, basic teacher training and native-language electronic courseware for general education institutions.

1997

The Tiger Leap Foundation was established. The first step for the organisation was to provide all Estonian schools with **computers and internet access**. All schools were provided with computers by 2000 and by the year 2001, all schools were connected to the Internet as well.

2000

Estonia passed the **Digital Signatures Act** legalising digital signatures with ID-cards.

m-Parking was introduced allowing drivers to pay for parking using their mobile phones.

Estonian Government adopted its paperless **e-Cabinet** system - the Information System for Government Sessions.

The parliament of Estonia passed legislation declaring Internet access a basic **human right**.

2002

X-Road was started by the Estonian Information Technology Center. In 2003 the Estonian government passed a legislation that demanded that every government agency must be connected to the X-Road data exchange layer by the year 2005.

e-School, the most used e-service of all time, was launched. It provides an easy way for parents, teachers and children to collaborate and organise all needed information for teaching and learning.

2003

First version of the state portal **eesti.ee** was launched.

2005

Estonia became the first country in the world to hold nationwide elections through Internet, and in 2007, it used **i-Voting** in parliamentary elections'.

2007

e-Business register was launched allowing users to register companies online.

Mobile-ID was launched allowing people to use a mobile phone as a form of secure digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents, but has the added advantage of not requiring a card reader.

2007

Estonia fell under the first nationwide **cyber attack** during the 'Bronze Nights' protests.

Introducing of **e-Police** system that involves two main tools: a mobile workstation installed in each patrol car, and a positioning system that shows headquarters every officer's location and status.

2008

Estonian government started testing the **blockchain** technology. Since 2012, blockchain has been in operational use in Estonia's registries, such as national health, judicial, legislative, security and commercial code systems.

A nationwide **e-Health** system integrating data from Estonia's healthcare providers to create a common record every patient can access online.

2010

e-Prescription system was launched to replace paper medical prescriptions.

2013

The Information Technology Foundation for Education (HITSA) was founded through the merger of the Tiger Leap Foundation, Estonian Information Technology Foundation and The Estonian Education and Research Network EENet.

2014

Estonia became the first country to offer electronic residency to people from outside the country establishing the **e-Residency** program.

2015

Cooperation agreement between Estonia and **Finland** was signed to continue the development of X-Road in cooperation by having a shared code base. Later that year Finland started the production use of X-Road (called Palveluväylä in Finland).

2017

Estonia became the first European country to legalize and regulate **ride-sharing.**

Estonian government legalised testing **self-driving vehicles** on all national and local roads.


e-Governance
©Rasmus Jurkatam

e-Governance

e-Governance is a strategic choice for Estonia to improve the competitiveness of the state and increase the wellbeing of its people, while implementing hassle free governance.

Citizens can select e-solutions from among a range of public services at a time and place convenient to them, as 99% of public services are now available to citizens as e-services. In most cases there is no need to physically attend the agency providing the service.

Thanks to a safe, convenient and flexible digital ecosystem, Estonia has reached an unprecedented level of transparency in governance and built broad trust in its digital society. As a result, Estonia saves over 800 years of working time annually and has become a hassle-free environment for business and entrepreneurship.

The development of e-governance, in particular the development of public e-services and the take-up of these by individuals and companies, has been significant. Estonia leads the way in the take-up of electronic identity (eID) and the use of e-voting.[1] Electronic authentication and digital signatures enable paperless interactions and administration, which makes everyday business faster and more flexible for everybody.

In Estonia you can establish a company within less than 20 minutes and without leaving your home. In 2011, 98.2% of businesses submitted their annual accounts electronically. Both individuals and companies find that public e-services help them to save time and money, and are largely satisfied with the provision of public services. In 2012, the satisfaction rates were 76% and 67% among businesses and individuals respectively.[2]

The major strength of the national ICT policy so far has been the systematic development of the state information system and ensuring its security. The following principles of Estonian information policy have been built up and followed in the process: distributed service-oriented architecture, appropriate security of data and data exchange, web-based solutions, orientation towards e-services, and use of strong authentication tools.

The basic infrastructure of the Estonian state information system or, in other words, the service infrastructure (X-Road, public key infrastructure and eID, the document exchange centre, state portal eesti.ee) has allowed Estonia to improve public services with ICT solutions fast and flexibly. The distributed and interoperable state information system has created a good potential for Estonia to seize and benefit from the trend towards more and more devices and machines being connected to the computer network.

Estonia's progress has additionally been driven by promoting the free and open

[1] At the general elections of 2011, 24.3% of voters cast their votes electronically

[2] "Green Paper on the Organisation of Public Services" (2013)

internet at both national and international levels. According to reports issued by Freedom House[3], Estonia is at the forefront of the freedom and openness of the internet: in 2010—2012 Estonia ranked first in terms of internet freedom and in 2013 the country came second after (new entrant) Iceland.

The digital solutions of both the public and private sectors have captured international attention and created a reputation for Estonia as a leading e-country. This is an important reference for local ICT companies when entering foreign markets. In addition, Estonia has achieved the status of a reliable partner and esteemed opinion leader on matters concerning information society and ICT development in various international forums, including the EU and the Open Government Partnership.[4]

The State Portal eesti.ee

The State Portal "eesti.ee" is a common denominator for the state's closely integrated central portals, which draw together public sector information and services and provide an environment for central and local government agencies for the exchange of mobile, geo-information, X-Road and other application services. More specifically, the State Portal is an architectural component of the state information system that gives visual identity to the term eState.

The State Portal is an integral information and service space that encompasses the following portals: the institution-based information portal eGovernment (www.riik.ee), the topic-based Information Portal and an interactive portal for the provision of e-services called the Citizen Portal (www.eesti.ee). Thus, the user can easily find information or services he or she is interested in by navigating in institution, topic or service view. The first two of these portals can be used without any entry restrictions and are meant for use by all.

Accessing the Citizen Portal, however, requires authentication either with the national ID card or with internet banking codes of commercial banks. A citizen's right to use the portal is checked on the basis of data of the Population Register, while the right of representation of businesses is verified in the Commercial Register.

The information portal eGovernment was launched in 1998 as a common access point to the information of constitutional institutions and state and local government agencies. The portal offers information about Estonian state institutions in Estonian, Russian and English (the same languages are used for navigation in the Information Portal). The aim of the Information Portal is, first and foremost, to give practical information about the rights and obligations of individuals residing in Estonia as well as about services provided by Estonian state agencies (e.g. how to register a birth, apply for state benefits etc).

[3] "Freedom on the Net". http://www.freedomhouse.org/report/freedom-net/freedom-net-2012

[4] http://www.vm.ee/?q=node/17953

Moreover, the Information Portal contains relevant phone numbers, information about e-services and necessary forms, links to legislation and useful websites. The interactive Citizen Portal is an environment for the use of e-services through the middleware X-Road that enables secure exchange of data. The portal allows to proceed e-forms, make enquiries into different state databases, use e-services, and digitally sign documents.

Every ID card owner has the right to use the official e-mail address (Forename.Surname@eesti.ee), which serves as the state's main channel for communication with its citizens.

Through its solutions, the State Portal "eesti.ee" seeks to create an integral e-services environment, linking together services provided by the public, private and third sector and offering information and assistance in communication with the state. Services aimed at citizens, entrepreneurs and officials proceed from their actual roles and role-related needs, offering citizen, institution and position based approach. The target groups of the State Portal are not restricted to the three above-mentioned user groups, but cover all residents of the Republic of Estonia, public sector bodies, civil servants and officials, private companies, foreign citizens to be identified electronically, as well as the wider public.[5]

Digital ID

In Estonia, every person can provide digital signatures using their ID-card, Mobile-ID or Smart-ID, so they can safely identify themselves and use e-services.

350M digital signatures

67% use ID-card regularly

5 days per year saved with digital signatures

98% of Estonia's 1.3 million citizens has an ID card, which is much more than simply a legal photo ID. Technically, it is a mandatory national card with a chip that carries embedded files, and using 2048-bit public key encryption, it can function as definitive proof of ID in an electronic environment.

Functionally, the ID card provides digital access to all of Estonia's secure e-services,

5 https://www.ria.ee/public/publikatsioonid/State_portal.pdf

releasing a person from tedious red tape and making daily tasks faster and more comfortable whether we are talking about banking or business operations, signing documents or obtaining a digital medical prescription.

Some examples of how the ID-card is regularly used in Estonia:

- legal travel ID for Estonian citizens travelling within the EU
- national health insurance card
- as a driver's licence
- proof of identification when logging into bank accounts
- for digital signatures
- for i-Voting
- to check medical records, submit tax claims, etc.
- to use e-Prescriptions

Electronic personal identification with an ID-card (digi-ID) or Mobile-ID is better and more secure than identification with a username and password in several ways.

- Electronic authentication provides assurance regarding the fact that correct data is received from the ID-card, thereby decreasing the risk of users submitting false data for service providers.
- All service providers are able to directly and securely provide their services to all ID-card holders without prior registration.
- This is also convenient for the users as they need not remember various user names and passwords — the same card and PIN are valid for all services.

The most important area of application of the ID-card is to give digital signatures. Using digital signatures is convenient and fast as it allows one to electronically and without using any paper perform the actions for which one previously had to give a signature on paper. Digital signatures are also very secure as it cannot be forged and the correctness is thereby ensured.

Pursuant to the Digital Signatures Act, only signatures with a valid certificate as of the moment of giving the signature are valid. The validity of the certificate can be quickly and conveniently checked with the help of the validity verification service.

The cooperation of three components is required for giving online signatures with the ID-card:

- the signature plugin that is loaded in the user's browser and communicates with the ID-card;
- the web application providing the possibility for digital signature;
- DigiDocService (or DigiDoc libraries) with which the web application communicates during signing and with the main functions thereof being forming the signed container (DigiDoc container) and performing a query as to the validity information of the certificate of the signatory.[6]

[6] https://www.id.ee/

Mobile-ID

Mobile-ID allows people to use a mobile phone as a form of secure digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents but has the added advantage of not requiring a card reader.

The system is based on a special Mobile-ID SIM card, which the customer must request from the mobile phone operator. Private keys are stored on the mobile SIM card along with a small application delivering the authentication and signature functions.

Here's how a Mobile-ID is used to log into a secure site, for instance a bank account:

- The user clicks the "Log in with Mobile-ID" option on a supported website
- The phone beeps and displays a screen indicating that a connection is being made
- The user is prompted to enter a Mobile-ID pin code into the phone
- The screen on the phone disappears and the user gains access to the secure website

As smart phones have become standard, having the Mobile-ID option will become increasingly handy, allowing users to vote, for instance, via a phone's web browser. Today, 12,2% of voters use Mobile-ID.

Smart-ID

Smart-ID is a convenient mobile application that works as an identification solution with no requirement for a SIM card. This is the best solution for those who travel or need to change their SIM card often but also for tablets that don't use SIM cards.

As a simple, easy to use and convenient alternative to bank code cards or ID-card, Smart-ID enables its users to log in to different e-services and confirm transactions and agreements.

Smart-ID can be used on smartphones and tablets. When using Smart-ID, one only needs a Wi-Fi network or mobile internet connection, no data roaming or special SIM cards are necessary.

Using Smart-ID for personal identification is free, unlimited and the app can be downloaded to any Android and iOS smart devices.

i-Voting

i-Voting is a unique solution that simply and conveniently helps to engage people in the governance process.

In 2005, Estonia became the first country in the world to hold nation-wide elections using this method, and in 2007, it made headlines as the first country to use i-Voting in parliamentary elections.

Internet voting, or i-Voting, is a system that allows voters to cast their ballots from any internet-connected computer anywhere in the world. Completely unrelated to the electronic voting systems used elsewhere, which involve costly and problematic machinery, the Estonian solution is simple, elegant and secure.

During a designated pre-voting period, the voter logs on to the system using an ID-card or Mobile-ID, and casts a ballot. The voter's identity is removed from the ballot before it reaches the National Electoral Commission for counting, thereby ensuring anonymity.

With any method of remote voting, including traditional postal ballots, the possibility of votes being forced or bought is a concern. Estonia's solution was to allow voters to log in and vote as many times as they want during the pre-voting period. Since each vote cancels the last, a voter always has the option of changing his or her vote later.

In the case of i-Voting, the cumulative time saved in the last Estonian elections was 11,000 working days.

i-Voting process

i-Voting is carried out according to the same scheme as the traditional envelope voting method. The downloaded i-Voting application encrypts the vote. The encrypted vote can be regarded as the vote contained in the inner, anonymous envelope. After that the voter gives a digital signature to confirm his or her choice. By digital signing, the voter's personal data or outer envelope are added to the encrypted vote.

i-Voting is possible only during the 7 days of advance polls — from the 10th day until the 4th day prior to Election Day. This is necessary in order to ensure that there would be time to eliminate double votes by the end of the Election Day.

To ensure that the voter is expressing their true will, they are allowed to change their electronic vote by voting again electronically during advance polls or by voting at the polling station during advance polls.

For example, if a voter cancels his/her electronic vote by going to the polling station to vote, it is guaranteed that only one vote is counted per voter. To that end, all polling stations are informed of the i-Voters on their list of voters after the end of advance polls and before the Election Day on Sunday. If it is found at the polling district that the voter has voted both electronically and with a paper ballot, the information is sent to the Electronic Voting Committee and the voter's i-Vote is cancelled.

Before the ascertaining of voting results in the evening of the Election Day, the encrypted votes and the digital signatures (i.e. the data identifying the voter) are separated. Then anonymous i-Votes are opened and counted. The system opens the votes only if they are not connected to personal data.

Verification of i-Votes

Verification of electronic votes (i-Votes) enables to receive more accurate information on the security of the computer that was used to cast the i-Vote. Verification makes it possible to detect when the computer is infected with malware that changes the i-Vote or blocks the i-Voting. The system was used first at the 2013 local elections. Voters will be able to verify their i-Votes with a smart device (smartphone or a tablet) equipped with a camera and Internet connection.

From 2017 universal verification features were added that will further allow for a more transparent process. The IVXV framework introduces data auditing where auditors are able to check all input and output files for their consistency throughout the process.[7]

e-Tax

Modern e-solutions have made setting up and running a business in Estonia quick and easy. Estonian e-solutions for business, such as electronic tax claims, have pared bureaucracy down to a bare minimum and facilitated an environment where business is convenient.

e-Tax is the electronic tax filing system set up by the Estonian Tax and Customs Board. Citizens can pay their taxes in Estonia in one click - all they need is 3-5 minutes for the tax filing process and it's done! Each year, around 95 per cent of all tax declarations in Estonia are filed electronically.

Using a secure ID, a taxpayer logs on to the system, reviews their data in pre-filled forms, makes any necessary changes, and approves the declaration form. The process typically takes three to five minutes. Even one-click tax returns have been possible since 2015 — the data that is already in the system is displayed for the user along with the calculated result, then all the users have to do is click on the confirmation button. All this can take less than a minute.

In addition to individual income tax claims, other declarations can be made in the system:

- An enterprise's declarations for income tax, social tax, unemployment insurance and contributions to the mandatory pension fund
- Value-added tax returns

[7] https://www.valimised.ee/en/internet-voting/internet-voting-estonia

- Alcohol excise, tobacco excise, fuel excise and packaging excise duty returns
- INF declarations
- Customs declaration

Taxation in the background

Starting from spring 2017 Estonian entrepreneurs are able to simultaneously pay out their salaries, declare and pay taxes in the Internet bank without entering the e-Tax Board/e-Customs.

LHV Bank, in cooperation with the Tax and Customs Board developed a Salary Payment service, which can be used by small and medium sized enterprises for the simultaneous payment of salary, declarations and payment of taxes. The new service is easing the declaration of taxes, by eliminating the need to enter data in different platforms.

When using the service, the LHV client can determine the respective features of the transfer (e.g. salary payment, rate of working time, calculation of tax-free income) in the Internet bank. The bank sends the source data for taxation to the Tax and Customs Board, who automatically calculates the amount of payable tax based on the person and returns to the bank the information on tax amounts to be paid in such a way that when making the transfer, the client can already see the related tax liability. The tax amount can be paid either immediately together with other payments or at a later date. The payments can be saved for making future salary payments together.

In October 2017 Estonian Tax and Customs Board announced the development of the new e-Tax/e-Customs (e-ETCB) portal that will fundamentally and visually transform the tax filing and payment system. "A new technological foundation will help reduce physical contact with us to the greatest possible extent. This will mean more technical solutions for sending data or otherwise interact with us and the services of e-ETCB will have a clearer and more convenient design," said Valdur Laid, Director General of Estonian Tax and Customs Board.[8]

[8] https://www.emta.ee/eng/development-new-etcb-e-portal-begins

State Information System RIHA

State Information System (RIHA) serves as a catalogue for the state's information system. At the same time, it is a procedural and administrative environment via which the comprehensive and balanced development of the state's information system is ensured. RIHA guarantees the transparency of the administration of the state's information system and helps to plan the state's information management.[9]

The objective of the system is to collect metadata about all state information systems, their administrators and service providers, services, service users, classifications and administrators of classifications. In Estonia, the establishment and maintenance of databases is regulated by the Databases Act, according to which it is mandatory for the administrators of information systems to register their databases and information systems in RIHA as well as to ensure updating of the submitted metadata.[10]

RIHA gives information on the following subjects:

- Which are the information systems and databases that make up the state's information system;
- Which data are collected and processed and in which information systems;
- Which services, incl. X-Road services, are provided and who is using them;
- Who are the responsible and authorised processors of the information systems and databases, and who are the contact persons;
- On which legal basis are the databases operated and the data processed;
- The reusable components that ensure the interoperability of information systems (XML assets, classifications, dictionaries and ontologies).

RIHA serves as the procedural and administrative environment for the use and employment of information systems and databases; the registration of services; the connection with the X-Road and the administration of reusable components (XML assets, classifications, dictionaries and ontologies).

e-Business Register

Estonia's e-Business Register is an advanced and secure tool that allows entrepreneurs to register new business online in just minutes without having to go to a notary or some other official. From 2011, most companies have been established over the internet using the e-Business Register and this process has come down from 5 days to 18 minutes.

[9] https://www.ria.ee/en/administration-system-of-the-state-information-system.html
[10] https://www.ria.ee/public/publikatsioonid/RIHA.pdf

The e-Business register allows you to register a new company over the internet, change data in the business register, file annual reports, manage the members list for political parties or make detailed inquires about other companies. All it takes to register an Estonian company is an ID card, Mobile-ID or e-Residency card, and an internet connection.

The e-Residency programme allows non-Estonian citizens to also access the e-Business register and use the digital solutions when establishing a company in Estonia. The e-Business register makes the process of registering a company and submitting documents like annual reports easy and efficient for users online no matter where they are.[11]

e-Land Register

The e-Land Register is a one-of-a-kind web application that contains information on all ownership relations and limited real rights for properties and land parcels. Currently, there are over 1 million immovables in the Land Register.

Paired with a geographical information system (GIS), the electronic Land Register delivers real-time geographical data through the X-Road, enabling advanced map-based visualizations that power many of the location-based services in Estonia.

A critical tool for the real-estate market, it provides total transparency; listing the registered owner of each property holding, showing the property boundaries and providing other information that potential buyers need to know.

Records information contain:

- Cadastral information — including address, area, purpose of land
- Ownership relations
- Encumbrances, restrictions, rights of use, other notations
- Mortgage information

The system has transformed the way property transactions are carried out in Estonia, eliminating the need to visit public offices and spend hours waiting for a civil servant to search records. This paper-free system has reduced the processing time for land transactions from up to three months to as little as 8 days.

Businesses benefit from the security of having instant access to land titles and the ability to confirm ownership with a few clicks.[12]

[11] https://e-estonia.com/solutions/business-and-finance/e-business-register

[12] https://e-estonia.com/solutions/interoperability-services/e-land-register

Population Registry

The Population Register is the state's database for holding basic information about each person living in Estonia. It contains their name, ID code, date of birth, place of residence, and other statistical data such as nationality, native language, education and profession. Each resident can review and correct their data in the register.

The register is connected to other systems via X-Road, and a variety of other state systems depend on its data for their services. For example, when individuals apply for child support, study allowance or concession status for public transport, data is retrieved from the Population Register. The same is true when a person uses i-Voting. The system retrieves the information automatically — no extra documents have to be submitted or online forms filled out.

The state also benefits because statistics are kept up-to-date, and functions such as voter registration and tax filing, which are based on place of residence, can be handled properly.[13]

[13] https://e-estonia.com/solutions/interoperability-services/population-registry

Architecture of the Digital Society

Running a modern state is a data-driven endeavour and for e-Estonia the open-source backbone is X-Road. This is the invisible yet crucial environment that allows the nation's various e-service databases, both in the public and private sector, to link up and operate in harmony, it allows citizens to to be requested data only once and saves more than 800 years of working time for the state and citizens annually.

Bear in mind the unique aspect of e-Estonia is that it lacks a centralised or master database — all information is held in a distributed data system and can be exchanged instantly upon request, providing access 24/7.

99% of state services are online

52,000 organisations as indirect users of X-Road services

800 years of working time saved annuallv

X-Road

Estonia's Information System is built in a decentralized manner meaning that it contains different technology stacks built in different time frames where the personal data is scattered and kept in a variety of databases. For these islands to be able to communicate with each other there needs to exist a data exchange layer that provides its members' autonomy, confidentiality, integrity and availability.[14]

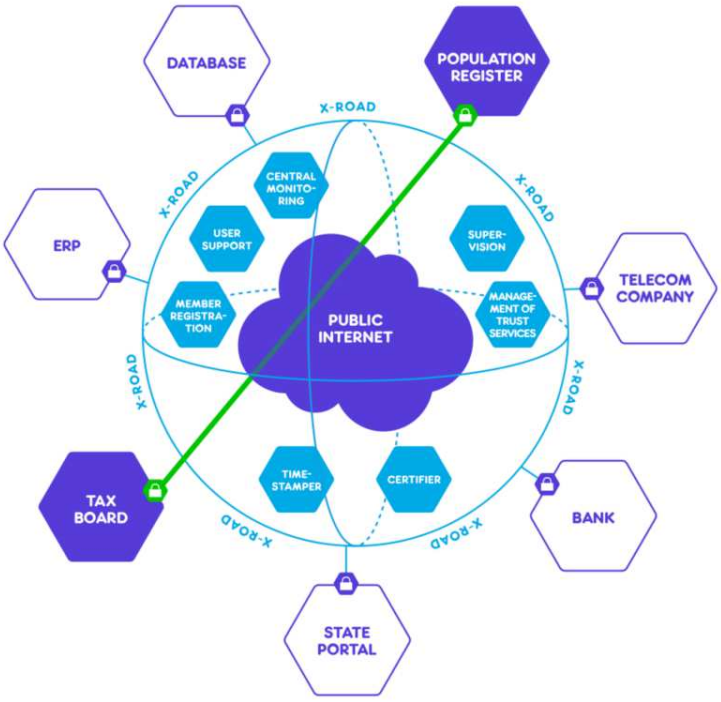


FIGURE 1. ESTONIAN X-ROAD. SOURCE: RUBIKS DIGITAL BLOG

Estonia's e-solution environment includes a full range of services for the general public, and since each service has its own databases they all use X-Road. To ensure secure transfers, all outgoing data from X-Road is digitally signed and encrypted, and all incoming data is authenticated and logged.

Public and private sector enterprises and institutions can connect their information system with X-Road. Joining the X-Road enables institutions to save resources, since a cooperative and secure data exchange layer already exists with all the other X-Road members. Data exchange between all the members of the X-Road ecosystem is significantly more efficient.[15]

X-Road was started in 2002 by the Estonian Information Technology Center. In 2003 the Estonian government passed a legislation that demanded that every government agency must be connected to the X-Road data exchange layer by the year 2005 and today there is more than 219 separate databases, 939 institutions and 1723 services connected, both from the government as well as private sector.

Because the Population Registry, Health Insurance Fund, and many other institutions are connected to X-Road, it means that one's personal information is also available on the network. The security over the data is solved by signing each data transaction with a digital stamp (signature) by the person who distributes the data. This means that at any given point you are able to query who, when and why has requested and received information about you. Each member can control separately who can access the data they hold. It is the capability of the individual data holder to decide over its access control that provides the autonomy part.

[14] https://blog.rubiksdigital.com/how-to-solve-the-digital-identity-and-bring-privacy-to-a-whole-new-level-79f67585df5a
[15] https://www.ria.ee/en/x-road.html

When talking about privacy one of the most significant areas is the health care. There are multiple laws in place to protect this data, one stating that people own their personal data giving them access to see who has viewed their data (for example their doctor, police official or other). While the X-Road still has a Certificate Authority that decides who is who in the network, the government is acknowledging the issue of integrity in cyberspace and working consistently to improve it.[16]

Originally X-Road was simply used to send queries to different databases. Now it has developed into a tool that can also write to multiple databases, transmit large data sets and perform searches across several databases simultaneously. X-Road was designed with growth in mind, so it can be scaled up as new e-services and new platforms come online.

So far, there haven't been any events that have severely hindered the X-Road. This resiliency suggests that the distributed architecture works remarkably well even in critical situations (like cyberwar).[17]

Today, X-Road is also implemented in Finland, Azerbaijan, Namibia and Faroe Islands. X-Road is also the first data exchange platform in the world that allows data to be automatically exchanged between countries. Since June 2017, automatic data exchange capability has been established between Estonia and Finland.

Connecting to the X-Road

There are several steps to take to connect with the X-Road. Actually using a database (a Register) requires making a detailed agreement with each of the database's owners. Imagine a municipality wants to process captured cats and reunite them with their owners. The municipality must:

- Become a member of the X-Road by entering into a contract with RIA, Estonia's Information Authority.
- Make an agreement with the Pet Register. In order to make this agreement the organization will have to provide an estimate of the number of requests per day.
- Make an agreement with the Population Register. Making this agreement will require proving that the organization's access to the personally identifiable information contained in the Population Register is necessary for completing a public task. For capacity planning purposes, estimates of the number of anticipated requests must also be provided to the Population Register.
- Secure the technological and operational ability to interact via the X-Road. This means obtaining servers, installing the X-Road software, and maintaining the system. In some cases it is possible to outsource this technical work to someone more capable outside the organization.[18]

[16] https://blog.rubiksdigital.com/how-to-solve-the-digital-identity-and-bring-privacy-to-a-whole-new-level-79f67585df5a

[17] https://www.ria.ee/en/introduction-to-xroad-part1.html

[18] https://www.ria.ee/en/introduction-to-xroad-part2.html

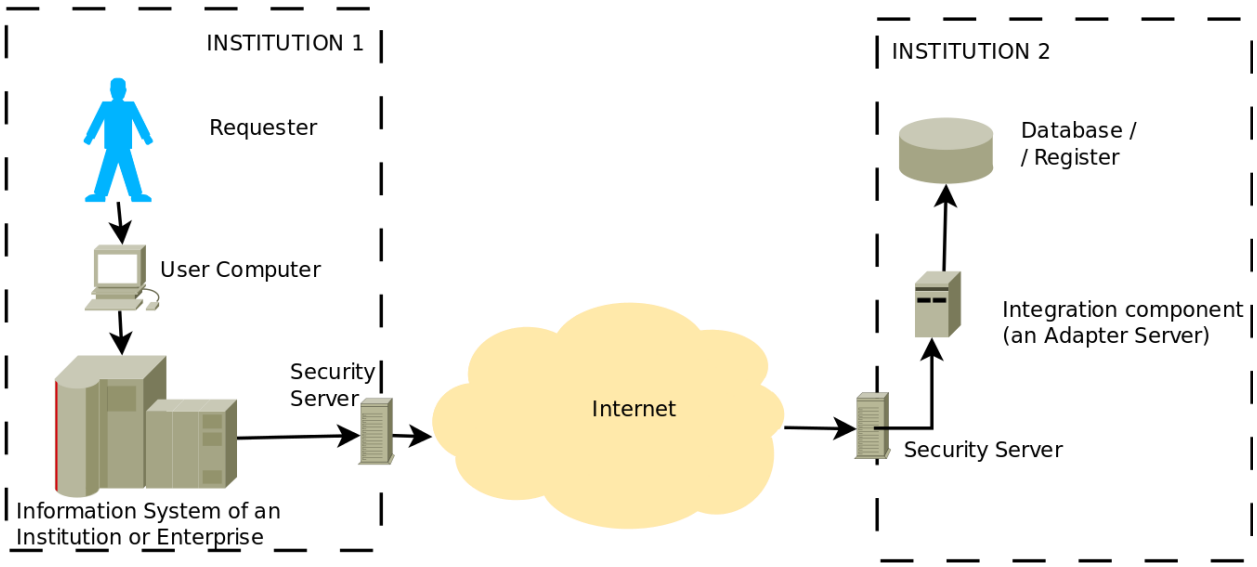


FIGURE 2. THE CONNECTIVITY DIAGRAM. AUTHOR: ANTO VELDRE

Another feature of the X-Road is MISP (mini-information-service-portal), a standard web portal to enable trivial requests that conform to prescribed parameters. The MISP makes it possible for users to access the X-Road via a normal internet browser. It does this by translating WDSL files directly into webpages.

MISP is intended for small and low budgeted institutions that are legally required to publish data of some kind. MISP makes X-Road participation more convenient for these organizations, which might otherwise be thwarted by the complexity of X-Road participation.

Even organizations using MISP must have a security server. Several private companies provide joint MISP + Security Server solutions to smaller municipalities. A tiny municipality will save a lot of money by not building its own server room.

MISP is only accessible to those who have logged in using two-factor eID. Further, for security reasons, MISP cannot be used to execute complex requests or access especially confidential information.[19]

X-Road Security

It is impossible to counterfeit requests and data on the X-Road. Every interaction that occurs via the X-Road is always logged. This constant logging facilitates one of the X-Road's most important design goals: data integrity. Only authorized persons should be able to access, modify and erase data via the X-Road.

All of this sounds good in theory, but how are these security requirements ensured in real life? First, the X-Road Centre collects statistics about X-Road usage from the

[19] https://www.ria.ee/en/introduction-to-xroad-part3.html

security servers. This enables it to know what requests were made of data service providers. Sometimes a single request will be flagged as anomalous and the Centre can then ask the initiator to clarify its grounds for making the request.

Additionally, each security server has a security log reflecting every request it has ever made.

There are several options to ensure the continued integrity of the logs. One of these is chaining, which means making latter logs cryptographically dependent on those that precede them. Chaining makes it impossible to fabricate events.

It is also possible to digitally sign and timestamp requests made in a given time period (day, month, year). This makes it possible to later determine with a high level of certainty whether a request was ever made or not. In other words, requests are non-repudiable. This means, no one can deny they occurred or change the details recorded about them. For these reasons, starting with X-Road version 6, Secure Signature-Creation Devices (SSCD's) are used by all X-Road participants. These devices enable fast and secure digital timestamping.

One of the main principles of the e-State is that no one should be able to forge records. Security logs are central to ensuring this data goal. Regulations and procedures that make the professional and legal costs of attempting to forge records very high are another important tool for protecting data integrity.[20]

The Trust Federation - Exporting Estonian Digital Infrastructure

The X-Road federation is the capability of X-Road to provide secure Internet-based data exchange across ecosystems (states) to members that belong in different ecosystems. The X-Road federation is a situation, where there are similar X-Road environments in different states (or other organizations). Every X-Road environment is managed by a competent organization (centre) that defines the applied security policy and manages the information of its ecosystem members.

For cross-border data services to exist, the X-Road centres need to conclude a federation agreement that entails the description of organizational and legal liabilities between the centres of different states. X-Road members that have joined the X-Road environment in their state (centre) are able to exchange data (cross-border e-services) with the X-Road members in other states.[21]

[20] https://www.ria.ee/en/introduction-to-xroad-part3.html

[21] https://www.ria.ee/en/x-road-trust-federation.html#what-is

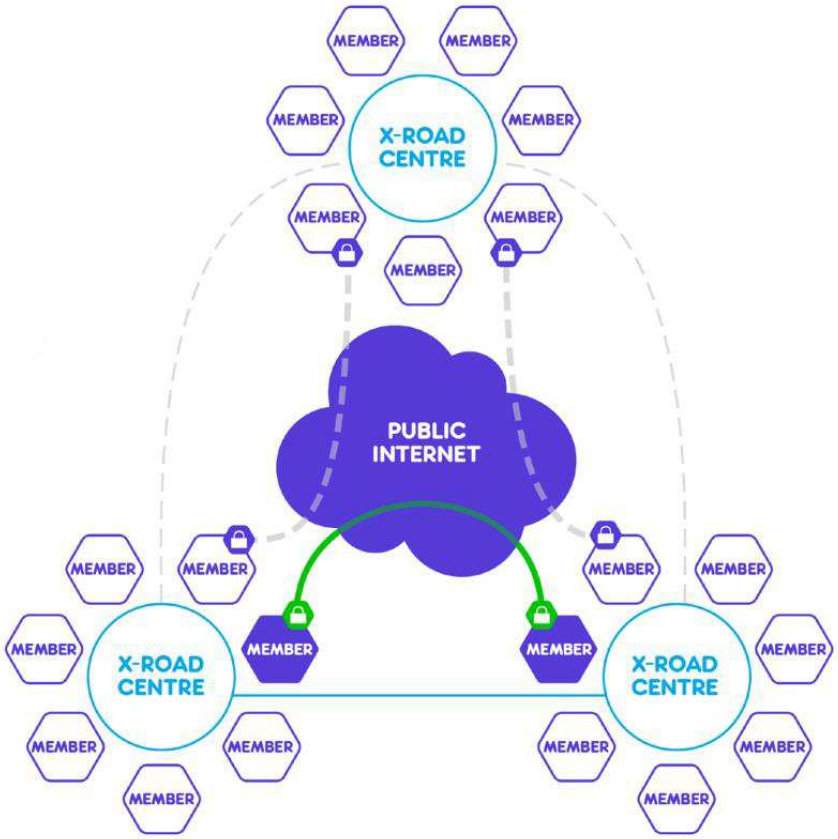


FIGURE 3. THE TRUST FEDERATION. SOURCE: RUBIKS DIGITAL BLOG

In 2013 the Prime Ministers of Estonia and Finland signed the Memorandum of Understanding about the cooperation in the field of ICT. The goal was to create the possibility of sharing resources, experience, and expertise in ICT development. The participants could also now promote cooperation in implementing the Estonian X-Road source code in Finland as well as work together on the future versions of the technology.

By early 2014 Estonia had given the X-Road to Finland under EUPLE license and a test environment of the version 5 was set up. In 2015 X-Road version 6 development environment was opened and a cooperation agreement between the parties was signed to continue the development of X-Road in cooperation by having a shared code base. Later that year Finland started the production use of X-Road (called Palveluväylä in Finland). Today, there are over 18 organizations joined with the production environment in Finland.

To manage the cooperation and its challenges Estonia and Finland have set up a management body and a working group both consisting of six people (50/50 from Estonia and Finland). Their goal is to guide the roadmap, to do risk management as well as share the technical information and coordinate the development of the day-to-day work. The role of the management body is to ensure all the parties involved in developing of the X-Road will share a common roadmap.

This form of federation opens many doors for the private sector to scale their business built on top of big data. Right now there are two countries that will form this federation but hopefully we will see other states joining in the future as well.

To bring an example of what it means to the end users then if you register a company on the X-Road from Estonia then you don't need to do it again in Finland, instead, you can immediately start querying data from the members situated in any of the federation countries.

In the end, the goal of X-Road is to be a communication channel for open services. This will mean that not only are users able to query the public infrastructure data in their operating country but also ask the same

information easily without additional contracts from other countries as well.[22]

Blockchain

Although X-Road, the layer itself and the core technology have been around for more than a decade already, it is how it is improved on that solid foundation that creates true innovation. Today we are seeing the involvement of blockchain with the X-Road data layer. Estonian government is using Guardtime's KSI Technology—an industrial blockchain platform.[23]

2007, under the auspices of the Estonian Government and the private sector, a team of Estonian cryptographers, network architects, software developers and security specialists designed the digital signature system that would eventually lead to KSI, providing exabyte-scale real-time authentication for all the world's networked digital assets. In Estonia KSI is used for independent verification of all government processes and protecting e-governance services offered to the public.[24]

KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy. A blockchain is a distributed public ledger — a database with a set of pre-defined rules for how the ledger is appended by the distributed consensus of the participants in the system. Due to its widely witnessed property, blockchain technology makes it also impossible to change the data already on the blockchain.

With KSI Blockchain deployed in Estonian government networks, history cannot be rewritten and the authenticity of the electronic data can be mathematically proven. It means that no-one — not hackers, not system administrators, and not even government itself — can manipulate the data.[25]

As an example, electronic patient records are a critical component of Estonian e-services and by integrating KSI blockchain technology it becomes possible to provide an independent forensic-quality audit trail for the lifecycle of those patient records, making it impossible for anyone who gains access to those records to manipulate information and cover their tracks.

Estonian eHealth Foundation uses Oracle technology to process and store the patient records and KSI blockchain is integrated at the Oracle database engine, providing increased security, transparency, auditability and governance for electronic systems and lifecycle management of patient records. KSI instrumented records will be irrefutable.

[22] https://blog.rubiksdigital.com/what-exporting-a-country-and-its-digital-infrastructure-looks-like-c809f2c87228
[23] https://blog.rubiksdigital.com/how-to-solve-the-digital-identity-and-bring-privacy-to-a-whole-new-level-79f67585df5a
[24] https://guardtime.com/solutions/egovernment
[25] https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

Mike Gault CEO of Guardtime commented: "Estonian (former) President Toomas Hendrik Ilves has repeatedly pointed out the biggest threat in cyberspace is integrity, and in particular the integrity of patient health care records. We are proud to announce that Estonia is again leading the world in digital innovation. This level of transparency and auditability is a global first and with US health care fraud measured in the hundreds of billions of dollars every year, the Estonian model should provide a valuable template to dramatically reduce this fraud both for the US and the rest of the world."

Margus Auväärt, Head of eHealth Foundation added: "Guardtime's KSI blockchain technology enables us to easily reach the highest integrity levels for our systems and data, as mandated by ISKE, an Estonian cybersecurity standard modeled after BSI IT-Grundschutz by German Federal Office for Information Security. Furthermore, the unparalleled scale and frequency of the KSI blockchain give us the capability to maintain continuous real-time situational awareness into the integrity state of assets under our control, not required by any standards, but enabling us to react to any incidents immediately, before potentially larger-scale damages can occur."[26]

Data Analysis Through Sharemind

Estonia's leading research and development company, Cybernetica, has developed Sharemind®, a data analysis platform to aggregate and analyse private data that may be inaccessible due to regulatory or proprietary reasons. Sharemind can remove regulatory roadblocks using its sophisticated solution. Sharemind helps to protect data assets against threats through its unique cryptographic solution.

With Sharemind secure computing technology, data owners share data in an encrypted form, giving no access of the original data to the partners. Sharemind can process encrypted data without having to remove the encryption. This prevents any single party from abusing private data by distributing control and responsibility for any operation.

Sharemind produces encrypted outputs for stakeholders that can be useful in making data-driven decisions. One key component of Sharemind's process is the computing done between a distributed network of servers. No analysis can be performed on the data by one independent actor, all servers must agree on the predetermined queries.

Sharemind was used in a DARPA prototype to determine possible satellite collisions. Sharemind's solution allows distrusting parties to collaborate on mutually beneficial outcomes by sharing encrypted data. The actual trajectories of the satellites were never revealed to the opposing parties, yet the outcomes of collision risk could be shared by the various stakeholders.

[26] https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency

In 2015, the Estonian Center for Applied Research used Sharemind to collect governmental tax and education records to run a large data study looking for correlations between students working during their university studies and students failing to graduate on time. The study included over 10 million data points and yielded interesting results for the stakeholders.

The Sharemind solution has been used for pilot projects for those listed previously as well as, the Estonian Ministry of Education, the Estonian Ministry of Finance, and is looking at pilot projects in the EU, US and the UK.[27]

Smart Grid Development

Significant influential trends in the energy sector include the integration of energy markets (single European energy market), the massive addition of geographically dispersed facilities with unplanned production cycles to the energy system, growing accumulation and consumption management options, climate politics and energy efficiency objectives, the addition of new types of market participants (ESCOs or energy service companies, energy cooperatives, aggregators, virtual power plants), the increased awareness of energy users and demand for new types of services, and the loss of boundaries between the energy, gas and heating markets.

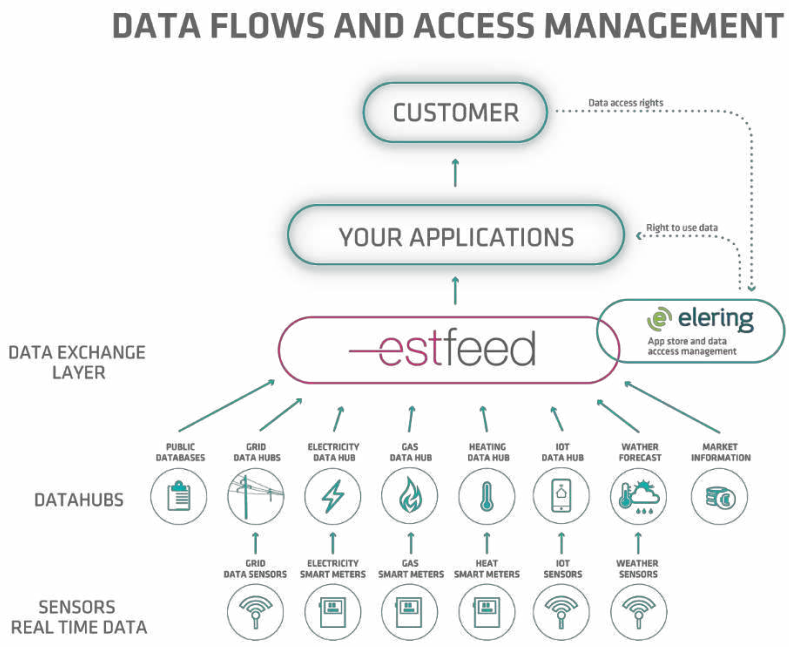


FIGURE 4. SOURCE: ELERING

All this means increasingly more unexpected energy flows, but also exponentially growing information flows in the energy system. The smart grid entails combined changes in the energy system resulting from the widespread deployment of information and communication technologies. It allows new services to be offered to consumers.

The platform allows end consumers, energy service providers, scattered (small) producers and network operators to

[27] https://e-estonia.com/solutions/interoperability-services/sharemind

increase energy production, transportation and consumption efficiency with the help of near real-time data on energy consumption.

The technical basis for the smart grid platform is the Estfeed data exchange layer. Estfeed is a data sharing platform designed for organizations and individuals to more efficiently organize their energy consumption. It helps customers to better understand the information related to where they use energy. With Estfeed, network operators can share data with confidence and get support from market participants. It is believed that implementing this technology widely would help Europe save up to 100 billion euros per year.[28]

Estonian electricity and gas system operator Elering has also created e-elering, a client portal for the applications that uses data through Estfeed platform as well as for other smart energy usage applications.

In the portal, consumers can view their own electricity and gas consumption data and give service providers mandates to access their data. In a specially designed information system, renewable energy producers can follow production data, submit applications for renewable energy subsidies, and conduct operations for certificates of origin for renewable energy production. The information system for connections to the transmission system is also available through e-elering, and third-party solutions for following the electricity and gas prices can be accessed.[29]

[28] https://netgroup.ee/project/estfeed/

[29] https://elering.ee/


cyber defence
©Aron Urb

Cyber Defence

Increased cybercrime and politically motivated attacks on electronic services mean cyber security is more important than ever for both the private and the public sector. Estonia's preparedness to handle cyber crises has significantly increased over the past decade. The country has created intrusion detection and protection systems, practised cooperation with both public and private institutions, significantly contributed to the awareness of users, and is participating in intensive international cooperation.

After its experience with the 2007 cyber attacks, Estonia has implemented blockchain technology to ensure data and systems integrity and combat insider risk, and became one of the most recognized and valued cyber security experts internationally. Since then Estonia became the home of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) and European IT agency. CCD COE is organizing the world's largest and most complex international technical live-fire cyber defence exercise Locked Shields with 900 participants from 25 nations. International conference Cycon is attracting 600 key experts and decision makers of the global cyber defence community to Estonia every year.

2007 Cyber Attack

In 2007 the Estonian government decided to move a memorial of the Soviet Red Army from the centre of Tallinn to a military cemetery on the outskirts of the city. The decision sparked outrage in Russian-language media and Russian speakers took to the streets. Protests were exacerbated by false Russian news reports claiming that the statue, and nearby Soviet war graves, were being destroyed.

Considered the first nationwide cyber attack in the world, Estonia was hit by major cyber-attacks which in some cases lasted weeks. Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic also known as DDOS attacks. Massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers.

The result for Estonians citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.

The 2007 attacks came from Russian IP addresses, online instructions were in the Russian language and Estonian appeals to Moscow for help were ignored.[30]

[30] http://www.bbc.com/news/39655415

The cyber attacks against Estonian information infrastructures that accompanied the 2007 spring 'Bronze Nights' protests met a collaboration network already in place; and indeed the horizontal collaboration between private and public sector information security experts was generally viewed as a major factor for successfully handling the attacks.[31]

Cyber Defence Unit of the Estonian Defence League

The Cyber Defence Unit of the Estonian Defence League, or the 'Estonian Cyber Defence League' as it is widely referred to, has caught worldwide attention as an innovative model for the involvement of volunteers in national cyber defence.

Originating in the long-time collaboration of both public and private sector cyber security experts of Estonia, and emerging in the aftermath of the 2007 cyber attacks against Estonian information infrastructures, the unit is focused on strengthening the professional cyber defence skills of its volunteer members in order to prepare and enhance support capabilities that can be provided in crisis.

The Cyber Unit includes specialists in key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc).[32]

The effect of the Cyber Defence Unit, in that it promotes public-private sector cooperation in cyber security, strengthens cyber security awareness in the population, and supports prevention and response to cyber threats, is wider still.

The Cyber Defence Unit is integrated into the Estonian Defence League, constituting one of the structural units of the latter. It has its own staff, manned by both volunteers and paid personnel, and consists of sections dealing with both administrative aspects of the Unit's operation and tasks related to cyber defence. The Unit is led by a commander subordinated to the Commander of Estonian Defence League. The latter is appointed by the national government and is, for the purposes of military command, subjected to the authority of the Commander of the Estonian Defence Forces.

However (referring to the peacetime situation), the role of the Commander of the Defence Forces towards the Defence League is limited, by law, to aspects of military capability, and not used for the administration of the Estonian Defence League, which remains a unique

[31] The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis, NATO Cooperative Cyber Defence Centre of Excellence (2013)

[32] http://www.kaitseliit.ee/en/cyber-unit

combination of a non-governmental organisation and military command.[33]

Critical Information Infrastructure Protection

The purpose of the critical information infrastructure protection (CIIP) is to maintain a trouble-free functioning of the country's essential information and communication systems under ordinary circumstances and to ensure their continuity on a minimum level during critical situations.

The Section of Critical Information Infrastructure Protection at the Estonian Information System's Authority (RIA) mainly concentrates on questions related to the protection of such information systems that are needed for the proper functioning of vital services. The main task of the section is to arrange protection for the state's critical public and private information systems on the national level.

On the national level, RIA arranges the protection of such public and private sector information systems that are relevant for the functioning of the state of Estonia. They mainly focus on the issues of protecting the information systems that ensure the functioning of vital services. Vital services are services necessary for organising the functioning of the society, healthcare, security and people's economical and social well-being.

On the strategic level, the protection is handled in the field of CIIP, where data about the critical information infrastructure (CII) are collected and maintained. Additionally, risk analyses related to CII are prepared, the respective security measures are developed and the supervision for following the methods is initiated.

On the operative level, RIA's subunit the Computer Emergency Response Team of Estonia (CERT) handles the protection of the information systems necessary for the provision of vital services.

CERT Estonia, established in 2006, is an organisation responsible for the management of security incidents in .ee computer networks. Its duty is to assist Estonian Internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats. CERT Estonia deals with security incidents that occur in Estonian networks, start there, or which it has been notified about by citizens or institutions either in Estonia or abroad.

The support provided by CERT Estonia depends on the type and severity of a security incident, on the number of users potentially affected by it and on resources available for the organisation.[34]

[33] The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis, NATO Cooperative Cyber Defence Centre of Excellence (2013)

[34] https://www.ria.ee/en/

Three-level IT Baseline Security System ISKE

The goal of implementing three-level IT baseline security system (ISKE) is to ensure a security level sufficient for the data processed in IT systems. The necessary security level is achieved by implementing the standard organisational, infrastructural/physical and technical security measures.

It is an information security standard that is developed for the Estonian public sector. According to Government Regulation, ISKE is compulsory for state and local government organisations who handle databases/registers. The first version of the ISKE implementation manual was completed by October 2003.

The preparation and development of ISKE is based on a German information security standard — IT Baseline Protection Manual (IT-Grundschutz in German) — which has been adapted to suit the Estonian situation.

A three-level baseline system means three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels).

Simplified process for the implementation of ISKE:

1. Mapping databases
2. Mapping information systems and other information assets
3. Identifying links between databases, information systems and other information assets
4. Identifying the required security class and level for databases
5. Identifying the required security class and level for information systems and other information assets
6. Identifying the typical modules, which comply with information systems, and other information assets
7. Identifying the required security measures for information systems and other information assets.

Information security is an ongoing process, which is aimed at ensuring the confidentiality, integrity and availability of data and assets. The goal is to find a balance between these three components.[35]

[35] https://www.ria.ee/en/

NATO Cooperative Cyber Defence Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) supports its member nations and NATO with cyber defence expertise in the fields of technology, strategy, operations and law.

The NATO CCD COE is a multinational and interdisciplinary hub of cyber defence expertise. The heart of the Centre is a diverse group of experts — researchers, analysts, trainers, educators — from 20 nations. The mix of military, government and industry backgrounds means the NATO CCD COE provides a unique international 360-degree look at cyber defence.

The NATO CCD COE is the home of the Tallinn Manual 2.0. The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Authored by nineteen international law experts, the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", the updated and considerably expanded second edition of the 2013 "Tallinn Manual on the International Law Applicable to Cyber Warfare", is an influential resource for legal advisers dealing with cyber issues. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence.

The Centre also organises the world's largest and most complex international technical cyber defence exercise Locked Shields. The annual scenario-based real-time network defence exercise, organised since 2010 focuses on training the security experts who protect national IT systems on a daily basis.

The NATO CCD COE is also organising the annual conference on cyber conflict, CyCon. Every year, over 500 decision-makers and experts from government, military and industry from all over the world approach the conference's key theme from legal, technology and strategy perspectives, often in an interdisciplinary manner.

As of 2017, Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed on as Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence. Austria and Finland have become Contributing Participants and Sweden is well on its way of doing the same. The Centre is staffed and financed by member nations and is not part of NATO's military command or force structure.[36]

[36] https://ccdcoe.org

Data Embassy

The Data Embassy is an extension of the Estonian government in the cloud, which means the state owns server resources outside its territorial boundaries. This is an innovative concept for handling state information, as states usually store their information within their physical boundaries. Those resources are under Estonian state control and must be capable not only of providing data backups, but also of operating the most critical services.

This new approach makes it possible for the Estonian state to continue operating under conditions where its local data centres have been stopped or disturbed due to a natural disaster, large-scale cyber attack, power failure or other crisis situation.

In the last 20 years, Estonia has developed into what the World Development report, compiled by the World Bank, last year called "closest to a digital society". However, being digital and therefore dependent on information and communication technology also creates challenges. One of them is the question of how to secure all the data that could become vulnerable in the case of a cyber or indeed a physical military attack.

For example, when Estonia regained its independence from the Soviet Union in 1991, it had to determine who its rightful citizens were. Approximately 80,000 people had fled the country during the last world war and there was the problem of how to return land and property to those whose assets were confiscated during the Soviet occupation. In order to establish this paper records and archives were used. However, in the digital society the country no longer stores this information on paper, raising the question of continuity or as in the case of Estonia today, digital continuity.

Russia's annexation of Crimea in 2014 brought the question of continuity back to the forefront of public discussions in Estonia and the government's Cloud Policy stated that, "to ensure service functionality and data continuity, capabilities needed to be developed outside of the country's borders." So even if a crisis develops, digital authentication and authorisation services would remain operational. To achieve this aim Estonia considered two options: a physical embassy for data in a friendly foreign country or a virtual embassy for data in a privately owned public cloud.

One of the two options to achieve the digital continuity — the cloud technology — was tested in late 2014, when Estonia embarked on a research project with Microsoft to see whether a public/private cloud computing partnership model could function. However, this was not enough: "The cloud technology provides a good opportunity, but the state also wants to maintain the full control and jurisdiction of their data and systems. For this reason the private cloud services are not exactly suitable for us," said Siim Sikkut, the Deputy Secretary General for Communications and State Information Systems at the Ministry of Economic Affairs and Communications. "Therefore, we started to develop and enhance the data embassy concept, just like Estonian embassies abroad, these are our sovereign embassies in foreign data centres."

During the last few years Estonia has held talks with a number of countries and has

now succeeded with one of the smallest countries in the European Union. The first data embassy is based in a high-security data centre in Betzdorf, a commune in eastern Luxembourg.

"The Luxembourg site stores the copies of the most critical and confidential data," Sikkut explained. "Once the first one is running, we will analyse and evaluate whether we need to enhance our capabilities. It is highly likely that we will set up additional data embassies, but that all depends on the cost and our experience," he said.

The Estonian data embassy has the same protection and immunity as the traditional embassies. "Luxembourg has been a very good partner. In essence, we are creating a new precedent in terms of international law and practice, a kind of innovation.

Luxembourg has been keen to think along with and contribute to the creation of the new concept. The 'physical' embassies are our sovereign territory under the Vienna Convention. Now we want to bring the same concept to the cyber world and data centres," Sikkut explained. This effectively means that officials from the host country will be barred from accessing the data.[37]

[37] https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/


mobility
©Jaanus Ree

Mobility and Transportation

Thanks to the location-based aspect of public services, Estonia has been able to increase the well-being and safety of its citizens. Estonia continues its commitment to innovation and new technologies by offering the opportunity to use Estonia as a test bed for self-steering technology - in 2017, the government made it legal to test self-driving vehicles on all national and local roads.

Intelligent Transportation Systems

A basic ingredient of any successful economy is a well-functioning transportation network — the roads, railways, ferries, border crossings and public services necessary for the efficient flow of people and goods.

In recent years, governments and industries have begun to improve these networks using Intelligent Transportation Systems (ITS) — advanced applications and innovative services that help users get the most out of their infrastructure.

Estonia has introduced a number of ITS solutions designed to make travel safer and logistics more convenient. For example, in March 2017, Estonia made it legal to test self-driven vehicles on all national and local roads in the country. Work is underway to create a full legal and cyber-risk management framework for using fully autonomous vehicles in regular road and traffic conditions.

The government's view is that self-driven vehicles are more than just cars with no hands on the wheel, but rather a disruptive force for tens if not hundreds of services both in the private and public sector. This is the concept for providing new, more efficient, convenient and sustainable public services across Estonia.

The aim is to reorganise the public transportation system using self-driven vehicles. The government has adopted a plan to create a fleet management system, integrating such vehicles into the public transport system with journey planning and call-to-order bus stops. Similarly, the government will launch pilots in other public service areas to seek new models of public service delivery based on autonomous mobility.[38]

Objectives of ITS Estonia:

- To provide platform for cooperation and innovation for Estonian public and private sector in the field of transport and logistics.
- To gain new knowledge concerning innovative ITS solutions and future technologies from ITS networks.

[38] https://e-estonia.com/solutions/location-based-services/intelligent-transportation-system

- To support export of Estonian ITS companies
- To be the driving force of starting ITS pilot projects in Estonian and international level.[39]

Incident Handling Platform

Guardtime and Estonian Government have built an Incident Handling Platform for connected vehicles.

Objective of the platform is to enable secure data exchange environment for connected vehicles and smart infrastructure. It ensures a trustworthy audit trail is available to handle incidents — while preserving privacy. It also allows to enforce connected car security — assuring that only authentic and authorized software is used. Guardtime's Blokchain technology stack is the technical enabler of the platform.

In case of an incident the governmental regulatory authority has immediate and trustworthy access to all relevant data. The solution enables access to audit trail („black box" contents of a connected vehicle) of all involved connected vehicles and objects. Relevant data includes vehicle identification, speed, location, radar/LIDAR readings, camera images etc. Cross-vendor interoperability and compliance with privacy regulations are built-in by design.

The solution also ensures that vehicles / objects which are compromised (hacked, „tuned" etc.) are timely discovered and prohibited from the ecosystem. Connected vehicles and objects verify integrity of other vehicles / objects on peer-to-peer basis. Alerts of compromises are provided to different parties (OEM, regulatory authority, vehicle owner).[40]

[39] https://its-estonia.com/

[40] https://its-estonia.com/en/2017/10/20/incident-handling-platform/

Smart Street Systems

Smart street systems are developing in several locations in Tallinn, Estonian capital. The main purpose is to test novel technologies on new street construction projects and provide real time data about challenges for transport and pedestrian movements. For example, the real time information from Kalaranna street is available for the citizens and the municipality through the smart street public webpage.

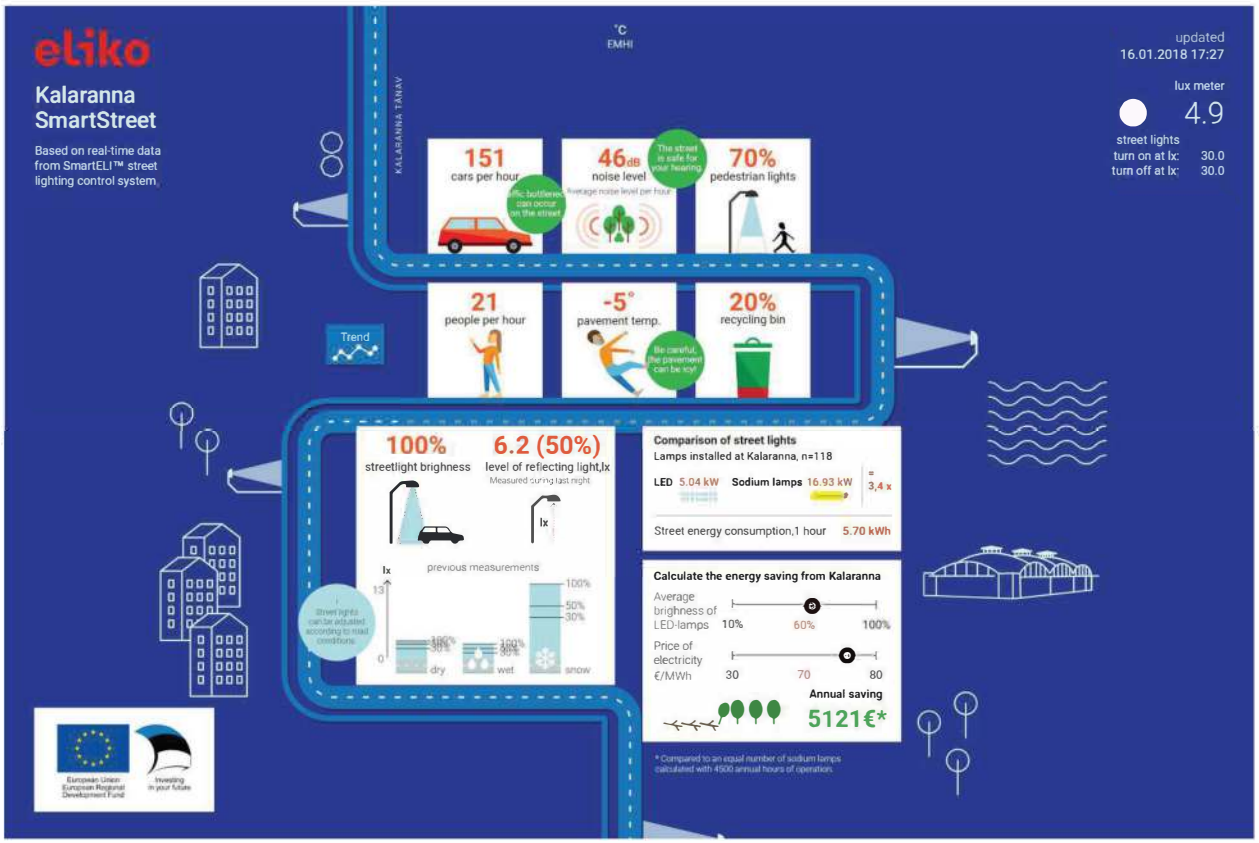


FIGURE 5. REAL TIME INFORMATION FROM KALARANNA STREET. SOURCE: WWW.ELIKO.EE/SMARTCITY

Kalaranna is a 2 km long street, reconstructed in 2015 and equipped with new LED lights and Eliko's SmartELI system. The street lighting system has a much higher throughput than would be necessary for just controlling the LED-lights. Therefore, different sensors were integrated into the SmartELI wireless communication network to get additional data about the street.

Local community members helped Eliko to select the sensors to reflect what citizens are concerned about in Kalaranna, such as pedestrian safety and noise pollution, electricity consumption, and traffic levels. Data arriving from the sensors in real time highlights how better information can improve municipal services. For example, waste collection and street maintenance may be flexibly managed through better analytics. The SmartELI open communication protocols ensure easy integration of additional devices to the existing network.

Kalaranna Smart Street has initiated a discussion about how can IT solutions make Tallinn a better living environment. Municipalities are keen to learn how to invest in future-proof technologies, how to save costs and use existing resources more sustainably. Eliko's vision is to make Kalaranna a collaborative space for researchers, companies and citizens to co-develop additional services for local citizens and visitors.[41]

Tallinn City projects in 2017-2020 will include new Traffic Light System (with motion sensors), Dashboard (weather station), Bike-cycle and Pedestrian Counting System with cameras. Also the street with variable direction traffic and continuous road signs will be implemented.[42]

The Smart Port Solution

Smart Port is a harbor traffic-flow management solution for the Port of Tallinn for pre-check in, check-in, and line management, which is suitable for ports with multiple ferry operators.

The goal is to minimize the time spent in the harbor by providing a fully integrated and comprehensive, easy to understand service for travelers with vehicles.

Passenger numbers have increased, but port sizes have largely remained the same, which creates a challenge in continuing to provide a high-quality service. Many city harbors are no longer able to expand horizontally due to physical limitations, so there is a need to grow vertically. This essentially means creating an enhanced value for companies, business clients as well as to the end user by maximizing the benefit and impact of the existing resources.

The Smart Port solution incorporates a rather unique, automatic check-in system with a license plate recognition-solution for passengers with vehicles. The new solution encompasses the entire travel process for passengers with vehicles, starting from online pre-registration to the automated check-in procedures, and the fully automatic traffic management at the harbor — right up to getting on the ship.[43]

[41] https://www.eliko.ee/smart-street-lighting-system-monitors-environment-traffic-tallinn/
[42] http://smartcitylab.eu/solutions/smart-street-systems
[43] https://its-estonia.com/en/2017/03/17/the-smart-harbour-solution/

Border Queue Management

Introduced in Estonia in 2011, the border queue management service is an ICT-based tool that lets car and truck drivers reserve time slots for passing through border checkpoints, thereby eliminating the need for physical queues.

Developed by the Estonian company GoSwift as part of a public-private partnership, the service is used at all three checkpoints on Estonia's border with Russia.

Prior to the system's introduction in 2011, cars and trucks were processed on a first-come first-served basis, which forced drivers to queue for hours or sometimes days near the border. The situation was particularly difficult for truck drivers as it made them vulnerable to fatigue and crime.

Making the queues virtual has meant that drivers arrive at the checkpoint at their appointed times and are processed quickly, with waiting times now averaging as little as 30 minutes. In addition to drastically improving the lives of drivers, the change has allowed logistics companies to save millions of euros through better planning.[44]

Mobile Parking

Mobile Parking is a convenient system that can be used in privately owned and public parking facilities in Estonia allowing drivers to pay for parking using their mobile phones.

The system can be used manually through a downloadable app, but can also be set up for automatic Mobile Parking so that user's phone does everything for her.

If global positioning is active in the settings in the phone, the Mobile Parking app will display the two closest parking zones on its front page. Manually commencing and terminating the parking session is fast and user can also see an overview of the parking sessions for the last six months.

The new fully automated mobile parking solution makes parking even easier. This means that the parking session will begin as soon as the ignition is turned off, and ends when the car re-starts. To use automatic parking user has to install the correct app on her smartphone, and pair the car and the smartphone using bluetooth.

The app will choose the right parking zone when parking in a paid parking area and will begin and end payment independently. User will receive a notification in the app regarding the start and end of her parking session. At the end of the month, the cost of the parking will be added to the driver's mobile phone bill.[45]

[44] https://e-estonia.com/solutions/location-based-services/border-queue-management

[45] https://e-estonia.com/solutions/location-based-services/mobile-parking

Ride-sharing Regulation

In 2017, Estonia became the first European country to legalize and regulate ride-sharing.[46] The new law regulates the activities of online platforms that offer rideshare services and run both ordering the ride as well as calculating the fare through an IT platform.

The bill that preceded in Parliament was introduced by 26 members and called for changes to the Public Transport Act, the Traffic Act, and the State Fees Act in order to regulate rideshare services and define their position compared to established and regulated taxi services.

The law disposes of the requirement of professional training for taxi drivers and instead leaves it to the taxi and rideshare businesses to arrange all necessary instruction. The result is flexible regulation that allows for different business models while still providing a clear legal framework for all taxi services.

The previous legal base was extended to include services as well that are offered through an online platform. In case both the ordering and the price calculation of a ride is done online, it disposes the requirement of a taximeter. Price limits set by local governments for taxi services don't apply to online platforms that display the price of a trip before the passenger gets into the car, as a too expensive ride can be rejected.

In all other cases, e.g. where a taxi is ordered through a call center, or if the online platform only arranges trips, but doesn't show the price up front, taximeters are still required.

Changes made to the bill during its second reading in the Riigikogu included getting rid of the requirement of professional training, and giving taxi drivers the right to offer services through IT platforms online.[47]

[46] https://www.forbes.com/sites/montymunford/2016/02/28/estonia-embraces-uber-and-taxify-as-first-european-country-to-legalize-and-regulate-ride-sharing/2/#6677f2ef61bf
[47] https://news.err.ee/602458/riigikogu-passes-uber-law-to-regulate-rideshare-services


public safety
©Visit Estonia

Public Safety

The introduction of IT has helped to strengthen public order in Estonia and assist in the case of accidents. The use of IT tools in the security services (e-Police, rescue board, emergency centre) has halved the number of deaths by accident in Estonia over the last 20 years.

Employees of the security services are now able to remotely determine 35% of the locations of accident victims to within a 5-metre radius, and 93% of emergency calls are answered within 10 seconds. Estonian police is no longer allowed to stop cars for technical checks, as all the relevant data is available using their onboard computer. This has made the police 50 times more efficient.

In 2000, Estonia made headlines pioneering a system that instantly pinpoints the location of any mobile phone used to make an emergency call.

35% of accidents located remotely within 5 metres

2nd fastest court proceedings in Europe

Police works 50 times more effective

e-Law

The e-Law system is an online database for the Estonian Ministry of Justice that allows the public to read every draft law submitted since February 2003. Built using blockchain technology, it is formally known as the Electronic Coordination System for Draft Legislation.

Readers can see who submitted the legislation, its current status, and changes made to it as it passed through the parliamentary process. Once an act becomes law, it is published in the online state gazette Riigi Teataja, another searchable database that acts as an open legal library.

A similar system used by Tallinn City Council makes it possible to follow all council sessions online, while city legislation and other documents are available on the municipal homepage. Projects such as these create an unprecedented level of transparency in the state, cut down on corruption, and encourage citizens to take an active interest in legislative affairs.

To increase international and business cooperation, almost 500 legal acts have now been translated from Estonian into English. Since 2014, people from 185 different countries have viewed the translated laws. [48]

e-Court

The e-Court system called Courtal is a fully comprehensive system for managing all court procedures. Thanks to fully automated court processes and electronic communication tools, the system is considered one of the most effective court systems in the world.

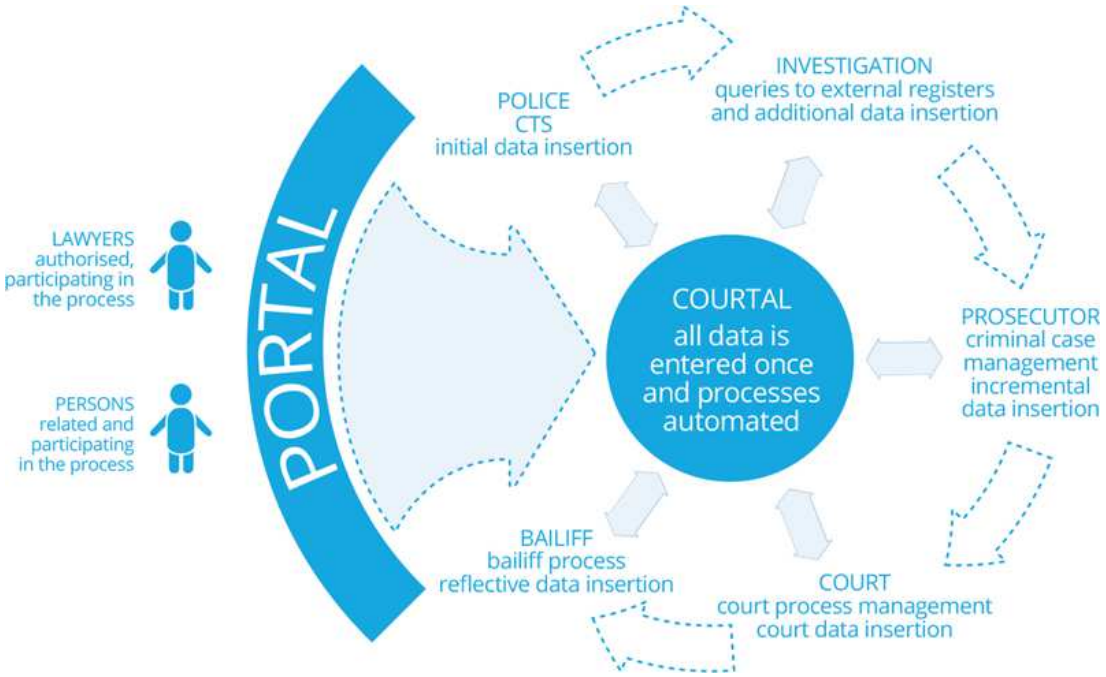


FIGURE 6. COURTAL INFORMATION SYSTEM. SOURCE: COURTAL.COM

The solution has been implemented for Estonian courts under the Ministry of Justice and paperless proceedings have been held since 2015.

The initial claim can be entered via a public portal 24/7 and within one hour the court clerk can confirm the case and appoint the first hearing. Once confirmed, the workflow engine delivers the necessary data to the portal for the allocated judge. Meanwhile, the judge and other participants can submit further items of evidence electronically, answer questions and even involve legal representatives and lawyers in the process.

If the case is simple, the hearing will be held electronically with no need to visit the court house. All participants will be sent the decision through the public portal using X-Road. Finally, the concluding or bailiff procedures are also automated — the fine is collected automatically without any need to physically attend to the payment.

Courtal operates under one-time data entry principles. All information that is generated during the work process, is reusable and

[48] https://e-estonia.com

participants in the process can use the data already in the system. It enables better automation. External users such as private persons, lawyers, attorneys, can access the process over Public Portal via secure channel.[49]

e-Police

Estonia's e-Police system is based on the principle that providing the best possible communication and coordination will lead to the most effective policing. This involves two main tools: a mobile workstation installed in each patrol car, and a positioning system that shows headquarters every officer's location and status.

The positioning system provides the operations centre real-time information about the location and status of each patrol vehicle. This information is clearly displayed on a map, making it easy for commanders to send the closest vehicle whenever a call comes in, thereby improving response times.

A mobile workstation is installed in every patrol car, providing officers in the field almost instantaneous access to vital information such as place of residence, photograph, telephone number or driving license data, vehicle, owner/user and technical inspection information and even whether the driver owns any registered weapons. In fact, the police could potentially access a dozen relevant databases, and the system is integrated with the information system of the Schengen Zone, allowing them to see if the vehicle is stolen or if the driver is wanted in another country.

Earlier, these queries were handled over the radio and typically took 15 to 20 minutes, now they take as little as 2 seconds. The difference allows officers more time to answer calls, resulting in more effective policing.[50]

Estonia is the first country to rely on the ID card for checking a driver's permit and related status information[51] – if the driver carries an identity document, there is no need to carry a driving licence issued in Estonia.[52] Police cars are equipped with an ID card reader enabling easy and fast access to the corresponding databases.

Web-constables

Web-constables are police officers working in internet. They respond to notifications and letters submitted by people via internet and train children as well as adults at issues of internet security. The first Estonian web-constable Andero Sepp started his work on 1 June 2011.

People contact web-constables by means of different (social media) portals as well as by

[49] http://www.courtal.com/
[50] https://e-estonia.com
[51] https://www.gemalto.com/govt/customer-cases/estonia-eid
[52] https://www.eesti.ee/en/traffic/vehicles-and-right-to-drive/driving-licence/

e-mail. Some issues are solved by advising only, but there are also such notifications that are forwarded for information or proceeding to relevant police stations. Greatest part of the questions is about issues related to fraud, thefts, defamation and traffic. There are no age limits and preferred is correspondence in Estonian, English or Russian. Letters are responded to at the first opportunity or at latest within three working days.

The purpose of web-constables is to advise, they do not proceed offences themselves.[53]

Digital Emergency Response System

The Estonian emergency response system "GIS-112" project was launched in 2010 to help reduce the response time of emergency services to help save more lives and reducing property damage.

At the heart of the system is a user-friendly digital map, located both in the control rooms of the Estonian Emergency Response Centre (EERC) and within the rescue vehicles and ambulances. Real-time data is fed in from multiple mobile devices, and the system recommends the most appropriate resources to respond to the emergency. The map displays the scene of the incident, the fastest route and the realtime location of available resources.

In short, the system has two components:

- Rescue center system in the command and control center which includes an emergency call registration system and a rescue planning and dispatch system
- m-Rescue mobile application on board all emergency vehicles.

The system helps decrease the number of casualties during fire accidents and speed help to the injured, thereby increasing the number of resuscitated patients and minimizing environmental and property damage from these accidents. The solution enables:

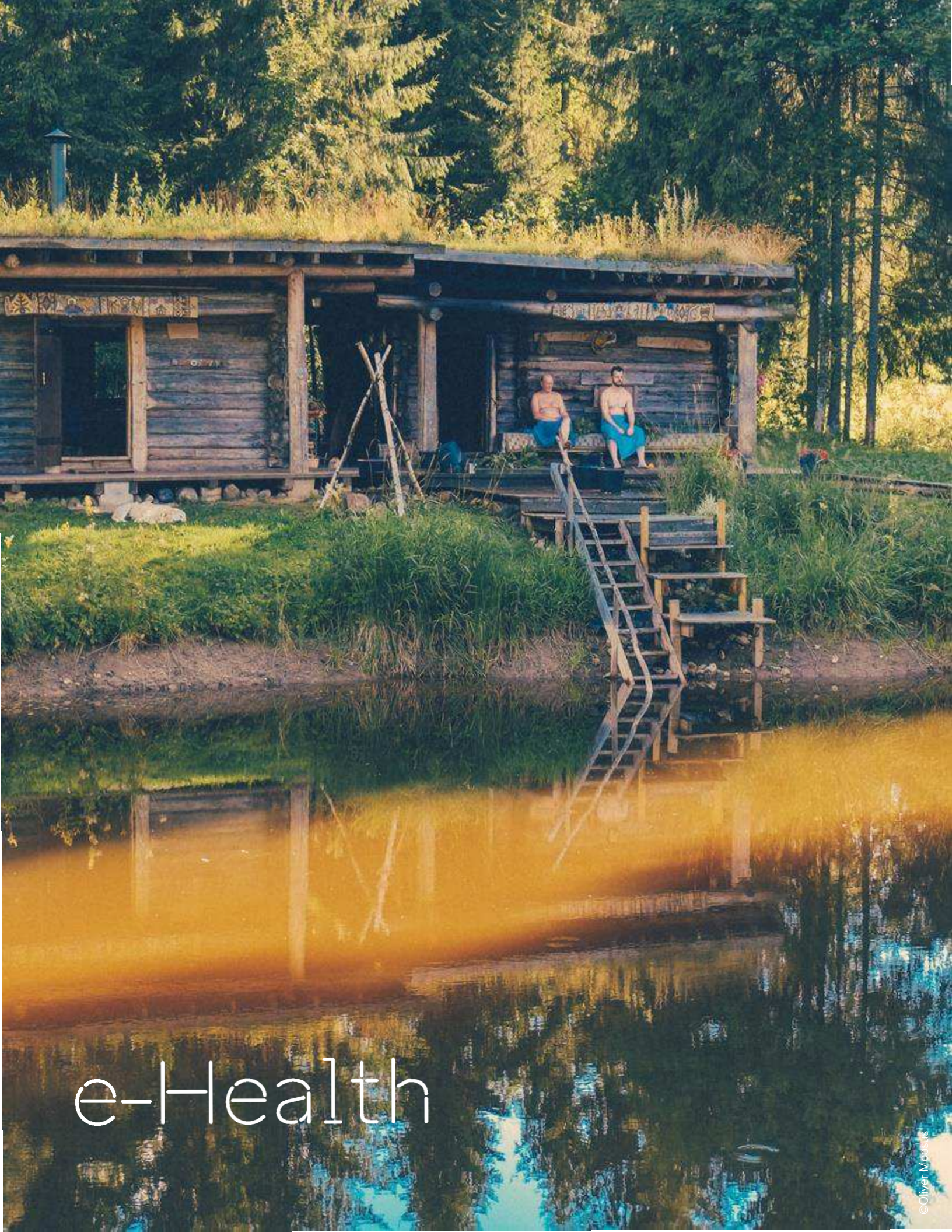
- Faster location of the scene of an accident by positioning the caller or accident location on a digital map
- More flexible and efficient decisions by displaying all resources and their status on the digital map
- Faster and accurate sharing of information by exchanging data electronically between the EERC, rescue teams and ambulance brigades
- Getting help to the scene faster using electronic map-based data exchange, drawing up the fastest set-off plan for each event, and displaying the fastest route to the scene
- A complete view of the events and more efficient resource management by showing rescue and ambulance

[53] https://www.politsei.ee

events on the map chronologically and geographically.

Emergency response system was developed by CGI in collaboration with the EERC, SMIT, the Estonian Rescue Board and the Estonian Health Board. The system went live in the summer of 2014.[54]

[54] https://www.cgi.ee/sites/default/files/files_ee/casestudies/cgi-case-study-innovative-emergency-response-system-helps-save-lives.pdf



e-Health

e-Health

In Estonia, patients own their health data and hospitals have made this available online since 2008. Today, over 95% of the data generated by hospitals and doctors has been digitized, and KSI Blockchain technology is used for assuring the integrity of stored electronic medical records as well as system access logs.

97% of prescriptions are digital

100% electronic billing in healthcare

97% of patients have countrywide digital record

e-Health solutions allow Estonia to offer more efficient preventative measures, increasing the awareness of patients and also saving billions of euros. Each person in Estonia that has visited a doctor has his or her own online e-Health record, containing their medical case notes, test results, digital prescriptions and X-rays, as well as a full log-file tracking access to that data.

Therefore, doctors can access their patient's electronic records, no matter where they are and make better informed treatment decisions.

Siim Sikkut, the Deputy Secretary General for Communications and State Information Systems at the Ministry of Economic Affairs and Communications:

"The building blocks we have built up, from digital prescriptions or nationwide electronic health records, are good pillars for further iterations of our e-health services. At the same time, there is definitely more we could and indeed should do to make use of tech to really transform the core of the health system here — opportunities based on new tech have increased in health, perhaps the most of all fields in the last few years. That is exactly why our government approved in December 2015 the new e-health strategy — to catch up with new tech opportunities.

The Estonian e-health strategy has five focus areas — basically five directions in which we will kickstart new innovation initiatives and systemic change.

First, personalized medicine — combining different data from national electronic health records to your genome information to offer better prevention and medical care that is fine-tuned to your personal conditions.

Second, we will work to integrate health services and stakeholders as well as health and welfare systems together for holistic case management throughout the whole healthcare chain.

Third, we will undertake digital steps to support moving our medicine towards an outcome-based model and comprehensive quality assessments.

Fourth, we will start introducing teleservices into the healthcare portfolio and also create the framework for relevant bottom-up innovation by companies.

Fifth to support all of this we will redesign and improve upon how data is captured, stored, and shared as the foundation for all other directions. Basically, we will be redesigning our core e-health information system.

The aim of redesigning our core e-health information system is to enable the world of connected health — to turn our e-health system from central data repository to a data exchange platform. So far, only licensed medical institutions can send data to the health record system (for them it is mandatory). But not only do people today capture so much data through wearables and various private services themselves but there is also enormous amounts of environmental data available . We want to remake e-health as a platform to enable various third-party services and devices to also enter data into people's health record if they choose to. This way, health specialists would have much more data to work from for prevention as well as treatment side.

We also want to remake the e-health information system to allow for more and better sharing of data beyond just the official health system, like now. If people want and consent, they could share all their health record easier with third-party services providers — be these a diagnostic app or innovative health services or other. These can offer you better service again, if they have more data to use. Thus, all in all, the vision is clear — the e-health core system should become a two-way exchange platform. At the moment this is more of an organizational redesign than a technical one. When implemented, it will make the promise of very personal, precise and timely health services."[55]

e-Health Records

The Electronic Health Record (e-Health Record) is a nationwide system integrating data from Estonia's different healthcare providers to create a common record every patient can access online.

Functioning very much like a centralized, national database, the e-Health Record actually retrieves data as necessary from various providers, who may be using different systems, and presents it in a standard format via the e-Patient portal. A powerful tool for doctors that allows them to access a patient's records easily from a

[55] http://connectedhealth.ee/siim-sikkut-e-estonia-stands-strong/

single electronic file, doctors can read test results as they are entered, including image files such as X-rays even from remote hospitals.

For assuring the integrity of retrieved electronic medical records as well as system access logs, blockchain technology is used.

For example, in an emergency situation, a doctor can use a patient's ID code to read time-critical information, such as blood type, allergies, recent treatments, on-going medication or pregnancy. The system also compiles data for national statistics, so the ministry can measure health trends, track epidemics, and make sure that its health resources are being spent wisely.

Patients have access to their own records, as well as those of their children. By logging into the e-Patient portal with an electronic ID-card, the patient can review doctor visits and current prescriptions, and check which doctors have had access to their files.

A special regime of laws and regulations has been established in order to regulate Estonian National Health Information System (ENHIS). The Health Services Organisation Act establishes the general basis for the functioning of ENHIS. On the other hand, there is no special regulatory regime applicable to e-health records recorded by healthcare service providers in their own local databases. Therefore general requirements for processing health records apply to e-health records that are not synchronised with the central database.

It is a distinctive feature of Estonian e-health that uniform classifications, standards and nomenclatures required for describing diseases, symptoms, and conditions have been developed and published.[56] The development of these classifications, standards and nomenclatures is at an advanced stage and the Estonian E-Health Foundation and the Ministry of Social Affairs organise the training of healthcare professionals in order to increase the usage of that uniform terminology.

While there is no legal obligation for encryption of e-health records, they need to be kept secure and confidential, and in practice both ENHIS data and the vast majority of e-health records that individual healthcare service providers process are encrypted. Healthcare service providers are not prohibited from using an interface or software that is provided by a private company and there are no restrictions for the location of the servers where the records are kept.

Patient consent is not necessary in order to create e-health records or share them for the purpose of providing healthcare. Estonian law provides patients with an opt-out for the sharing of ENHIS data: the patient can make all or particular e-health records inaccessible in the system. In order to invoke that right, a patient must submit an application to his or her healthcare service provider or to the Ministry of Social Affairs.

Access and updating of e-health records

Any Estonian healthcare professional is able to access ENHIS data for any patient, if the

[56] http://pub.e-tervis.ee/

healthcare service provider that employs the healthcare professional has a valid Estonian activity licence and unless a particular patient has prohibited access to his or her data. ENHIS data must only be accessed for the purpose of providing healthcare services. Patients are the owners of their health data and can view the access log to their data on the patient platform 'My E-Health'. Patients have as a rule full access to all of their ENHIS data.

Healthcare professionals have the legal obligation to update ENHIS when providing a healthcare service to a patient. Before gaining access to ENHIS data, the validity of the healthcare provider's activity licence and healthcare professional's registration are checked.

The legal framework applicable to e-health records that are part of the healthcare service provider's local database are more ambiguous. Healthcare providers are required to document the provision of healthcare services, yet this documentation does not have to be electronical.

The breach of confidentiality by healthcare professionals is a criminal offence under the Penal Code. If the patient's rights have been violated upon processing of personal data, he or she may claim damages in civil court.

Archiving and secondary use

ENHIS data is archived indefinitely. Archiving of ENHIS data is regulated by the Statute of Health Information System.

Secondary use of e-health records is allowed for scientific research or statistics and it is mainly regulated under the Health Services Organisation Act and the Personal Data Protection Act. The requirements for secondary use of e-health records depend on whether the data is anonymised or not. If the data is anonymised, it does not constitute personal data and therefore falls outside the scope of the Personal Data Protection Act. Anonymised (coded) health data is not personal data and can be used for scientific research or official statistics without the consent of the patient. There is therefore no opt-out system in this regard.

The patient can however opt-out of secondary use of non-anonymised ENHIS data. In order to do that, the patient must submit an application to his or her healthcare provider (to prohibit use of ENHIS data connected to that provider) or to the Ministry of Social Affairs (to prohibit use of all personal data in ENHIS).[57]

[57] Overview of the national laws on electronic health records in the EU Member States - National Report for the Republic of Estonia by Milieu Ltd and Time.lex

e-Prescription

One of the key innovations in Estonia's e-Healthcare system, e-Prescription, is a centralized paperless system for issuing and handling medical prescriptions.

When a doctor prescribes medicine using the system, he or she does so electronically, with the aid of an online form. At the pharmacy, all a patient needs to do is present an ID-card. The pharmacist then retrieves the patient's information from the system and issues the medicine.

Because the e-Prescription system draws on data from the national health insurance fund, any state medical subsidies that the patient is entitled to, also appear, and the medicine is discounted accordingly. Another major advantage of the system is that doctor visits are no longer needed for repeat prescriptions.

A patient can contact the doctor by e-mail, Skype or phone, and the doctors can issue repeats with just a few clicks, and the patient can collect the medicine from their closest pharmacy.

Today, 97% of all prescriptions in the country are issued electronically. This frees up time for patients and doctors, and reduces administrative strain on hospitals.[58]

The Digital Prescription database and the Estonian National Health Information System (ENHIS) is separate and independent from each other and exist in parallel. However, the Digital Prescription database is connected to the ENHIS, as some of its content is automatically transferred to the ENHIS, but in order to see the full history of digital prescriptions, the patient has to log in to the state platform eesti.ee. So Digital Prescription database and the ENHIS have part of their data in common.

The usage of the two databases by healthcare professionals is not interdependent, even though in most cases healthcare professionals have access to both. As an exception, pharmacists do not have access to ENHIS data. They have access to the Digital Prescriptions platform and can view only valid and open prescriptions, not any past ones.

It is not obligatory for doctors to have access to the ENHIS in order to write a regular prescription or ePrescription. However, all healthcare professional do have such access to patients' e-health records on the ENHIS.[59]

[58] https://e-estonia.com/solutions/healthcare/e-prescription

[59] Overview of the national laws on electronic health records in the EU Member States - National Report for the Republic of Estonia by Milieu Ltd and Time.lex

The Estonian Genome Project

The Estonian Genome Project is a large population-based databank that was established with health records and biological samples from a large portion of the Estonian population for use in biomedical and genetic research to improve the public healthcare in Estonia. The Genome Centre today holds more than 52,000 DNA samples that is 5 percent of the Estonian population.

There are currently more than 120 biobanks worldwide, but the majority of them focus on genomic research rather than personalized medicine. The Estonian biobanking system, by contrast, is built on a law that fundamentally protects gene donors' privacy and establishes their rights. The Estonian Human Genes Research Act governs the activities of the biobanking project: It establishes anonymity in clinical research, enables donors to decide which studies they want to participate in, and gives donors full control over who has access to their data. By default, a donor's doctor is the only other person who can look at his or her genetic information through the portal, unless the donor authorizes more people.[60]

Unlike other gene discovery efforts, participants in population-based projects are not selected by specific disease type but rather via a random sampling process. The unbiased nature of the recruitment process provides a more accurate measure of the disease risk provided by particular genetic variants.[61]

The efforts to establish the Genome Centre started back in 1999 with a decision to establish a foundation that, under the Estonian Human Genes Research Act, has three objectives — to gather information on the health of the Estonian population and their genes, study this cohort scientifically from both genetic and medicals aspects and use the data obtained to improve national health.

Up to 2011, the main goal of the Genome Centre was to establish an extensive database and to carry out research studies based on that data. In 2017, the centre passed a key milestone — the gene donors in the database received their personal whole genome sequences, which means that the Genome Centre in the form planned back in 2000 — a repository for data — came to fruition.

"It took longer, but the result was much better as well. Work on the Genome Centre continues: if genetic medicine, an important component of personalized medicine, is to expand nationwide to everyone interested, the Genome Centre will have to grow ten times bigger and the sequencing of the whole genome for these people will have to be done as well. As such, it would already be part of the health information system. Then we will also see significant outcomes in healthcare that would cost significantly less per person than they have to this point, "says Estonian Genome Centre director Andres Metspalu.

[60] https://www.theatlantic.com/health/archive/2015/10/is-a-biobank-system-the-future-of-personalized-medicine/409558/

[61] Drug Development Research 62:97–101 (2004)

"The current Genome Centre donors received their personal whole gene sequences, which their general practitioners can use as an additional instrument in diagnosis and determining course of treatment, just like MRIs, ultrasound, X-rays or laboratory testing where the specialist records the findings of the test or procedure. A whole gene sequence will allow doctors to make personal recommendations or take the genetic information into account in determining treatment. For instance, if you have a complete lack of an enzyme like CYP2D6 that helps metabolize medicines, codeine-based pain relievers won't work. As codeine itself isn't an analgesic, it needs to be broken down into morphine first. Quite a few examples like that are known," says Metspalu.

The main objective of the practical output is to realize preventive medicine: if all Estonian people could get their whole genome sequenced, the risks would be known in advance and they could be dealt with. "Today Estonia has about 70,000 type 2 diabetics — if we could help even one-fifth of them, that would be a great number. We have 28,000 people who have gone blind from glaucoma, but in 90% of the cases, it is a form of the disease where the possibilities of genetics could be applied and people could be sent early for monitoring and have their intraocular pressure measured. Breast cancer is another disease where we could identify people who should undergo early screening," Metspalu says.

"Healthcare information specialists are currently working to make sure all of the information gets to General Practitioners (GPs) in a matter of seconds, not minutes as it is now. The Genome Centre would make sure that at some point, when GPs look at patient data, they also see their genetic risks and whether a given drug is suitable for them. The other major task is to develop a system — once we have a whole gene sequence, it can be refined and updated all the time, upon discovery of variants that are connected to some trait. So our information continues to become more accurate," he adds.[62]

[62] http://connectedhealth.ee

education

Education

The educational digital revolution in Estonia aims to implement modern digital technology more efficiently and effectively in learning and teaching, and to improve the digital skills of the entire nation. For example, it includes ensuring that every student receives the necessary knowledge and skills to access modern digital infrastructure for future use.

Estonia's success in the digital revolution can be seen in the educational landscape since twice as many students pursue IT careers in Estonia than the average in other OECD countries. Higher education is free in Estonia at public universities.

e-School has more than 200,000 active users

1st in Europe in the OECD PISA test

85% of schools use e-School

ELIIS - The Online Software for Kindergartens

ELIIS is an online software solution that provides innovative and digital solutions for pre-schools and kindergartens to organize their daily work.

Used in 50% of kindergartens, ELIIS is easily manageable to people otherwise not so familiar with computers. The environment is protected against non-authorized users and the access for teachers and parents to see and manage the data can be specified in each section by the staff of each organization.

The experience and feedback so far has been very positive: kindergarten teachers have been freed from filling in large amounts of daily paperwork, especially reports, in order to dedicate more time for the children.

Parents are happy because of the comfortable and quick feedback about their children and overall activities done in the preschool or kindergarten. Mutual communication has become more convenient, accurate and fast.

Parents have a convenient way to have a say in class activities, to be aware of your child's and kindergarten activities, browse pictures of events and be in a direct contact with teachers.

Simple, convenient and paperless environment for all kindergarten employees allow compact communication with parents and storing all documents in one place.

Comprehensive reporting and statistics about meals and occupancy, control teachers and class listings and communicate by sending notices or messages to kindergarten employees or parents.

ELIIS functionality includes:

- A teacher-friendly class register / journal
- Weekly and monthly plans
- Child development map
- Thorough communications module for teachers, managers and parents
- Events calendar with gallery
- Short surveys for getting feedback from parents
- Children profiles with different customizable maps
- Detailed statistical reports
- Document management
- Announcement board
- Annual goals[63]

ProgeTiger Programme

Programme ProgeTiger was launched in Estonia in 2012 when the idea of teaching programming and robotics was introduced to Estonian schools. Also at that time the start-up Codecademy.com was making headlines in the world and Estonia took a big step to be on board with this initiative. They started to train teachers, develop learning materials and translate Codecademy.com programming courses.

Today the ProgeTiger programme has developed into technology programme widely targeted at engineering sciences, design & technology and information & communication technology (ICT).

Programme is aimed at preschool, primary and vocational education in effort to integrate technology education into curriculum, offering teachers educational resources and training opportunities, financially supporting kindergartens and schools in acquiring different programmable devices.

ProgeTiger programme is supported and funded by the Estonian government through the Estonian Ministry of Education and Research.

Curricular support - in primary education there is a national cross-curricular theme called "Technology and Innovation" which requires all teachers to implement technology in their teaching. That means that teachers have to integrate technology in their subjects in different fields (for example

[63] https://e-estonia.com/

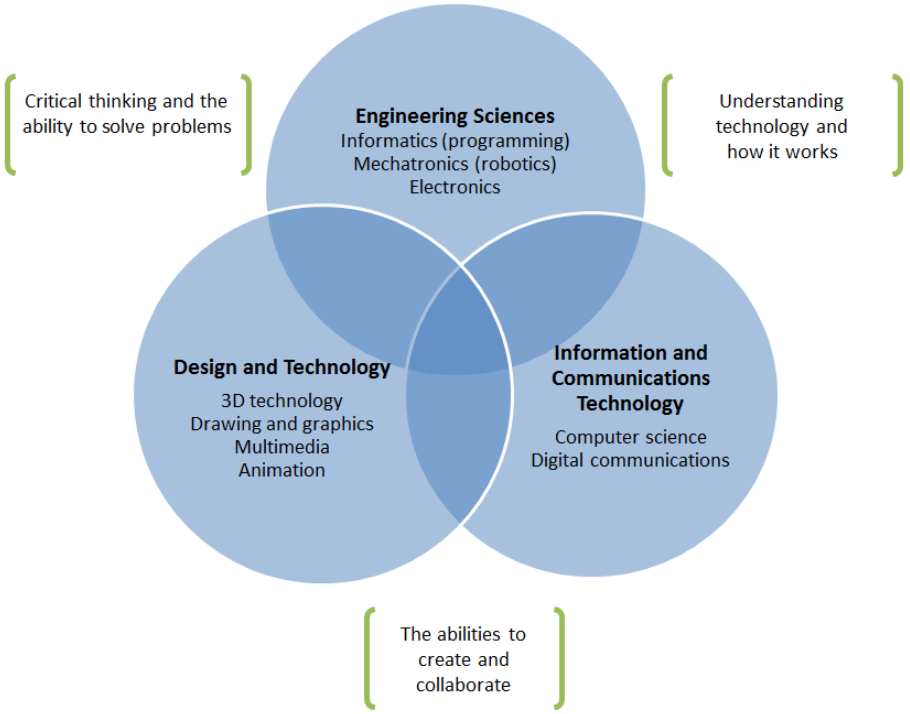


FIGURE 7. PROGETIGER PROGRAMME IS TARGETED AT ENGINEERING SCIENCES, DESIGN & TECHNOLOGY AND INFORMATION & COMMUNICATION TECHNOLOGY. SOURCE: HITSA

using Scratch in mathematics, music programs in music lessons and so on).

It does not say what to use or how to use technology specifically. Teachers can choose themselves how they want to do this. Also there is different national optional curriculas and schools own subjects in technology education (programming, robotics, 3D graphics, computer science, informatics etc.) which schools can choose to add into their school programme (approximately 67% of Estonian schools have one or more optional lesson in their programme).

At all educational levels Estonia has extra-curricular activities in kindergartens and schools. Also there are many voluntary initiatives and children have a chance to be involved in different recreational activities (like robotics, coding clubs etc.).

Some examples what teachers do in schools:

- In preschool, teachers teach and use LEGO WeDo, Kodu Game Lab, tablets (apps), programmes to make animations etc.
- In primary school, teachers teach and use Kodu Game Lab, Logo MSW, Scratch, LEGO Mindstorms EV3, mobile app making programmes and environments, many different programmes and environments which are used for teaching various subjects (music, mathematics, physics, biology), e-labs etc.
- In high school and vocational education, teachers teach and use different programming languages (Python, JavaScript etc), Codecademy.com courses, 3D graphics, robotics, programmes to make games, web-pages and apps etc.[64]

[64] http://hitsa.ee/it-education/educational-programmes/progetiger

e-School

The two most widely used web applications for schools in Estonia are called e-School and Stuudium. These innovative tools provide an easy way for parents, teachers and children to collaborate and organize all the information necessary for teaching and learning.

eKool (the Estonian name for its e-School service) was launched in 2002. It is the most used e-service of all time in the country. In 2010, 95% of Estonian students used the service. The application is used on an ongoing regular basis by 28 to 30% of the population. Access to eKool is voluntary and secure.[65]

Stuudium is a suite of online apps for schools that connects teachers, parents and students. Study materials, information about academic progress and simple messaging are accessible in one online environment.[66]

These systems provide an array of functions for its various users:

- Teachers enter grades and attendance information in the system, post homework, and evaluate student behaviour. They also use it to send messages to parents, students or entire classes.
- Parents use it to stay closely involved in their children's education. With the help of round-the-clock access via the internet, they can see their children's homework assignments, grades, attendance information and teacher's notes, as well as communicate directly with teachers via the system.
- Students can read their own grades and keep track of what homework has been assigned each day. They also have an option to save their best work in their own personal e-portfolios.
- The school staff can use a flexible intranet system to effectively communicate with coworkers. Management can get a deep understanding of overall progress in the school through set of real-time reports on absences and academic progress.
- District administrators have access to the latest statistical reports on demand, making it easy to consolidate data across the district's schools.

[65] https://www.gemalto.com/govt/inspired/estonia/ekool

[66] https://stuudium.com/en/

DreamApply

Studying abroad is becoming more attractive year after year. Universities have to cope with an increasing number of applications from across the globe meanwhile differentiating high-quality students. In most universities today, student admission is often overly bureaucratic and difficult to track.

DreamApply is a specialised international higher education/mobility management software, offering its users a tablet and phone friendly user interface. It is mainly used for the recruitment process of full-degree candidates in full time and part time studies in all levels (BA, MA, PhD and even summer courses) but it is also used for incoming and outgoing exchange management. Not only for student exchange but also staff and teacher exchange.[67]

As a student recruitment and marketing system, it contributes to increasing the number of enrolled students by concluding and solving different problems, such as having all relevant information related to the admission available in one place, and reducing irrelevant e-mailing and administrative work for university personnel. Several university application systems have been built using the DreamApply platform; for example, in Estonia, Italy, Finland, Lithuania and Ireland.

DreamApply was launched in 2011 in Estonia and today serves universities in 20 countries.

Information Technology Foundation for Education (HITSA)

The Information Technology Foundation for Education (HITSA) is a non-profit association established by the Republic of Estonia, the University of Tartu, Tallinn University of Technology, Eesti Telekom and the Estonian Association of Information Technology and Telecommunications.

The role of the HITSA is to ensure that the graduates at all levels of education have obtained digital skills necessary for the development of economy and society and the possibilities offered by ICT are skillfully used in teaching and learning. This helps improve the quality of learning and teaching at all levels of education.

In the field of information technology and education HITSA represent Estonia in international cooperation projects and initiatives.

The HITSA's Innovation Centre develops an evaluation model of educational technological skills, which is meant as a self-analysis tool and professional development

[67] https://dreamapply.com/about-us/

support tool for teachers and for their evaluation. The evaluation model and the development of training courses are based on the digital skills standards of the International Society for Technology in Education (ISTE), which provides an ideological framework for learners, teachers and educational managers to follow.

To improve these competencies, Innovation Centre organises briefing sessions, training courses, seminars and conferences.

The HITSA's Development Centre for Information Systems administers two national information systems in education - Admission Information System (SAIS) and the Study Information System (SIS). The aim of information systems is to secure safe, effective and flexible environment, which supports and automates study processes and facilitates the exchange of information between educational institutions and learners.

For general education, vocational education and higher education institutions HITSA offers the learning environment Moodle. Moodle is one of the most widely used learning management systems in Estonia that supports community-based learning over the Internet and is suitable both for the creation of online courses and for supporting classroom teaching.

Learning resources

Digital learning resources consist of learning materials (including textbooks, educational online videos and mobile apps, teaching games, e-worksheets, online tests, study objects), which are published in digital format (e.g. on the Internet, in databases or digital data media).

The HITSA's Innovation Centre supports the creation, adaption and re-use of digital learning resources and to that effect develops guidelines for the creation of high-quality learning materials. Innovation Centre also coordinates the work of the network of educational technologists in order to provide them guidance and support for creating digital learning assets in their own educational institutions.

The role of the educational technologist at an educational institution is to coordinate and develop e-learning process and to provide guidance to teachers and managers. These people know the tools of digital era and their usage methods very well and help introduce them into the study process.

The HITSA provides free access to two repositories of electronic learning materials and study objects to all users. Users can freely browse and download materials in both repositories:

The e-learning repository mainly holds learning materials in vocational and higher education in different formats, which concern different theoretical and practical matters in different fields of study. All learning materials have been released under Creative Commons licence. The HITSA's Innovation Centre is the official representative of Creative Commons in Estonia.

The repository of the School Life (Koolielu) educational portal mainly contains electronic learning assets sorted in line with the general education curricula. The subject experts of Koolielu update it on an ongoing basis with exciting learning materials that relate to the

curriculum. Anyone can give their contribution to the improvement of the database. The quality of the learning assets is guaranteed by subject experts who review all materials before their release.

The integrated educational portal is targeted at teachers and lecturers at all levels of education but all people interested in education are welcome to visit it. The portal has three main courses of activities:

- Diversification of teaching through exciting learning materials and the use of new technological means.
- The sharing of newest educational know-how and best practices. On every weekday, Koolielu presents major education-related news from Estonia and exciting experiences in educational technology from all the word. Koolielu also publish interviews and features with interesting individuals who have something to say in educational matters.
- The opportunity to interact and share through communities, chat-rooms and classified ads.
- Easy to consolidate data across the district's schools.[68]

Estonian Education Information System

The Estonian Education Information System (EHIS) is a state database that brings together all the information related to education in Estonia. The database stores details about education institutions, students, teachers and lecturers, graduation documents, study materials and curricula.[69]

This service is intended for anyone in education, whether students enrolled in general, vocational, higher or hobby programmes, or the teachers and academic staff providing that education. It is also possible to access information on the qualifications and further training completed by teachers and academics. EHIS is also part of monitoring the education system so that the authorities can make sure it prepares people for the labour market of the future.

EHIS stores data entered since 2005, so detailed information on general education levels across the population from school to university is available on request. Applying for university studies by simply transferring your details to the desired university is the most common use of the EHIS database.

[68] http://hitsa.ee

[69] https://e-estonia.com/

e-Residency

e-Residency

Estonia is creating a borderless digital society for global citizens as the first country to offer e-Residency. E-Residency is a transnational digital identity that anyone in the world can apply for to obtain access to a platform built on inclusion, legitimacy and transparency. E-residents then have access to the EU business environment and can use public e-services through their digital identity.

Estonia believes that countries will one day compete for e-residents based on the quality of their public e-services and their business environment.

People from 150+ countries have applied for e-Residency

Estimated 1.8bn EUR value from e-Residency to Estonia

2500+ companies have been established by e-residents

The primary reason e-residents are joining this community is to run a trusted location-independent EU business online with all the tools needed to conduct business globally.

e-Residents can:

- Establish and manage a location-independent company online from anywhere in the world
- Establish a trusted EU company online in one day
- Apply for a business bank account and credit card, and conduct secure e-banking
- Access international payment service providers (Paypal, Braintree, etc.)
- Digitally sign and transmit documents
- Declare Estonian taxes online

E-residents receive a digital ID-card with two PIN numbers for secure digital authentication and digital signatures. Secure digital signatures are legally equivalent to a handwritten signature and face-to-face identification in Europe, as well as between partners upon agreement anywhere around the world.

e-Residency Program Benefits for Estonia

On 21 October 2014, Estonia's parliament unanimously voted to extend national digital e-residency rights to foreigners. Launched in December 2014, the Republic of Estonia is one of the first countries in the world to offer government issued digital residency to non-resident citizens.

The innovative program has five main benefits for the Republic of Estonia:

Boost in domestic economic growth

- E-residents' companies boost local job creation rate and enhance demand for various local professional services.
- Job growth and increased demand encourage local consumption, boost economic confidence and create a platform for incremental economic growth.

Opportunity to scale

- Incremental demand from e-residents will provide an opportunity to local entrepreneurs to scale their businesses
- Increase the efficiency of operational assets, boost technological growth
- Cross-sectional opportunities for fintech and other new economy entrepreneurs.

Increasing national security

- Becoming interconnected with the rest of the world increases Estonian national security
- More nations are vested in Estonian wellbeing, ongoing development and national independence.

Estonia as travel destination

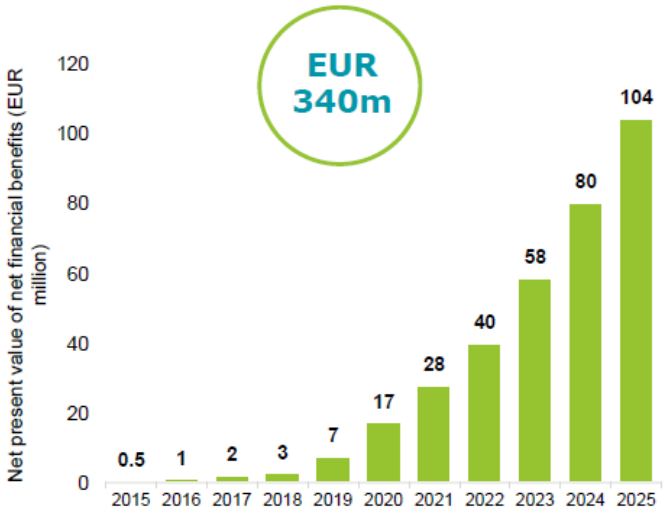
- Increasing international recognition is likely to boost interest in Estonia as travel destination
- This provides opportunities to regional tourism sectors across Estonia, encouraging local entrepreneurs is hospitality and other related sectors.

Estonia as brand

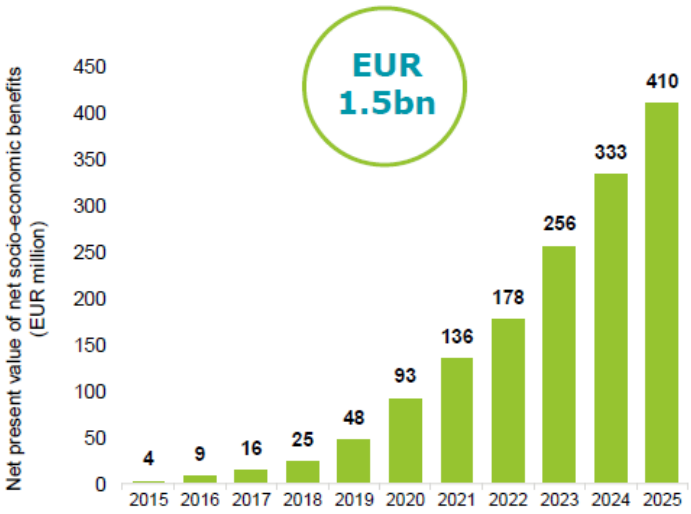
- Positive and forward-looking image of Estonia will increase the national visibility and economic and social bargaining power
- e-Estonians are the best sales team beyond the traditional country borders.

It is estimated that total cumulative net present value from e-Residency to Estonia is EUR 1.8bn of which EUR 340M is estimated to be related to direct financial benefits via incremental taxes and state fees and EUR 1.5bn as an estimated spillover impact via indirect socio-economic benefits.

Total estimated net direct financial benefits from e-Residency to Estonia



Total estimated net indirect socio-economic benefits from e-Residency to Estonia



Source: Deloitte analysis

By 2025 the borderless nation is expected to increase by close to 1 million e-residents, who have established an estimated 175 thousand companies globally. This would create close to EUR 70,000 of direct and indirect net profit created by an average e-resident company that is expected to remain in Estonia. That is an estimated total return of EUR 101 per 1 euro of investment (ROI) into the development of the programme.[70]

e-Residents Community

Joining the community of global location independent entrepreneurs and technology leaders is one of the key reasons for e-residents to join the program.

To address this, Rubiks Digital, the Digital Innovation Group was the first private sector representative to build a platform targeting Estonian e-residents exclusively.

Launched in 2015, eResNetwork claimed to be the world's safest community for digital citizens — all of the users on the network were validated through the e-Residency digital ID-card.[71]

Started with a lean approach and focused on learning from its users, the initial platform quickly became the main source of information, business networking and communication for e-Residents.

Using the feedback from its users, the responsibility was handed over to the official e-Residency team of Enterprise Estonia in

[70] Key Stakeholders' Report, Deloitte Estonia (December 2017)

[71] https://blog.rubiksdigital.com/the-first-networking-platform-for-e-residents-is-live-a6d963a14a6b

2018 to build the new improved community platform that would be tailored for the unique e-Residency community aiming to enhance their international businesses.

Estcoin

In August, 2017, Kaspar Korjus, the Managing Director at e-Residency, proposed an idea for Estonia to issue its own crypto tokens through Initial Coin Offering (ICO). Those crypto tokens, called Estcoins would make Estonia the first country with an Initial Coin Offering.[72]

The idea was supported by the Digital Innovation Group, Rubiks Digital claiming that this bold move would bring cryptocurrencies to a new era. Governmental cryptocurrency could solve the tax evasion and regulatory issue at the same time. "Having the possibility to supervise revenue generated by mining, the regulatory body could restrict the number of miners, similar to setting interest rates to control the traditional money supply, while collecting tax on this revenue," told Olavi Miller, Former Economist of the Central bank of Estonia.[73]

Although just an idea, the proposal went viral almost instantly, generating a large amount of media coverage globally, including in most major publications with around 200 million people to read about the idea.

The e-Residency team continued to pursue the idea and after a number of discussions with Estonia's Ministry of Finance, Members of both the national and EU Parliament, the Bank of Estonia, companies conducting ICOs, and law firms, the idea evolved with three potential action plans:

1. The community estcoin

The community estcoin would be structured to support the objective of growing the new digital nation by incentivising more people around the world to apply for and make greater use of e-Residency. This includes encouraging investors and entrepreneurs to use e-Residency as their platform for trusted ICO activity.

For example, e-residents should be able to earn estcoins if they drive web traffic to e-Residency, successfully sign up a new e-resident, post a tender within the community that provides work to another e-resident or Estonian company, or spend time providing useful advice to other e-residents.

Estcoins would enable that platform to grow faster through a network effect, but it's possible that any funds raised could also be allocated to further develop this platform, as well as provide investment into companies that operate within Estonia's business environment.

[72] https://medium.com/e-residency-blog/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894

[73] https://blog.rubiksdigital.com/how-estonia-could-bring-an-end-to-bitcoin-df5bdfe484ca

2. The identity estcoin

In this model, estcoins would be the blockchain-based tokens used for activities within the digital society, such as digitally signing documents, logging into services or enforcing smart contracts.

Estonians and e-residents would receive a certain amount of tokens that are personal and attached to their digital identity and can then acquire more tokens when required. Even if these identity estcoins would need to be purchased, this would not raise any additional revenue for Estonia, but merely contribute to the maintenance of the network. In fact, everyone would save money as a result of this proposal.

Identity estcoins would eliminate some of the technology that is currently required to operate the digital nation and that would also eliminate much of the costs and hassle that this technology brings.

3. The euro estcoin

The euro estcoin would combine some of the decentralised advantages of crypto with the stability and trust of fiat currency and then limit its use within the e-resident community.

The way euro estcoins would operate within the e-Residency community would be similar to how other types of tokens operate within video games or simulated online worlds. E-residents could purchase euro estcoins within their new platform then trade them with other e-residents and cash out when required, while ensuring that all necessary banking and taxations rules are followed.

The main difference of course is that e-residents are not playing with these tokens within the platform for fun. Instead, what they can win from the introduction of this variant of estcoin is frictionless global trade with other e-residents.[74]

[74] https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790


conclusion
© Johannes Arro

Conclusion

The story of the Estonian Digital background is not a story of overnight success or finding the next big thing. It is a story of consistency, trial and error and open discussion between the state and its citizens. It has been a joint effort for more than 20 years for this nation of 1,3 million people.

Becoming a digital nation, is not a privilege of a small country, if anything, it has been a survival route for a country with no natural resources, with insignificant political power, tiny population and limited capacity to protect its sovereignty.

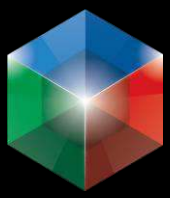
Involving its citizens to the decision process through open innovation and taking calculated risks to improve the lives of its people has really been the only way forward for Estonia. But now that Estonia has taken the necessary steps, it is even easier for other countries as well as corporations to follow their footsteps.

"We have learned from our own experience as well as from working with others — more than 120 governments have been exposed to or have tried to implement the Estonian digital government experience — that in the digital world, the size of the country does not matter. Despite some contextual differences, governments are very similar in the way we work.

Hence, digitization know-how and often even solutions can be copied well enough. For example, most of our digital government solutions are openly usable by others, starting with X-Road. Just try it out!

Also, the Estonian companies and partners who have helped us build the digital government here are happy to partner with governments and tech companies abroad to transfer know-how (including necessary legal and policy frameworks) and implement solutions there similar to those that work so well in Estonia." Siim Sikkut, the Deputy Secretary General for Communications and State Information Systems at the Ministry of Economic Affairs and Communications.

It is time to follow Estonia in its journey, even pass them where possible and emerge yourself fully to the digital world as this is really the only way forward.



Innovation Is Born Here

www.rubiksdigital.com